ВОДИЧ ЗА ИМПЛЕМЕНТАЦИЈУ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА

веб: www.nsa.gov.rs

Проф.др Горан Д. Матић

Београд, 2025. година

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!

САДРЖАЈ

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

ПРОЦЕНА ПРЕТЊЕ ЗА БЕЗБЕДНОСТ ТАЈНОГ ПОДАТКА ИЛИ САМОПРОЦЕНА ПО ЗАКОНУ О ИНСПЕКЦИЈСКОМ НАДЗОРУ И ЗАКОНУ О ТАЈНОСТИ ПОДАТАКА

Процена претње за безбедност тајног податка (самопроцена) по Закону о тајности података представља безбедносну процену која се примењује у раду са тајним подацима. Она обухвата:

- **Анализу и процену мера безбедности**
- **Идентификацију ризика**
- **Усаглашеност са прописима**

Органи јавне власти дужни су да редовно извршавају Процену претње за безбедност тајног податка (самопроцену) ради осигурања безбедног поступања са тајним подацима. За спровођење самопроцене или процене претње за безбедност тајног податка **одговоран је старешина органа јавне власти**. Он има кључну улогу у иницирању и надгледању процеса самопроцене.

Разлика између Процене претње за безбедност тајног податка код одређивања мера заштите тајних података (члан 30. Закона о тајности података) и Процене могуће штете по интересе Републике Србије код одређивања степена тајности података (члан 10, став 3. Закона о тајности података):

Критеријум	Процена претње	Процена могуће штете
Фокус	Анализа ризика и безбедносних мера	Потенцијалне последице откривања тајних података по интересе државе
Сврха	Заштита података, предузимање мера за безбедност	Процењивање последица по безбедност, одбрану, спољне односе
Кључне активности	Оценити могућности заштите података	Проценити утицај на националну безбедност и однос са другим земљама

Ова разлика између процена из члана 30. и члана 10. став 3. закона лежи у фокусу и сврси процене. Процена претње за безбедност тајног податка обухвата анализу ризика и безбедносних мера, као и могућности заштите података. Са друге стране, процена могуће штете разматра потенцијалне последице откривања тајних података по интересе државе, као што су безбедност, одбрана и спољни односи.

Ко спроводи процену претње за безбедност тајног податка или самопроцену?

- Старешина органа јавне власти може да одреди:
  - **Запосленог или групу запослених** са стручним знањем који ће директно бити задужени за спровођење самопроцене.
  - **Комисију** која укључује представнике различитих организационих јединица ради свеобухватног приступа процени.

Кључни критеријуми за процену претње - Према члану 30. Закона о тајности података, процена се заснива на следећим критеријумима:

1. **Степен тајности** – одређује ниво заштите.
2. **Природа документа** – анализира се садржај документа.
3. **Процена претњи** – идентификују се извори ризика и предлажу мере смањења.

Руковалац тајних података има важну улогу у:

- Оперативном управљању подацима у складу са законом.
- Праћењу примене безбедносних мера заштите података.
- Обезбеђивању исправности и комплетности документације.

Док је руководилац органа одговоран за спровођење процене, руковалац тајних података често пружа техничку и оперативну подршку у оквиру овог процеса.

Унутрашња контрола - Према Члану 84. Закона о тајности података:

- има задатак да прати и проверава спровођење Процене претње за безбедност тајних података (самопроцене) и других безбедносних процедура.
- Она се фокусира на идентификацију могућих недостатака и предлаже корективне мере како би обезбедила усклађеност са прописима.

Одговорност за унутрашњу контролу има руководилац органа јавне власти, а у одређеним органима јавне власти (нпр. министарства унутрашњих послова, одбране, или Безбедносно-информативна агенција), постоје посебно задужене организационе јединице за ове задатке.

Образовање и обука: Основни елементи заштите тајних података - представља кључну компоненту у изградњи свести запослених о заштити тајних података и развоју безбедносне културе:

1. **Разумевање процедура:** Обука доприноси бољем познавању и примени прописаних процедура у раду са тајним подацима.
2. **Умањење људских грешака:** Стечена знања и вештине омогућавају запосленима да:
    - Препознају и избегну опасности.
    - Адекватно реагују на претње.
    - Осигурају исправно поступање са подацима.
3. **Спремност и одговорност:** Безбедносна активност подразумева:
    - Спремност деловања у складу са усвојеним знањима, вештинама и вредносним ставовима.
    - Препознавање претњи и реаговање на њих.
    - Ангажовање надлежних органа у случају потребе.

Континуирана обука: Кључне области - укључују:

- **Рад са тајним подацима:** Разумевање безбедносних процедура.
- **Информациону културу и свест:** Праксе заштите информација и управљања ризицима.
- **Организациону безбедност:** Развој заједничких вредности и стандарда.
- **Сајбер хигијену:** Одржавање дигиталне безбедности кроз превенцију и заштиту система.

Значај и циљеви - доприносе заштити кључних вредности:

- **Националне безбедности.**
- **Одбране и унутрашњих послова.**
- **Људских слобода и права.**
- **Поверљивости информација и података.**

За едукације, обуке и тренинге у вези са применом Закона о тајности података надлежна је Канцеларија Савета за националну безбедност и заштиту тајних података.

Технолошка подршка - Употреба савремених технолошких алата као што су:

- **Енкрипциони софтвери**
- **Системи за праћење**

Ови алати омогућавају прецизнију идентификацију претњи. Усклађеност са међународним стандардима као што је **ISO/IEC 27001** доприноси успостављању најбољих пракси у примене мера информационе безбедности тајних података.

Самопроцена по Закону о инспекцијском надзору - Обухвата:

- **Редовно праћење процедура**
- **Идентификацију неправилности**
- **Корекцију ако је потребно**

Инспекцијски и стручни надзор - спроводе:

- **Министарство правде** – инспекцијски надзор.
- **Канцеларија Савета за националну безбедност и заштиту тајних података (КСНБиЗТП)** – стручни надзор који укључује:
    - Контролу рада са тајним подацима.
    - Унутрашњу контролу у складу са стандардима.

Примена у пракси:

Пример 1: Чување и обрада тајних података ("Строго поверљиво") Орган јавне власти који ради са документима у папирној форми открио је недостатке у примени мера физичке безбедности. **Мере корекције:**

- Инсталација видео-надзора.
- Ограничење приступа само овлашћеним лицима.
- Замена сефа вишим нивоом заштите.

Пример 2: Дигитална размена уз стране стандарде Органи јавне власти приликом спровођења мера информационе безбедности користе платформе са неактуелним протоколима. **Мере корекције:**

- Прелазак на платформе усклађене са најновијим међународним стандардима (нпр. ENISA препоруке).
- Обука службеника за правилно коришћење дигиталних алата.
- Континуирано праћење ефикасности система.
- Сарадња са међународним експертима за информациону безбедност.

Закључак

Процена претње за безбедност тајног податка или самопроцена није само идентификација неправилности, већ и континуиран процес унапређења. Комбинација редовне процене, обуке, технолошких решења, унутрашње контроле и надзора осигурава највиши ниво заштите.

ЛИСТА ЗА ПРОЦЕНУ БЕЗБЕДНОСТИ ОРГАНА ЈАВНЕ ВЛАСТИ ЗА РАД СА ТАЈНИМ ПОДАЦИМА (САМОПРОЦЕНА)

Ова листа служи за процену безбедносних капацитета органа јавне власти у складу са прописима о заштити тајних података и инспекцијском надзору (самопроцена). Процена се врши кроз поенско и описно оцењивање, како би се добио јасан увид у стање безбедности и области које је потребно унапредити и сачињава је сам орган јавне власти, као интрумент за имплементацију Закона о тајности података.

Континуирано праћење и побољшање безбедносних мера је кључно за усклађеност са прописима и смањење ризика од компромитације података.

Овај модел омогућава брзу процену и идентификацију слабих тачака у систему безбедности. Систематско оцењивање заштите тајних података је кључно за безбедност. Применом ових критеријума и методологије оцењивања, могуће је одредити ниво усклађености и предузети мере за унапређење.

1. Организациона безбедност и законска усклађеност

- Да ли је донет интерни акт о заштити тајних података?
- Да ли је именовано лице за безбедност тајних података?
- Да ли је успостављен систем интерне контроле у раду са тајним подацима?
- Да ли су запослени упознати са процедурама руковања тајним подацима?
- Да ли постоји план за поступање у ванредним ситуацијама које могу угрозити тајне податке?

2. Персонална безбедност

- Да ли сви запослени који приступају тајним подацима поседују одговарајуће безбедносне сертификате?
- Да ли се врши редовна провера безбедносне подобности запослених?
- Да ли постоје процедуре за пријаву безбедносних ризика код запослених (нпр. компромитовани контакти, финансијски проблеми)?
- Да ли постоји програм едукације и подизања свести о заштити тајних података?

3. Физичка безбедност

- Да ли објекат у коме се обрађују тајни подаци има одговарајуће безбедносне зоне?
- Да ли је периметар објекта физички обезбеђен (ограде, камере, контролисани улаз)?
- Да ли постоји систем контроле приступа просторијама у којима се чувају тајни подаци?
- Да ли се примењују процедуре заштите од пожара, поплава и других природних опасности?
- Да ли постоји безбедносни систем за откривање неовлашћеног приступа (аларми, сензори)?

4. Информациона безбедност

- Да ли ИКТ инфраструктура има одговарајућу акредитацију од стране Министарства одбране и Канцеларије Савета за националну безбедност и заштиту тајних података?
- Да ли је имплементиран стандард ISO/IEC 27001 у складу са прописима?
- Да ли постоји систем за управљање приступом ИТ системима који садрже тајне податке?
- Да ли се врши редовна анализа рањивости и тестирање безбедносних мера?
- Да ли постоји механизам за праћење и евидентирање приступа тајним подацима у дигиталном облику?
- Да ли постоји процедура за управљање инцидентима у области информационе безбедности?
-

5. Административна безбедност

- Да ли је успостављен функционалан руковалац тајних података?
- Да ли је успостављен систем унутрашње контроле над руковањем тајним подацима?
- Да ли постоје процедуре за означавање, чување и дистрибуцију тајних података?
- Да ли се примењују мере заштите приликом архивирања и уништавања тајних докумената?

6. Безбедност комуникација

- Да ли се користе одобрени криптографски системи за комуникацију тајних података?

- Да ли су комуникациони канали заштићени од прислушкивања и неовлашћеног приступа?
- Да ли постоји политика управљања мобилним уређајима и преносним медијима који могу садржати тајне податке?
- Да ли постоји систем заштите од електронског надзора и прислушкивања?

7. Управљање безбедносним инцидентима

- Да ли постоји процедура за пријаву, анализу и решавање безбедносних инцидената?
- Да ли су запослени обучени да препознају и пријаве безбедносне инциденте?
- Да ли постоји план континуитета пословања у случају безбедносног инцидента?
- Да ли су предузете мере заштите од инсајдерских претњи?

8. Индустријска безбедност

- Да ли се поверљиве набавке са физичким и правним лицима врше на основу посебних безбедносних процедура?
- Да ли се проверава безбедносна подобност привредних субјеката са којима се склапају уговори?
- Да ли постоји систем заштите тајних података у процесу јавних набавки?

УПУТСТВО ЗА ПРОЦЕНУ

Методологија оцењивања:

1. **Поенска оцена** (1-5)

   1 - Нема имплементације
   2 - Делимично имплементирано
   3 - Основни ниво имплементације
   4 - Добра имплементација
   5 - Потпуна имплементација

2. **Описна оцена**

   - Кратак опис тренутног стања
   - Кључни изазови и проблеми
   - Препоруке за унапређење

Основни критеријуми

- **Правилност означавања тајних података**: Проверити да ли је ниво тајности правилно одређен у складу са Законом о тајности података.
- **Мере физичке заштите**: Оцењује се да ли су обезбеђени одговарајући услови за складиштење и руковање тајним подацима.
- **Контрола приступа**: Испитује се да ли је ограничен приступ само овлашћеним лицима.
- **Обука запослених**: Процена нивоа обучености особља које рукује тајним подацима.
- **Поступање у случају инцидента**: Ефикасност мера за одговор на компромитацију података.

Описне препоруке за унапређење

На основу извршеног оцењивања, препоручују се следеће мере за побољшање заштите тајних података:

1. **Унапређење означавања тајних података**
   - Осигурати да се ознаке тајности доследно примењују на сва документа у складу са Законом о тајности података.
   - Спровести редовну контролу правилности означавања и ускладити недостајуће ознаке.
2. **Јачање физичке заштите**
   - Побољшати складиштење тајних података применом савремених безбедносних ормара и просторија са контролисаним приступом.
   - Инсталирати додатне системе надзора и алармне системе у складу са ризицима.
3. **Строжа контрола приступа**
   - Применити принцип „минималних овлашћења“ како би се приступ тајним подацима ограничио само на лица којима је то неопходно.
   - Ревидирати и ажурирати листу овлашћених лица и редовно вршити проверу безбедносних сертификата.
4. **Побољшање обуке запослених**
   - Организовати обавезне обуке за све запослене који рукују тајним подацима, са посебним нагласком на поступање у ванредним ситуацијама.

- Развити приручнике и материјале који ће бити доступни запосленима за брзу референцу.

5. **Јачање процедура у случају инцидента**

   - Успоставити јасне и документоване процедуре за поступање у случају компромитације тајних података.
   - Спроводити редовне симулације безбедносних инцидената ради провере спремности запослених и система.
6. **Редовна ревизија и унапређење безбедносних мера**

   - Успоставити механизам за периодично оцењивање безбедносних мера и усклађивање са најбољим праксама.
   - Спроводити независне безбедносне провере како би се утврдиле слабости и благовремено исправиле.

Финална оцена:

- **80-100% - Висок ниво безбедности** (систем у потпуности усклађен са прописима, мала потреба за унапређењем)
- **60-79% - Средњи ниво безбедности** (испуњени кључни захтеви, али постоје области које треба унапредити)
- **40-59% - Низак ниво безбедности** (значајни недостаци, неопходно унапређење у више области)
- **0-39% - Критичан ниво безбедности** (хитно предузимање мера за усклађеност са прописима)

Ова методологија омогућава брзу и објективну процену безбедносних капацитета органа јавне власти, идентификацију слабих тачака и предузимање мера за побољшање.

ФИНАЛНА ОЦЕНА – ПОЕНСКА СКАЛА

Укупан број питања: **40**
Минималан могући број поена: **40** (ако се свуда добије 1)
Максималан могући број поена: **200** (ако се свуда добије 5)

Проценат усклађености	Поенски опсег	Ниво безбедности
80-100%	**160 – 200 поена**	Висок ниво безбедности (систем у потпуности усклађен, мала потреба за унапређењем)
60-79%	**120 – 159 поена**	Средњи ниво безбедности (испуњени кључни захтеви, али постоје области које треба унапредити)
40-59%	**80 – 119 поена**	Низак ниво безбедности (значајни недостаци, неопходно унапређење у више области)
0-39%	**40 – 79 поена**	Критичан ниво безбедности (хитно предузимање мера за усклађеност са прописима)

Примери оцењивања

Ови примери показују како се оцењује ниво безбедности институције и које мере је неопходно предузети за унапређење заштите тајних података.

Пример 1 – Висока оцена (5)

Организација је у потпуности применила све мере заштите, укључујући:

- Коректно означавање тајних података.
- Прецизно дефинисане процедуре за руковање подацима.
- Савремене системе физичке заштите (собе са контролисаним приступом, противпровалне ормаре).
- Редовну обуку запослених.
- Брзо и ефикасно поступање у случају безбедносног инцидента.

Пример 2 – Средња оцена (3)

Организација је успоставила основне мере заштите, али има следеће недостатке:

- Ознаке тајности нису увек доследно примењене.
- Нису спроведене све препоручене мере физичке заштите.
- Доступ запосленима није увек ограничен у складу са прописима.
- Обуке нису редовне.

Пример 3 – Ниска оцена (1-2)

Организација има озбиљне недостатке у заштити тајних података:

- Ознаке тајности су често нетачне или их нема.
- Подаци су сачувани у неадекватним условима.
- Приступ није ограничен овлашћеним лицима.

- Недостатак обуке и процедура за реаговање у случају инцидента.

Пример оцењивања са препорукама

Пример 1 – Средњи ниво безбедности (145 поена / 72,5% усклађености)

Оцена: Институција је постигла 145 од могућих 200 поена, што значи да је ниво усклађености 72,5%. Ово је **средњи ниво безбедности**, што указује на постојање одређених недостатака који могу утицати на заштиту тајних података.

Кључне слабости:

- Ознаке тајности нису увек доследно примењене (чести пропусти у означавању појединих докумената).
- Физичка заштита није на оптималном нивоу (неки документи се чувају у неодговарајућим условима).
- Контрола приступа није у потпуности у складу са прописима (појединi запослени имају шири приступ него што је неопходно).
- Обуке запослених се одржавају повремено, али нису систематизоване.
- Недостатак формализованих процедура за реаговање у случају безбедносног инцидента.

Препоруке за унапређење:

1. **Побољшати означавање тајних података** кроз увођење интерне контроле означавања и спровођење обуке о правилном означавању докумената.
2. **Ојачати физичку заштиту** набавком одговарајућих противпровалних ормара и увођењем додатних безбедносних мера за складиштење тајних података.
3. **Ограничити приступ тајним подацима** само на лица којима је приступ неопходан за обављање посла и редовно ажурирати листе овлашћених лица.
4. **Усвојити формализовани програм обуке**, који ће се одржавати најмање два пута годишње са практичним вежбама и тестирањем запослених.
5. **Развити и имплементирати процедуре за реаговање у случају безбедносног инцидента**, укључујући симулације могућих сценарија како би запослени били боље припремљени.

Пример 2 – Низак ниво безбедности (85 поена / 42,5% усклађености)

Оцена: Институција је освојила 85 од могућих 200 поена, што значи да је ниво усклађености **42,5%**. Ово указује на **низак ниво безбедности**, што значи да постоје значајни недостаци који могу довести до компромитације тајних података.

Кључне слабости:

- Већина докумената није адекватно означена тајношћу, што ствара ризик од неовлашћеног приступа.
- Подаци се чувају у неадекватним просторима без одговарајуће физичке заштите.
- Не постоји системска контрола приступа тајним подацима – запослени без одговарајућих овлашћења могу доћи у контакт са поверљивим информацијама.
- Обуке запослених нису организоване, а свест о важности безбедности података је на ниском нивоу.
- Не постоје процедуре за поступање у случају инцидента, нити је икада спроведена симулација безбедносног инцидента.

Препоруке за унапређење:

1. **Хитно увести правилно означавање тајних података** у складу са законом и успоставити механизам контроле исправности означавања.
2. **Обезбедити адекватно складиштење тајних података**, укључујући набавку безбедносних ормара и забрану чувања података у неадекватним условима.
3. **Успоставити строг систем контроле приступа**, укључујући издавање приступних дозвола само овлашћеним лицима и редовну ревизију листе корисника.
4. **Организовати интензивне обуке за запослене**, са посебним нагласком на основне принципе заштите тајних података и последице пропуста.
5. **Развити и применити јасне процедуре за поступање у случају безбедносног инцидента**, уз обавезно спровођење тестирања и симулација кроз практичне вежбе.
6. **Редовно спроводити независне безбедносне ревизије** како би се идентификовале критичне слабости и предузеле корективне мере.

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.

ЗДРАВСТВЕНО-МЕДИЦИНСКИ АСПЕКТ БЕЗБЕДНОСНИХ ПРОВЕРА

Здравствено-медицинска процена у оквиру безбедносних провера има за циљ утврђивање да ли лице поседује психофизичке способности неопходне за

приступ, руковање и заштиту тајних података. Поступак мора бити у складу са стандардима националне безбедности, националним законодавством, али и уставним правима појединца.

Кључне области процене

1. **Когнитивне способности** - Испитује се способност логичког мишљења, памћења, концентрације и процене ситуације. Присуство неуролошких или органских оштећења мозга, деменције или озбиљних неуролошких обољења може бити препрека за издавање безбедносног сертификата.

3. **Психичка стабилност** - Особе са тешким психијатријским дијагнозама као што су шизофренија, тешки облици биполарног поремећаја са психотичним епизодама или поремећаји личности који доводе у питање расуђивање и поузданост, могу се сматрати непоузданим за руковање поверљивим подацима.

4. **Зависности** - Активне зависности од алкохола, наркотика или других психоактивних супстанци се сматрају озбиљним ризиком. Таква стања директно утичу на способност расуђивања, самоконтроле и одговорности.

5. **Поремећаји пажње и импулсивности** - Тешки облици поремећаја пажње и хиперактивности (ADHD), уколико значајно утичу на понашање и контролу импулса, могу довести до ограничења или одлагања у процесу издавања сертификата.

Процедура

- **Анализа здравствене документације**: Органи надлежни за вршење безбедносне провере могу захтевати медицинске извештаје, уверења о здравственом стању или мишљење надлежног психијатра или неуролога.
- **Психолошка и психијатријска процена**: Уколико постоји сумња или индикација на ментално здравствене потешкоће, лице се обавезно упућује на детаљну процену или вештачење.
- **Медицинско вештачење**: У сложенијим случајевима спроводи се вештачење од стране комисије, уз примену стручних стандарда и етичких начела.

Правна основа за обраду здравствених података - Обрада здравствених података у оквиру безбедносне провере врши се искључиво **уз писану сагласност лица – кандидата за издавање безбедносног сертификата.** Ови подаци се прикупљају, обрађују и чувају у строгој законској процедури, у складу са националним и европским прописима који штите приватност и људска права.

Правни основ за ову обраду обухвата:

- Закон о тајности података („Службени гласник РС”, бр. 104/2009),
- Уредба о обрасцима безбедносних упитника („Службени гласник РС”, бр. 30/2010),
- Закон о заштити података о личности („Службени гласник РС”, бр. 87/2018),
- Општу уредбу о заштити података – General Data Protection Regulation (GDPR), Регулатива (ЕУ) 2016/679 Европског парламента и Савета од 27. априла 2016. године.

У складу са наведеним прописима:

- **Обрада осетљивих података о здрављу могућа је само на основу изричитог пристанка лица:** Обрада података о здрављу у контексту безбедносних провера може се вршити искључиво уз слободно, информисано и недвосмислено пристајање лица, у складу са Законом о заштити података о личности и Општом уредбом о заштити података (GDPR). Без таквог пристанка, обрада није дозвољена, осим ако није другачије прописано законом.

- **Сврха обраде мора бити јасно дефинисана и ограничена на безбедносну процену:** Податке о здрављу је дозвољено обрађивати искључиво у унапред одређену сврху безбедносне процене – односно процене психофизичке способности лица за приступ тајним подацима, у складу са посебним прописима и принципом минимализације података.

- **Подаци се користе искључиво од стране овлашћених органа, у строго контролисаним условима:** Приступ осетљивим подацима имају само надлежни органи који су изричито овлашћени за њихову обраду, и то у оквиру строго дефинисаних процедура и мера заштите, што укључује техничке, организационе и кадровске мере безбедности.

- **Лице има право на информације, увид, исправку, ограничење обраде и друга права гарантована законом и GDPR-ом**: Свако лице има право:

- да буде обавештено о томе да се његови подаци обрађују и у коју сврху, о да затражи приступ својим подацима,
- да тражи исправку нетачних или непотпуних података,
- да затражи ограничење обраде у одређеним случајевима,
- као и да уложи приговор или жалбу надлежном органу.

Право на брисање („право на заборављеност") такође припада лицу, уколико су испуњени услови из члана 17. GDPR-а – на пример ако подаци више нису неопходни за сврху због које су прикупљени, ако лице повуче сагласност, или ако су подаци обрађени незаконито. Ипак, ово право може бити ограничено ако постоји легитиман правни основ за задржавање података, као што је обавеза чувања ради заштите националне безбедности или других јавних интереса, у складу са законом.

Резултати безбедносне процене:

Апсолутне сметње: Уколико се проценом утврди да лице није психофизички способно за руковање тајним подацима, издавање безбедносног сертификата се одбија. Ова одлука подразумева постојање трајних и неспојивих околности са приступом тајним подацима. Апсолутне сметње подразумевају трајна или тешка здравствена стања која представљају неспојивост са обављањем послова који укључују приступ тајним подацима. Таква стања обично укључују: – **шизофренију (F20)** и сродне психотичне поремећаје, – **биполарни афективни поремећај (F31)** са нестабилним током и честим епизодама, – **органске менталне поремећаје (F00–F09),** укључујући све форме **деменције, – епилепсију са честим губитком свести или тешким нападима (G40),** – **антисоцијални, параноидни или тешки гранични поремећај личности (F60)**, – **активну зависност од психоактивних супстанци (F10–F19)** или нестабилну ремисију, – **тешке когнитивне дефиците или менталну ретардацију (F70–F73).**

Релативне сметње: Уколико постоје пролазне или контролисане околности – као што је здравствено стање које је под терапијом и редовним надзором – могу се предузети мере као што су: – одлагање одлучивања, – додатна медицинска вештачења, – поновна процена здравственог стања након одређеног времена. Релативне сметње могу укључивати: – **депресију (F32–F33)** под контролом, – **анксиозне поремећаје (F40–F41)** без поремећаја у понашању, – **контролисану епилепсију**, са уредним ЕЕГ налазима и редовном терапијом, – **блажи неуротични поремећаји**, без утицаја на расуђивање и стабилност понашања.

Препоруке за формулисање стручног мишљења (вештачења) - Стручна лица, најчешће специјалисти психијатрије или неуропсихијатрије, ангажована у поступку безбедносне провере, обавезно сачињавају **писмено стручнопсихијатријско вештачење**, које представља један од кључних доказа у доношењу одлуке о подобности лица за приступ тајним подацима. Без таквог вештачења, није дозвољено доношење негативног решења (одбијање безбедносног сертификата).

Вештачење мора да садржи следеће елементе:

1. **Дефинисана дијагноза** - Наводи се прецизна дијагноза у складу са важећом међународном класификацијом болести (ICD-10 или ICD-11), са шифром и описом стања.
2. **Процена клиничке стабилности** - Стручњак треба да наведе да ли је стање стабилно, под терапијом, у ремисији или са честим рецидивима. Формулација може бити, на пример: „Стање под стабилном терапијом, без рецидива у последњих 12 месеци. Контролни прегледи редовни, без знакова дезорганизованог понашања.“
3. **Процена капацитета за руковање тајним подацима** - Оцена психичке и когнитивне способност лица да разуме, чува и правилно поступа са поверљивим садржајима, уз процену: – нивоа пажње и концентрације, – критичности у размишљању, – могућности предвиђања последица својих поступака, – стабилности афекта и самоконтроле.
4. **Препорука о сметњи** - Стручњак у вештачењу мора недвосмислено навести да ли се ради о: – апсолутној сметњи (стање је неспојиво са обављањем послова од значаја за безбедност и тајне податке), или – релативној сметњи (стање је под контролом и не представља трајну препреку). У случају релативне сметње, треба дати: – јасан интервал за поновну процену (нпр. „препоручује се поновно вештачење за 12 месеци“), – услове под којима се може размотрити позитивна оцена (нпр. „уз наставак редовне терапије и психијатријског праћења“).
5. **Потпис и печат** - Вештачење мора бити потписано од стране овлашћеног стручњака, уз назив здравствене установе и датум.

Проблеми у вези са стручним мишљењем и применом Закона о здравственој заштити - У поступку безбедносне провере често се захтева стручно мишљење о психофизичкој способности лица за руковање тајним подацима. Међутим, поједине законске одредбе ограничавају могућност укључивања конкретних дијагноза у документацију која се доставља органима ван система здравствене заштите. Према члановима 45. и 46. Закона о здравственој заштити, здравствени

радници не смеју у извештаје који се користе изван здравственог система уносити дијагнозу и шифру болести, осим уколико лице на то није дало писмену информисану сагласност. Ова забрана има за циљ заштиту приватности и медицинских података лица, али у исто време представља изазов у поступцима који захтевају процену психофизичке способности као што је безбедносна провера.

Уколико лице да писмену сагласност, стручно мишљење може садржати дијагнозу и шифру болести према важећој класификацији болести (нпр. F32.1 – умерени депресивни поремећај). У оваквим случајевима мишљење лекара може директно указати да ли се ради о апсолутној или релативној сметњи за безбедносни сертификат, уз предлог интервала за поновну процену. Уколико сагласност није дата, лекар не сме наводити дијагнозу или шифру болести, већ се уместо тога израђује описно стручно мишљење. То мишљење садржи процену стабилности здравственог стања и његовог утицаја на способност лица за одговорно руковање тајним подацима. Пример формулације која се у пракси користи гласи: „Здравствено стање је стабилно, под редовним надзором. Нема елемената који би у овом тренутку представљали ризик по безбедност у погледу руковања тајним подацима.“

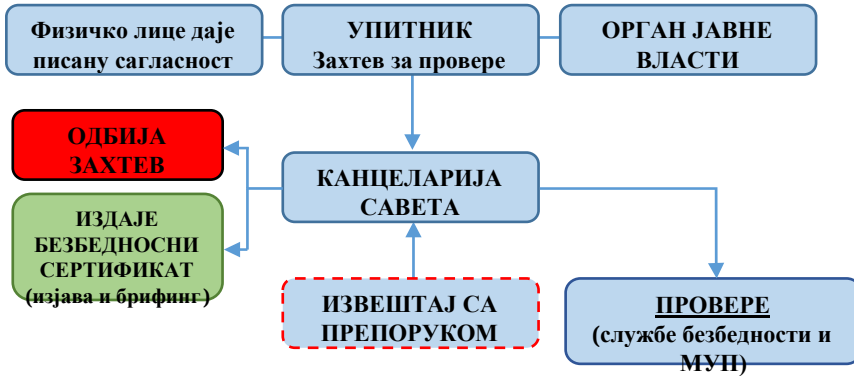
У сваком случају, неопходно је да постоји уредно вештачење као основ за доношење негативне или позитивне процене, јер се без мишљења стручњака не може утврдити да ли постоје апсолутне или релативне сметње. Поступање мора бити усклађено како са прописима о безбедносној провери, тако и са Законом о здравственој заштити, водећи рачуна о заштити осетљивих података лица које је предмет провере.

Правни и етички оквир - Поступак безбедносне провере мора бити спроведен у складу са важећим правним прописима и етичким принципима, уз поштовање људских права и основних слобода лица које је предмет провере. Посебно је важно поштовање начела пропорционалности, односно да се мере и ограничења предузимају само у мери у којој су неопходна ради заштите безбедносних интереса. Право на приватност, укључујући и заштиту личних и здравствених података, мора бити обезбеђено током целокупног поступка. Уколико у поступку буде донета негативна одлука, лице има право на увид у релевантну документацију и на подношење жалбе надлежном органу, у складу са Законом о општем управном поступку. Жалба се подноси Министарству правде, које врши контролу над спровођењем поступка и законитошћу донете одлуке.

Спровођење поступка у складу са правним и етичким оквиром представља предуслов за очување легитимности безбедносне провере и поверења у институције које је спроводе.

Област процене	Опис	Могући утицај на безбедносни сертификат
Когнитивне способности	Памћење, логичко расуђивање, концентрација, способност процене и доношења одлука.	Апсолутна сметња у случају присуства тешких неуролошких поремећаја који онемогућавају поуздано руковање тајним подацима.
Психичка стабилност	Присуство поремећаја као што су шизофренија, биполарни афективни поремећај, тешки облици поремећаја личности.	Може довести до одбијања издавања сертификата или до привременог одлагања ради додатне процене и лечења.
Зависности	Употреба или злоупотреба алкохола, дрога и других психоактивних супстанци.	Углавном представља апсолутну сметњу, осим у случајевима стабилне апстиненције потврђене од стране стручних служби.
Контрола импулса / ADHD	Симптоми као што су импулсивност, хиперактивност, поремећај пажње, неадекватно социјално понашање.	Релативна сметња; утицај се процењује у складу са тежином стања, стабилношћу и терапијским одговором.
Процедура процене	Увид у здравствену документацију, интервју са психијатром/психологом, психолошко тестирање, евентуално додатно вештачење.	Обавезна је код свих кандидата за које постоје медицинске индикације или на основу безбедносног упитника.
Правна основа	Обрада података о здрављу се врши уз изричит пристанак лица и у складу са релевантним прописима.	Закон о заштити података о личности (Сл. гласник РС, бр. 87/2018); Закон о тајности података (Сл. гласник РС, бр. 104/2009); Уредба о безбедносном упитнику (Сл. гласник РС, бр. 76/2010, 103/2013); Општа уредба о заштити података – GDPR.
Права лица	Лице има право на приступ информацијама, увид, исправку, ограничење обраде, жалбу и, у одређеним случајевима, брисање података.	Права се остварују у складу са Законом о заштити података о личности и GDPR-ом, укључујући право на правну заштиту и надзор Повереника.

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.
13. Министарство информисања и телекомуникација, Париска 7, 11000 Београд,
14. Институт за политичке студије, Добриньска 11, 11000 Београд,
15. Републички геодетски завод, Булевар војводе Мишића 39, 11040 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 SRPS/EN техничке стандарде.

Зонирање и акредитација простора у складу са прописима о тајности података

Зонирање и акредитација простора представљају део унутрашњег система мера заштите тајних података, дефинисаних **Законом о тајности података** („Службени гласник РС“, бр. 104/2009), подзаконским актима које доноси Влада, као и **упутствима Канцеларије Савета за националну безбедност и заштиту тајних података у складу са одредбама члана 87. Закона о тајности података**. Посебно важан подзаконски акт у овом домену је **Уредба о посебним мерама физичко-техничке заштите тајних података** („Службени гласник РС“, бр.

89/2013). Циљ зонирања и акредитације, који се спроводи преко стручног надзора је обезбеђивање физичке и техничке заштите тајних података у складу са њиховим степеном тајности, применом одговарајућих мера и процедура.

1. Зонирање простора

Простори у којима се чувају, обрађују и преносе тајни подаци разврставају се у три врсте зона:

1.1. Административна зона

Административна зона је намењена за **обраду и чување тајних података степена тајности „Интерно“**.

Карактеристике административне зоне:

- Одређује се простор или просторија која се може **надзирати**, укључујући улаз, излаз и кретање лица и возила;
- На улазу у зону мора бити **истакнуто обавештење о надзору приступа и кретању**;
- Примењују се основне мере физичко-техничке заштите, као што су **евиденција приступа**, **контролисан улаз**, и мере спречавања неовлашћеног копирања, снимања или изношења докумената;
- Простор мора бити обезбеђен од неовлашћеног уласка и мора омогућити контролу присуства запослених и посетилаца.

1.2. Безбедносна зона II степена

Ова зона обухвата **просторе у којима се обрађују и чувају тајни подаци степена тајности „Поверљиво“, „Строго поверљиво“ и „Државна тајна“**, али **без непосредне обраде** – најчешће се односи на архиве, складишта или просторије у којима се документи само чувају.

Специфичне мере у овој зони:

1. **Надзор и евиденција улаза и излаза** – потпуна контрола кретања;
2. **Ограничен приступ** – запослени имају приступ само подацима потребним за рад и до нивоа за који имају сертификат;
3. **Пратња лица** – лица са дозволом за приступ могу у зону само у пратњи овлашћеног запосленог;
4. **Забрана уношења опреме** – механички, електронски и магнетно-оптички уређаји се уносе само уз одобрење овлашћеног лица;

5. **Физичко и противпровално обезбеђење**, као и **повремени прегледи просторија** по завршетку радног времена.

1.3. Безбедносна зона I степена

Ово је највиши ниво безбедносне зоне. У овој зони се тајни подаци **највиших степена („Поверљиво“, „Строго поверљиво“, „Државна тајна“) непосредно обрађују** – кроз рад на документима, унос у информационе системе, штампање, уништавање и пренос.

Мере које се примењују укључују:

- **Строгу контролу приступа**, биометрију или двофакторску идентификацију;
- **Видео-надзор** и **24-часовно физичко обезбеђење**;
- **TEMPEST заштиту** (заштита од електромагнетног одашиљања);
- **Заштиту ИТ система**, приступа базама података и електронској комуникацији;
- **Системе детекције упада**, аларме и контролу периметра.

2. Стручни надзор - Акредитација простора

Стручни надзор, односно акредитација је формални поступак утврђивања да одређени простор испуњава прописане услове за чување и обраду тајних података.

Поступак обухвата:

- **Израда интерне процене ризика, као и Плана заштите тајних података (процедура** и мера заштите), у складу са упутствима Канцеларије;
- **Техничка провера и стручни надзор простора** од стране Канцеларије;
- Издавање **потврде о акредитацији**, која важи за конкретан простор, врсту активности и степен тајности.

3. Самопроцена и стручни и инспекцијски надзор

Орган државне управе или други субјект који поступа са тајним подацима обавезан је да:

- редовно врши **самопроцену примене мера безбедности**;
- одржава **евиденције о приступу и кретању у зонама**;
- припрема **план рада са тајним подацима, процене ризика и мере унапређења**;
- омогући и организује **стручни надзор и акредитацију простора и процедура,** који спроводи Канцеларија Савета (ради се по захтеву органа јавне власти)
- **омогући инспекцијски надзор**, који спроводи надлежно министарство.

4. Инспекцијски надзор

Надзор над применом закона и уредбе спроводи **Министарство правде**, које:

- контролише усклађеност простора и мера са издатом акредитацијом;
- прегледа документацију и техничку опрему;
- у случају пропуста, изриче **мере отклањања неправилности** и може суспендовати приступ или акредитацију.

5. Завршна напомена

Сви субјекти који обрађују или чувају тајне податке дужни су да:

- обезбеде просторе у складу са прописаним зонама;
- прибаве акредитацију од надлежног органа;
- континуирано спроводе мере заштите и пријављују сваку промену у организацији или техничким условима.

6. Основни циљеви зонирања и акредитације

- ✓ Очување поверљивости, интегритета и доступности тајних података
- ✓ Увођење зона контролисаног приступа и физичко-техничких баријера
- ✓ Усклађеност са домаћим и међународним стандардима
- ✓ Смањење ризика од неовлашћеног приступа или компромитације
- ✓ Повећање одговорности и транспарентности унутар органа јавне власти

Преглед зона и мера заштите тајних података

Зона	Степен тајности података	Намена простора	Кључне мере заштите
Административна зона	„ИНТЕРНО“	Обрада и чување података нижег степена	- Надзор улаза, излаза и кретања лица/возила - Обавештење о надзору на улазу - Евиденција приступа - Забрана неовлашћеног уношења и изношења података
Безбедносна зона II степена	„ПОВЕРЉИВО“, „СТРОГО ПОВЕРЉИВО“, „ДРЖАВНА ТАЈНА“	Чување података (нпр. архиве, складишта)	- Потпуна контрола улаза и излаза - Приступ само уз сертификат и по принципу потребности - Улаз других лица само уз пратњу - Забрана уношења електронских уређаја без дозволе - Противпровално обезбеђење и прегледи простора
Безбедносна зона I степена	„ПОВЕРЉИВО“, „СТРОГО ПОВЕРЉИВО“, „ДРЖАВНА ТАЈНА“	Непосредна обрада података (канцеларије, сервер-собе)	- Строга контрола приступа (биометрија, картице) - Видео-надзор и физичко обезбеђење 24/7 - TEMPEST заштита - Системи заштите ИТ инфраструктуре - Аларми, контрола периметра, двострука заштита

Радне тачке за рад са тајним подацима
– препоруке за поступање у прелазном периоду –

До потпуне имплементације Закона о тајности података и свих организационих и безбедносних мера, органи јавне власти који у свом раду поступају са тајним подацима могу формирати приступне радне тачке за рад са тајним подацима, као облик интерне организације органа јавне власти који још увек нису у могућности да обезбеде потпуно испуњавање услова за рад у регистарском систему и иплементације Закона о тајности података.

Појам радне тачке за рад са тајним подацима

Радна тачка за рад са тајним подацима представља функционални одређени део радног простора унутароргана јавне власти који је посебно организован ради пријема, обраде, приступа и чувања тајних података у органу јавне власти.
Радна тачка не представља званично успостављену административну, односно безбедносну зону, већ служи као привремено решење за рад са тајним подацима у контролисаним и безбедним условима, до успостављања зона у складу са Уредбом о посебним мерама физичко-техничке заштите тајних података.

Циљеви успостављања радне тачке

На првом месту, краткорочни циљ успостављања радне тачке је да се омогући рад са тајним подацима у условима организације рада и размештаја органа јавне власти када пуна имплементација Закона о тајности података није технички, организационо и/или финансијски изводљива, али без умањивања нивоа безбедности тајних података у односу на одређени степен тајности.
Дугорочни циљ се огледа у успостављању административних и безбедносних зона према Уредби о посебним мерама физичко-техничке заштите тајних података и пуној имплементацији прописа о раду са тајним подацима у органима јавне власти.

Основни услови за успостављање радне тачке за рад са тајним подацима

Да би се успоставила радна тачка, потребно је приликом формирања испунити минимум техничко-организационих услова, који не смеју бити нижи од основних услова за заштиту тајних података који су прописани Уредбом о посебним мерама физичко-техничке заштите тајних података:

- Морају бити спроведене активности из дела административне безбедности:
  - Израђена Процена ризика и угрожености тајних података,
  - Донета одлука о одређивању тајних података у органу јавне власти,
  - Израђен Каталог тајних података,
  - Донета одлука о одређивању овлашћених лица за креирање тајних података,

- Донета одлука о одређивању Руковаоца тајних података
- Установљена Листа овлашћених лица за приступ тајним подацима у органу јавне власти,
- Донет План заштите тајних података у органу јавне власти,
- Донет План заштите тајних података у ванредним и хитним случајевима, односно случајевима нарушавања безбедности,

- Радна тачка мора бити у физички затвореном и обезбеђеном простору, са закључавањем и ограниченим приступом који је дозвољен само овлашћеним лицима;
- На улазу у простор радне тачке, поставља се обавештење о забрани неовлашћеног
  уласка и режиму рада са тајним подацима;
- Успоставља се систем евидентирања о приступу простору, у електронском облику (аутоматски или ручно) или физички кроз вођење евиденције у папирном облику;
- Приступ и рад са тајним подацима се дозвољава искључиво лицима која су овлашћена према Листи овлашћених лица за приступ тајним подацима у органу јавне власти и која поседују одговарајући безбедносни сертификат за приступ тајним подацима;
- Успоставља се систем контроле и забране уношења техничке опреме и електронских уређаја (мобилни телефони и сатови, преносни рачунари, оптоелектронска средства, меморијски уређаји и сл.);
- Успоставља се систем евидентирања приступа тајним подацима;
- Тајни подаци се одмах након завршетка рада са њима депонују назад у сигурносне сефове и/или акредитоване просторе;

Успоставља се систем контроле коришћења радне тачке, на начин да је дозвољен рад само у току радног времена, док се у ванрадно време успоставља систем обилазака и контроле од стране чуварске службе у органу јавне власти.

Обавезе органа јавне власти и унутрашње процедуре

Орган јавне власти који успоставља радну тачку доношењем интерних аката регулише:

- локацију радне тачке, у складу са проценом ризика и циљем умањивања претњи по безбедност тајних података,
- именује одговорна лица за рад радне тачке и контролу и надзор над радом исте,
- врсту тајних података и највиши степен тајности који је могуће обрађивати у радној тачки,
- доноси упутство за рад радне тачке, којим регулише сва поступања у вези са радом са тајним подацима у радној тачки,

- регулише контролу поступања над радом са тајним подацима у радној тачки,
- спроводи поступак индивидуалне процене испуњености услова за заштиту тајних података.

Канцеларија Савета за националну безбедност и заштиту тајних података, до успостављања пуне имплементације прописа за заштиту тајних података у органима јавне власти, може пружити стручну помоћ кроз обезбеђивање стандардизованог упутства о радним тачкама и давање смерница за испуњавање минималних организационих и техничких услова.

* 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.

ПРОЦЕДУРА ЗА ОЗНАЧАВАЊЕ И ОДРЕЂИВАЊЕ СТЕПЕНА ТАЈНОСТИ ПОДАТАКА

Процедура за означавање и одређивање степена тајности података представља кључни корак у заштити осетљивих информација, докумената и података, као и очувању интереса Републике Србије. Ова процедура има за циљ

да обезбеди безбедност података, уз транспарентност и одговорност органа јавне власти. Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја. Поступак означавања и одређивања степена тајности у органима јавне власти у Републици Србији регулисан је Законом о тајности података и подзаконским актима, и обухвата следеће кораке:

1. **Доношење формалне одлуке о тајности:**

Орган јавне власти је у обавези да донесе генеричну или појединачну писмену одлуку о одређивању степена тајности података, уз процену утицаја и потенцијалне штете по интересе Републике Србије у случају откривања, злоупотребе или уништења података. Тајност податка, под условима и на начин утврђен законом о тајности података, одређује овлашћено лице. При одређивању степена тајности податка, овлашћено лице одређује најнижи степен тајности који спречава настанак штете по интересе Републике Србије. Овлашћена лица која имају право да одређују степен тајности података према члану 9. Закона о тајности података су: председник Републике, председник Владе, руководилац органа јавне власти, изабрани, постављени или именовани функционер органа јавне власти који је за одређивање тајних података овлашћен законом, односно прописом донесеним на основу закона, или га је за то писмено овластио руководилац органа јавне власти, као и лице запослено у органу јавне власти које је за то писмено овластио руководилац тог органа.

2. **Идентификација категорија података:**

Подаци се анализирају како би се утврдило да ли испуњавају услове за означавање као тајни, укључујући прописима предвиђене категорије података, као и процену могућег утицаја на националну безбедност, јавни интерес, територијални интегритет и економске интересе. У овом кораку се такође разматра и општи значај података, као и последице које би њихово откривање могло имати на рад органа јавне власти.

3. **Одређивање степена тајности:**

На основу процене, подаци се разврставају или категоришу у један од следећих степена тајности узимајући у обзир озбиљност потенцијалне штете по нарушавање интереса Републике Србије настало као последицу неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последицу друге радње обраде тајних података у складу са уредбама о ближим критеријумима за одређивање степена тајности „државна тајна“, „строго поверљиво“, „поверљиво“ и „интерно“ („Службени гласник Републике Србије“ број 46/2013, 70/2013, 86/2013, 105/2013, 66/2014 и 79/2014):

• **ДРЖАВНА ТАЈНА** - који се одређује ради спречавања настанка неотклоњиве тешке штете по интересе Републике Србије;

• **СТРОГО ПОВЕРЉИВО** - који се одређује ради спречавања настанка тешке штете по интересе Републике Србије;

• **ПОВЕРЉИВО** - који се одређује ради спречавања настанка штете по интересе Републике Србије; или

• **ИНТЕРНО** - који се одређује ради спречавања настанка штете за рад, односно обављање задатака и послова органа јавне власти који их је одредио.

4. **Означавање података:**

Подаци добијају јасну ознаку која укључује степен тајности, начин престанка тајности, податке о овлашћеном лицу, датум означавања, назив органа који је донео одлуку и правну основу. Ознака мора бити видљива и у складу са прописаним стандардима у Уредби о начину и поступку означавања тајности података, односно документа („Службени гласник Републике Србије“ број 8/2001). Документ који садржи тајни податак означава се одговарајућим степеном тајности, изнад назива документа, на врху сваке странице, на средини. Ознака одговарајућег степена тајности на документу исписује се тамнијим словима већег формата од слова текста документа. Ако документ садржи више страница, свака страница се означава редним бројем странице у односу на укупан број страница. Сваки документ мора имати ознаку степена тајности на врху прве стране и спољне стране предњих корица ако оне постоје или на врху насловне стране. Ако документ нема насловну страну, прва страна ће се сматрати као насловна. Приликом означавања документа не сме доћи до уништења или оштећења тајног податка, односно документа на којем се он налази.

5. **Евиденција и контрола:**

Тајни подаци се уписују у регистар и евиденцију тајних података ради праћења и контроле. Евиденција о тајним подацима води се одвојено од осталих евиденција органа јавне власти. Евиденција садржи: редни број, назив органа јавне власти, назив унутрашње организационе јединице органа јавне власти која је одредила степен тајности, садржај предмета, датум пријема предмета, класификациона ознака предмета, податке о уступању документа другом органу, податке о промени степена тајности, начин и датум престанка тајности, податак када је предмет архивиран и напомену. Орган јавне власти је у обавези да обезбеди адекватну административну, физичку и информациону безбедност.

6. **Ревизија и ажурирање:**

Ознаке тајности се периодично преиспитују и ревидирају како би се утврдило да ли је потребно задржати, променити или укинути степен тајности, због

временског ограничења, престанка тајности утврђивањем датума, наступањем одређеног догађаја и истеком рока. Одлука о опозиву тајности податка доноси се ако наступе чињенице и околности услед којих податак престаје да буде од интереса за Републику Србију.

7. **Последице непоштовања процедура:**

Непоштовање прописаних процедура означавања и заштите тајних података може довести до озбиљних последица. Ове последице не обухватају само административне и организационе последице, већ могу бити и озбиљне правне и кривичне природе. У зависности од врсте прекршаја и тежине поступка, могу се применити различите казнене мере, укључујући санкције против органа јавне власти и одговорних лица, као и опасност по безбедност Републике Србије.

Казнене мере: У складу са Законом о тајности података, непоштовање процедура означавања, чувања и обраде тајних података може довести до различитих казнених мера:

Прекршајне санкције се могу изрећи у случају када одговорна лица не испуне обавезе у погледу означавања, чувања или размене тајних података, или ако дође до њиховог неовлашћеног откривања. Прекршаји могу обухватити:

- Неадекватно означавање степена тајности.
- Недовољну заштиту тајних података.
- Неоправдано откривање података без одобрења или одлуке овлашћеног лица.

Кривичне санкције су озбиљније и применљиве су у случају кршења процедура које могу довести до значајне штете по безбедност Републике Србије. Члан 98. Закона о тајности података прописује кривично дело које укључује:

- **Неовлашћено откривање тајних података**: Лице које без овлашћења открије тајне податке или их користи у незаконите сврхе, може бити кривично гоњено.
- **Злоупотреба тајних података**: Лице које злоупотреби тајне податке, било да их дели, продаје или на неки други начин користи против националне безбедности, може бити осуђено на казне затвора.
- **Недопуштена измена или уништавање тајних података**: Лица која униште, измене или на неки начин ометају очување тајних података, као и лица која не предузму прописане мере заштите података, могу бити кривично санкционисана.

У складу са чланом 98. Закона, **кажњавање се може изрећи казном затвора до 5 година**, зависно од природе дела. Утврђивање казне зависи од тога да ли је дошло до озбиљне штете по безбедност Републике Србије, односно да ли је дело довело до нарушавања националне безбедности.

Угрожавање безбедности - Непоштовање процедура означавања и заштите тајних података може директно угрозити националну безбедност, што може довести до:

- **Штете по безбедност Републике Србије**: Откривање, злоупотреба или уништавање тајних података може нанети озбиљну штету одбрани, дипломатским и политичким односима или економским интересима земље.
- **Откривање података од војног или обавештајног значаја**: Ако дође до откривања података који се односе на војне операције, обавештајну активност или стратегије одбране, то може довести до директне претње по сигурност земље и њених грађана.
- **Злоупотреба информација**: Неовлашћени приступ тајним подацима може довести до извоза осетљивих информација и коришћења од стране странака које имају непријатељске намере према Србији.

Губитак поверења - Недостатак адекватне заштите тајних података може довести до значајног губитка поверења у органе јавне власти. Када грађани, правни субјекти или међународни партнери сазнају да се подаци који су од великог значаја за националну безбедност не чувају на адекватан начин, то може:

- **Нарушити углед органа јавне власти**: Откривање пропуста у заштити тајних података може довести до негативних реакција јавности и партнерских земаља, што нарушава кредибилитет власти.
- **Нарушити однос са међународним партнерима**: Недовољна заштита података може довести до кршења међународних споразума, што отежава сарадњу са иностранством.
- **Погоршање унутрашњег поверења**: Институтима и грађанима може бити изгубљено поверење у способност органа јавне власти да адекватно управљају тајним подацима и да гарантују националну безбедност.

Правне импликације - Када дође до кршења процедура означавања и заштите тајних података, могу се покренути и правни поступци против одговорних лица:

- **Судски поступци**: Ако се утврди да је поступак означавања или обраде података био незаконит, могу се покренути цивилни поступци, где се може захтевати одговорност за штету коју су органи јавне власти или њихови запослени нанели.
- **Прекршајни поступци**: Уколико је дошло до прекршаја у смислу неправилног чувања или поступања са тајним подацима, могу се изрећи новчане казне или друге мере као што су упозорење или јавна опомена.

- **Поступци због повреда радне дисциплине**: Одговорна лица која су прекршила процедуре могу бити предмет дисциплинских мера, као што су опомена, суспензија или отказ.

Поштовање процедура означавања и заштите тајних података није само законска обавеза, већ и морална и професионална одговорност свих запослених у органима јавне власти. Адекватна примена ових мера је основа за јачање поверења грађана, очување националне безбедности и интегритета државних институција, као и за заштиту од опасности које могу угрозити интересе Републике Србије. **Свако кршење ових процедура представља значајан ризик који може довести до озбиљних последица, укључујући угрожавање сигурности земље, економског интегритета и међународних односа.** Доследност у примени мера заштите тајних података осигурава стабилност, повећава међународни кредибилитет и јача безбедност државних институција, чиме се ствара чврст основ за адекватно реаговање на претње националној безбедности.

ПОСТУПАЊЕ У СЛУЧАЈУ ИНЦИДЕНТА СА ТАЈНИМ ПОДАЦИМА

Безбедносни инцидент у раду са тајним подацима представља сваки догађај, радњу или пропуст који може угрозити или већ угрожава безбедност тајних података. Ови инциденти обухватају ситуације као што су губитак, крађа, оштећење или неовлашћено откривање података, али и одступања од прописаних мера заштите. У таквим случајевима, обавеза пријаве инцидента од стране свих лица која раде са тајним подацима је од кључне важности. Реакција на инцидент укључује процену ризика, примењивање мера санације и обавештавање надлежних органа, како би се спречиле даље последице и унапредио систем заштите података.

Дефиниција безбедносног инцидента - Безбедносни инцидент у раду са тајним подацима обухвата сваки догађај, радњу или пропуст који доводи или може довести до угрожавања, компромитације или неовлашћеног приступа тајним подацима. То укључује ситуације у којима долази до губитка, крађе, оштећења, уништења или неовлашћеног откривања домаћих или страних тајних података. Безбедносним инцидентом се сматра и свако одступање од прописаних мера заштите утврђених законом, подзаконским актима, безбедносним политикама и интерним процедурама. Овакви инциденти могу настати услед намерних радњи (као што су шпијунажа или злоупотреба овлашћења) или ненамерних пропуста (нехат, немар, техничке грешке), а у оба случаја последице могу бити озбиљне и подложне правној одговорности. Упознавање са појмом и

механизмима поступања у случају безбедносног инцидента представља кључни сегмент система заштите тајних података.

Обавеза обавештавања - Сва лица која на било који начин раде са тајним подацима имају неодложну обавезу да пријаве сваки безбедносни инцидент или сумњу на повреду мера заштите. Обавештавање се врши непосредно надређеном, овлашћеном лицу за заштиту тајних података или руководиоцу органа. У зависности од тежине и природе инцидента, обавештавају се и Канцеларија Савета за националну безбедност и заштиту тајних података, службе безбедности (БИА или ВБА у складу са надлежностима) или надлежно тужилаштво. Ова обавеза се заснива на члану 35. став 3. Закона о тајности података и односи се на сва лица која су:

- запослена, ангажована или овлашћена за руковање тајним подацима;
- преносила, обрађивала или чувала податке, чак и ван службених просторија;
- уочила повреду мера као део безбедносног, техничког или организационог система;
- примила пријаву или самостално открила инцидент као овлашћено лице.

Одлагање, прикривање или непријављивање инцидента сматра се тешком повредом обавеза и може водити дисциплинској, прекршајној или кривичној одговорности.

Класификација инцидената - У складу са одредбама Закона о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. У најширем смислу, свака компромитација штићених података подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што представља повреду основних принципа заштите и може довести до озбиљних последица по јавне органе, правна лица или појединце. Компромитација може настати, на пример, када је сеф са тајним подацима остављен отворен и без надзора, када неовлашћено лице има увид у садржај, ако се подаци преносе преко небезбедних канала комуникације или се износе ван службених просторија без адекватне заштите. Повреда може настати и ако се не поштује прописана процедура за уништавање тајних података.

Најчешћи узроци инцидената су људске грешке и немар запослених, недовољна обученост лица која рукују тајним подацима, сајбер напади, злоупотреба додељеног приступа, као и технички пропусти у мерама физичке и техничке заштите. Конкретни ризици укључују ненамерна открића података лицима која немају право да их знају, погрешну конфигурацију система, намерне злоупотребе попут саботаже, шпијунаже или хакерских напада, као и губитак уређаја који садрже тајне податке. Класификација инцидената врши се у односу на

потенцијалну или насталу штету по интересе Републике Србије, као и на утицај на интегритет и доступност података. Сврха класификације је процена ризика и приоритизација мера одговора.

Први ниво представља повреду радне дисциплине, када поступање није довело до компромитације података, али је било несавесно или незаконито, као што је непоштовање процедура, немар у примени заштитних мера, непријављивање губитка података или приступ без основе у службеној функцији. У тим случајевима примењују се дисциплинске мере у складу са законом, које могу укључити упозорење, смањење плате, премештај, разрешење или отказ. **Други ниво** подразумева прекршај, када инцидент није довео до компромитације, али указује на озбиљне пропусте у примени мера заштите. Такви случајеви укључују, између осталог, неправилно означавање тајности, изостанак образложења о одређивању тајности, непредузимање мера од стране руковаоца, као и достављање података неовлашћенима без откривања садржаја. За ове прекршаје закон предвиђа новчане казне у распону од 5.000 до 50.000 динара. **Трећи и најтежи ниво** јесте кривично дело, када је дошло или је могло доћи до компромитације тајних података, било неовлашћеним саопштавањем, губитком, откривањем или прибављањем података без одобрења. Закон разликује казне у зависности од степена тајности: за податке означене као „интерно“ или „поверљиво“ предвиђена је казна затвора од 3 месеца до 3 године, за „строго поверљиво“ од 6 месеци до 5 година, а за „државну тајну“ од 1 до 10 година. У тежим облицима, као што су кривична дела почињена из користољубља, у иностранству или у условима ратног стања, казне могу достићи и до 15 година затвора. Ако је дело учињено из нехата, санкције су блаже и крећу се од новчаних казни до пет година затвора, зависно од степена тајности. Оваква класификација омогућава доследно реаговање, примену одговарајућих мера и унапређење безбедносне културе у систему заштите тајних података.

Процена околности и правна квалификација - У складу са Законом о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. Компромитација подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што нарушава основне принципе заштите и може имати озбиљне последице по јавне органе, правна лица или појединце. Примери компромитације укључују остављање отвореног сефа са поверљивим подацима, увид неовлашћених лица, коришћење небезбедних канала комуникације или непоштовање прописаних процедура за уништавање података. Узроци најчешће проистичу из људске грешке, немара, недовољне обучености, злоупотребе приступа, сајбер напада или техничких пропуста у

мерама заштите. Инциденти се процењују и правно квалификују као: – Повреда радне дисциплине, када није дошло до компромитације, али је поступање било несавесно или противзаконито (нпр. непоштовање процедура, приступ без основа); – Прекршај, ако је прекршен закон или прописана процедура без директне компромитације, али са озбиљним пропустима у примени мера заштите (нпр. непотпуно означавање или пропуст у поступању руковаоца); – Кривично дело, када је дошло или је могло доћи до озбиљне компромитације (нпр. неовлашћено откривање, губитак, прибављање података без одобрења).

О тежини инцидента одлучује више фактора: врста и степен тајности података, намера извршиоца, настала или могућа штета и потенцијални утицај на националну безбедност. Погрешна правна квалификација може довести до пропуста у поступању и озбиљних последица. У зависности од квалификације, примењују се различити механизми: – за дисциплинске повреде – интерне мере (упозорење, разрешење, отказ), – за прекршаје – новчане казне, – за кривична дела – казне затвора у распону од три месеца до десет година, а у тежим случајевима и до петнаест година. Процена ризика и последица је суштинска за разумевање степена угрожености. Она мора обухватити не само конкретну штету, већ и могуће импликације по државу, права појединаца или међународне односе.

Поступање у случају инцидента - У случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних или страних тајних података, овлашћено лице или старешина органа јавне власти обавезно:

- хитно утврђује околности инцидента и врши процену штете;
- примењује мере санације и спречавања сличних случајева;
- саставља извештај у складу са члановима 36. и 84. Закона о тајности података;
- иницира унутрашњу контролу ради утврђивања узрока и одговорности.

Сваки такав инцидент се сматра безбедносним ризиком високог нивоа и захтева брзу, координисану и документовану реакцију. Потребно је одмах обавестити:

1. орган од ког је податак потекао;
2. надлежно тужилаштво и Канцеларију Савета за националну безбедност и заштиту тајних података;
3. Безбедносно-информативну агенцију, ако је инцидент од ширег значаја.

Извештај о инциденту мора да садржи опис догађаја, анализу узрока, процену ризика и предузете мере.

Препоручене мере - Канцеларија Савета за националну безбедност и заштиту тајних података препоручује да сваки орган установи системске мере за превенцију и брз одговор:

- редовне безбедносне провере и анализе ризика;
- континуирану едукацију запослених;
- прецизне процедуре за руковање тајним подацима;
- техничке и организационе мере у ИКТ и другим критичним секторима.

Руковалац тајних података у органу јавне власти или старешина органа играју кључну улогу у управљању инцидентом. Њихове обавезе укључују:

- **Утврђивање чињеница**: у сарадњи са стручњацима идентификују се узроци и околности инцидента (нпр. људска грешка, технички пропуст или злоупотреба); • **Процена штете**: утврђује се обим и последице инцидента по безбедност, систем и међународне обавезе;
- **Хитне мере**: техничка и организациона санација, обустављање приступа, изолација система;
- **Спречавање понављања**: ревизија процедура, додатне обуке, јачање контролних механизама;
- **Извештавање:** доставља се извештај Канцеларији Савета за националну безбедност и заштиту тајних података о свим мерама и закључцима.

Циљ је системски приступ, усклађен са законом, који обезбеђује поуздану заштиту података и јачање безбедносне културе у институцији.

Контролна листа у случају инцидента - Органи јавне власти и правна лица се охрабрују да примењују унапред дефинисану листу за проверу, као алат за брзо и ефикасно реаговање у случају инцидента. Листа треба да обухвати:

- прецизну идентификацију и одређивање врсте и озбиљности инцидента;
- благовремено обавештавање свих релевантних актера и структура;
- детаљну анализу, потпуну документацију догађаја и процену настале штете;
- предузимање корективних мера ради отклањања последица, као и превентивних мера ради спречавања понављања сличних инцидената.

Тиме се обезбеђује координисан и систематски приступ у управљању инцидентима.

На крају - Ефикасно управљање инцидентима са тајним подацима представља не само темељ безбедносне културе, већ и кључни елемент у очувању интегритета и поверења у безбедносне системе. Сви инциденти морају бити обрађени у строгом складу са законом, уз брзу, али пажљиву реакцију, и одлучност организације да минимизира насталу штету. Поред тога, неопходно је спровести свеобухватну процену и применити адекватне корективне и превентивне мере које не само да спречавају поновно настајање инцидената, већ и стално унапређују систем заштите, чинећи га отпорнијим и ефикаснијим у будућности

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.

ПРИНЦИП НУЛТОГ ПОВЕРЕЊА У РАДУ СА ТАЈНИМ ПОДАЦИМА

Информациона безбедност у раду са тајним подацима представља један од кључних концепата заштите националних, корпоративних и институционалних вредности. Савремени информациони системи који управљају тајним подацима морају бити отпорни на потенцијалне претње и компромитацију. **Принцип нултог поверења је безбедносни приступ који елиминише подразумевано поверење и захтева континуирану верификацију идентитета и приступа. У раду са тајним подацима, овај модел осигурава да само овлашћени корисници могу приступити тајним подацима и информацијама.** Принцип нултог поверења се значајно разликује од традиционалних модела безбедности, посебно од **периметарског приступа** („castle and moat“), који претпоставља да су корисници унутар мреже поуздани.

ПРИНЦИП НУЛТОГ ПОВЕРЕЊА

1. **Никада не веруј, увек проверавај** – сваки захтев за приступ се верификује без обзира на локацију корисника.
2. **Минимални приступ** – корисници добијају само онолико привилегија колико им је неопходно.
3. **Континуирано праћење** – активности корисника се анализирају у реалном времену ради детекције потенцијалних претњи.
4. **Шифровање података** – тајни подаци се чувају и преносе у шифрованом облику.
5. **Сигурни комуникациони канали** – употреба VPN-а, шифрованих е-порука и безбедних платформи за размену тајних података и информација.

Принцип нултог поверења vs. Традиционални безбедносни модели у раду са тајним подацима

Карактеристика	Традиционални модел	Принцип нултог поверења
Приступ	Дозвољава приступ корисницима унутар мреже	Захтева верификацију за сваки приступ
Контрола приступа	Заснована на локацији корисника	Континуирана аутентификација и ауторизација
Сигурност података	Фокус на заштиту периметра	Шифровање и минимални приступ
Претпоставка о поверењу	Корисници унутар мреже се сматрају поузданим	Нико није поуздан по дефиницији
Мониторинг	Ограничен надзор активности	Континуирано праћење и анализа
Заштита комуникације	Стандардни канали комуникације	Шифровани и сигурни канали

Know и Принцип нултог поверења су два принципа безбедности који се примењују у раду са тајним подацима, али имају различите приступе и циљеве.

Сличности

- **Ограничен приступ** – Оба модела ограничавају приступ тајним подацима и информацијама само на овлашћене кориснике.
- **Минимални приступ** – Корисници добијају само онолико привилегија колико им је неопходно за обављање посла.
- **Заштита тајних података** – Оба модела имају за циљ спречавање неовлашћеног приступа и компромитације тајних података и информација.

Разлике

Карактеристика	Need to Know	Принцип нултог поверења
Фокус	Приступ подацима заснован на улози корисника	Континуирана верификација сваког приступа
Претпоставка поверењу	Корисници који имају одобрење се сматрају поузданим	Нико није поуздан по дефиницији
Контрола приступа	Дефинисане листе приступа на основу пословних потреба	Динамичка аутентификација и ауторизација
Мониторинг	Периодичне провере приступа	Континуирано праћење и анализа активности
Заштита комуникације	Фокус на интерне процедуре и контролу приступа	Шифровани и сигурни комуникациони канали

Примена у информационим системима

- **Need to Know** се користи **у класичним безбедносним структурама**, као што су војне и државне институције, где се приступ подацима заснива на хијерархији и улогама.
- **Принцип нултог поверења** је погодан за **модерне ИКТ системе**, посебно у cloud окружењима, где се приступ подацима мора динамички контролисати и верификовати.

Принцип нултог поверења је еволуција безбедносног приступа, јер елиминише подразумевано поверење и примењује строге мере верификације. У комбинацији са **Need to Know**, може значајно унапредити заштиту тајних података у информационим системима од посебног значаја.

Како имплементирати Принцип нултог поверења у раду са тајним подацима?

- ✓ **Строга контрола приступа** – дефинисање правила приступа и примена мултифакторске аутентификације.
- ✓ **Шифровање података** – коришћење криптографије за заштиту поверљивих информација.
- ✓ **Сигурни комуникациони канали** – избегавање јавних мрежа и коришћење VPN-а.
- ✓ **Континуирано праћење и анализа** – примена система детекције упада (IDS) и безбедносних информационих система (SIEM).
- ✓ **Едукација запослених** – обука за препознавање сајбер претњи и социјалног инжењеринга.

Принцип нултог поверења је идеалан модел за заштиту тајних података, јер елиминише ризик од неовлашћеног приступа и осигурава да се сваки захтев за приступ строго контролише.

* 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

Положај индустријске безбедности у систему заштите тајних података у Републици Србији представља посебан део система заштите тајних података и уређена је Законом о тајности података („Службени гласник РС“, бр. 104/09). Она се примењује на правна лица и предузетнике који у оквиру пословне сарадње са органима јавне власти приступају тајним подацима, обрађују их или их чувају. Циљ индустријске безбедности је спречавање неовлашћеног приступа, откривања, злоупотребе или губитка тајних података када се они налазе ван непосредне контроле органа јвне власти, односно код правних лица.

Обавезе правних лица у области индустријске безбедности - Према Закону о тајности података и пратећим прописима, правна лица која обрађују тајне податке дужна су да:

- успоставе интерни систем организационих, техничких и безбедносних мера заштите тајних података;
- имају запослене који су подвргнути безбедносној провери;
- примене мере физичко-техничке заштите простора и информационих система;
- уреде писменим путем са органом јавне власти на који ће начин радити са тајним подацима и како ће исте преносити;
- поседују важећи **Сертификат за правно лице**, који издаје Канцеларија Савета за националну безбедност и заштиту тајних података.

Ови услови су детаљније уређени **Уредбом о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа** („Службени гласник РС“, бр. 63/2013).

Улога органа јавне власти - Орган јавне власти који уступа тајне податке обавезан је да:

- процени ризик у погледу уступања тајних података;
- провери испуњеност услова код правног лица у складу са Законом о тајности података;
- надзире спровођење мера заштите током трајања уговорног односа.

На тај начин се обезбеђује континуитет у примени прописа и одржава висок ниво безбедности података и ван непосредне контроле државе.

Однос према другим прописима – Закон о одбрани и Закон о производњи и промету наоружања и војне опреме - Индустријска безбедност је у Републици

Србији у потпуности дефинисана Законом о тајности података („Службени гласник РС“, бр. 104/2009). Овај закон представља темељни акт који уређује систем заштите тајних података, укључујући и оне податке који се односе на производњу и промет наоружања и војне опреме.

Иако неки тајни подаци могу бити додатно квалификовани као подаци од значаја за одбрану, њихова заштита не произилази из Закона о одбрани („Службени гласник РС“, бр. 116/2007, 88/2009, 88/2009 - др. закон, 104/2009 – др. закон, 10/2015 и 36/2018), већ искључиво из Закона о тајности података. Закон о одбрани и одговарајући подзаконски акти само ближе одређују категорије тајних података и прописују посебне мере поступања у оквиру система одбране, али не уводе посебан или паралелан режим заштите. На тај начин, у Републици Србији постоји јединствен, интегрисан систем заштите тајних података, који се примењује на све органе јавне власти, привредне субјекте и друга лица, уз могућност прописивања додатних спецификација у складу са њиховим делокругом рада.

Посебно у области производње и промета наоружања и војне опреме, Закон о производњи и промету наоружања и војне опреме („Службени гласник РС“, бр. 36/2018) прецизира појам индустријске безбедности производње наоружања и војне опреме. Према том закону, индустријска безбедност у овом контексту подразумева:

„Индустријска безбедност производње наоружања и војне опреме је систем безбедносно-заштитних мера и поступака којима се испуњавају организациони и технички услови за чување техничке документације за производњу наоружања и војне опреме и других тајних података, и спречава уништење или оштећење капацитета за производњу наоружања и војне опреме, угрожавање безбедности људских ресурса, уништење, оштећење или отуђење наоружања и војне опреме и техничке документације за производњу наоружања и војне опреме, као и одавање тајних података о производњи наоружања и војне опреме.“

Ова дефиниција не уводи нови правни режим заштите тајних података, већ у складу са Законом о тајности података, конкретизује посебне безбедносне и техничке мере које се примењују у области производње и промета наоружања и војне опреме.

Према томе, све безбедносно-заштитне активности у вези са индустријском безбедношћу у сектору одбране, као и у другим секторима где се рукује тајним подацима, морају бити засноване на општим начелима и обавезама прописаним Законом о тајности података, уз примену посебних мера дефинисаних секторским прописима, као што су Закон о одбрани и Закон о производњи и промету наоружања и војне опреме.

Сертификат за правна лица – предуслов за приступ тајним подацима - Сертификат за правна лица представља званичну потврду да је одређено правно лице способно да примењује мере заштите тајних података у складу са Законом о тајности података („Службени гласник РС“, бр. 104/2009) и подзаконским актима који ближе уређују ову област. Сертификат издаје **Канцеларија Савета за националну безбедност и заштиту тајних података**, након спроведеног поступка издавања сертификата и безбедносне процене, које врше надлежни органи (БИА или МУП – у зависности од надлежности).

Захтев за издавање сертификата може поднети **искључиво орган јавне власти** који планира да са правним лицем закључи уговор који подразумева приступ тајним подацима. Правна лица **не могу самостално подносити захтев**, осим ако имају статус органа јавне власти – што се доказује мишљењем Министарства правде. Такав изузетак важи, на пример, за јавна предузећа и друге субјекте основане од стране државе.

Орган јавне власти који подноси захтев дужан је да се у самом захтеву јасно изјасни да ли је правном лицу потребан капацитет за обраду и чување тајних података у свом седишту или ће се ти подаци обрађивати искључиво у просторијама органа јавне власти. **Ова информација је од суштинског значаја за утврђивање потребе за акредитацијом простора у правном лицу.** Уз захтев се прилаже прописана документација, у складу са моделом који објављује Канцеларија, укључујући и попуњен безбедносни упитник за овлашћено лице. По завршетку безбедносне провере, Канцеларија доноси решење и издаје сертификат који важи у складу са највишим степеном тајности података којима ће правно лице приступати. У пракси, постоје **две ситуације у којима запослени у правном лицу приступају тајним подацима**:

1. **Када се тајни подаци обрађују и чувају у просторијама самог правног лица** – у овом случају, потребно је да правно лице има **акредитован простор**, односно обезбеђене и технички проверене услове за чување и руковање тајним подацима, као и интерне процедуре за њихову заштиту.
2. **Када запослени у правном лицу обрађују тајне податке искључиво у просторијама органа јавне власти** – у том случају, није потребна акредитација простора у правном лицу, већ се фокус ставља на безбедносну проверу и поузданост самог лица које ће имати приступ.

У оба случаја, одобрење у виду сертификата за правно лице је обавезно, као и испуњеност свих услова у складу са законом и прописаним процедурама.

Орган јавне власти који уступа тајне податке има обавезу да:

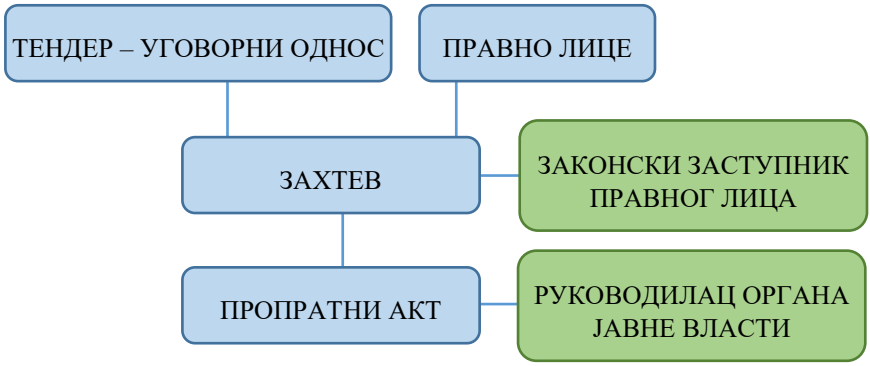
- Изврши процену ризика у погледу уступања тајних података.
- Увери се да правно лице испуњава све услове прописане Законом о тајности података.
- Контролише спровођење мера заштите за време трајања уговорног односа.

На овај начин, континуирано се одржава висок ниво заштите тајних података, без обзира на то да ли су под непосредном контролом органа јавне власти или су уступљени трећим лицима.

Сертификат се може **опозвати** уколико се утврде нове околности које представљају безбедносни ризик или уколико правно лице не поступа у складу са прописаним мерама и обавезама заштите тајних података. Правна лица **без важећег сертификата не могу приступати, обрађивати, нити чувати тајне податке** који потичу од органа јавне власти, нити могу учествовати у поверљивим уговорним активностима које подразумевају руковање таквим подацима.

Индустријска безбедност, као саставни део система заштите тајних података, омогућава да правна лица ван система јавне управе, под условима дефинисаним законом, приступају, обрађују и чувају тајне податке, али искључиво на основу претходне безбедносне провере и уз поседовање важећег сертификата за правно лице. Правни основ за овакво учешће субјеката ван јавне управе утврђен је искључиво **Законом о тајности података**, који обезбеђује јединствен и свеобухватан нормативни оквир, без могућности преплитања или дуплирања надлежности са другим законима.

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.

ПОДИЗАЊЕ БЕЗБЕДНОСНЕ КУЛТУРЕ И СВЕСТИ

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?).

ИНФОРМАЦИОНО 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.

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 интерне 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.

СМЕРНИЦЕ ЗА ОБУКУ ЗАПОСЛЕНИХ О ЗАШТИТИ ТАЈНИХ ПОДАТАКА

Смернице представљају званичан скуп препорука, корака и најбољих пракси осмишљених како би се обезбедило правилно и одговорно руковање штићеним информацијама, а посебно тајним подацима. Оне служе као основа за развој и спровођење обука запослених у органима јавне власти и другим организацијама, са циљем унапређења безбедносне културе, свести и вештина у обради свих штићених података, односно заштити тајних података. Смернице укључују детаљно дефинисане циљеве, методологије и ресурсе који подржавају њихову примену, а посебно се ослањају на законе, прописе и најновије стандарде у области заштите тајних података.

Препоруке за развој и спровођење програма обуке

Развој и спровођење програма обуке за заштиту тајних података је од суштинског значаја за осигурање да сви запослени разумеју своје обавезе и примењују најбоље праксе у руковању штићеним информацијама, а посебно тајним подацима. **Канцеларија Савета за националну безбедност и заштиту тајних података** пружа бројне ресурсе који могу помоћи у креирању и имплементацији оваквих програма. Ове смернице представљају важан корак у подизању безбедносне свести и културе запослених, као кључног аспекта заштите информација и података у органима јавне власти.

Циљеви смерница

- Осигурати да сви запослени разумеју значај заштите тајних података.

- Обезбедити континуирану едукацију о правилима и процедурама руковања тајним подацима.
- Развити систем за редовну евалуацију и унапређење програма обуке.
- Оспособити унутрашње тренере који ће спроводити обуке у својим организацијама.
- Подстаћи изградњу културе безбедности унутар организације и примену најбољих пракси у заштити осетљивих података.

Кључне компоненте програма обуке

1. Теоријско знање
- Укључити детаљну обуку о правним и регулаторним оквирима (нпр. Закон о тајности података).
- Објаснити различите нивое означавања тајности („интерно“, „поверљиво“, „строго поверљиво“, „државна тајна“) и како их правилно применити.
- Представити практичне примере из реалног живота како би запослени разумели значај поштовања регулативе.

2. Практична примена
- Организовати вежбе које симулирају управљање приступом тајним подацима (нпр. размену докумената са ограниченим приступом).
- Укључити сценарије за реаговање на инциденте цурења информација, са нагласком на утврђивање слабих тачака.
- Додати примере хипотетичких пропуста ради бољег разумевања последица.

3. Аналитичке вештине
- Увести алате за процену ризика (нпр. алатке за утврђивање вероватноће и утицаја пропуста).
- Омогућити симулације у којима учесници процењују безбедносне изазове и осмишљавају стратегије за њихово решавање.

4. Критичко размишљање
- Организовати радионице са етичким дилемама у обради тајних података (нпр. ситуације сукоба интереса или понашања у сложеним условима).
- Подстицати дискусије о потенцијалним последицама неодговарајућег руковања поверљивим информацијама.

Кључни кораци у развоју програма обуке

1. Анализа потреба за обуком

- Идентификовати специфичне потребе организације у вези са заштитом тајних података.
- При анализи потреба, узети у обзир следеће теме обуке:
  - Систем заштите тајних података
  - План заштите тајних података
  - Персонална безбедност (поступак издавања сертификата физичким и правним лицима)
  - Умањење инсајдерске претње
  - Индустријска безбедност (учешће правних лица у поверљивим набавкама)
  - Физичка безбедност
  - Информациона гаранција
  - Административна безбедност
  - Унутрашња контрола која се спроводи унутар органа јавне власти
  - Стручни надзор и контрола које обавља Канцеларија Савета
- Користити **Водич за имплементацију Закона о тајности података** који пружа смернице за успостављање система заштите тајних података у органима јавне власти.

2. Развој наставног плана и материјала

- Прилагодити садржај обуке на основу идентификованих потреба.
- Користити приручнике као што су:
  - Систем заштите тајних података – скрипта
  - Информациона безбедност у ИКТ системима за рад са тајним подацима – скрипта
  - Поступак издавања безбедносног сертификата – персонална безбедност (скрипта)
  - Индустријска безбедност – скрипта
- Развити посебан програм „**тренинга за тренере**.“
- Развити интерактивне модуле, тестове, квизове и симулације како би обука била што ефикаснија и занимљивија.

3. Спровођење обуке

- Организовати редовне обуке за све запослене.

- Искористити актуелне обуке које нуди **Канцеларија Савета** (контактирати на: obuke@nsa.gov.rs).
- Спроводити **тренинг за тренере** ради изградње интерних капацитета за континуирану обуку.
- Развити наставне методе за преношење знања и обуку нових запослених.
- Обезбедити континуирано усавршавање тренера кроз посебне програме обуке.
- Организовати редовне радионице и размену искустава између тренера.
- Увести систем сертификације за запослене који успешно заврше обуку:
  - Сертификате издаје сам орган јавне власти или **Канцеларија Савета за националну безбедност и заштиту тајних података**.
  - Сертификати потврђују компетенције и могу се користити за оцењивање државних службеника и намештеника.

4. Улога менаџмента

- Руководиоци треба да промовишу значај заштите тајних података и активно подржавају програме обуке.
- Обезбедити да менаџмент редовно прати примену мера безбедности и пружа пример запосленима.
- Интегрисати безбедносну културу и свест у процесе доношења одлука.
- Обавезати руководиоце да периодично пролазе напредне обуке о безбедносним политикама и раду са тајним подацима.
- Осигурати да се безбедносне смернице из Плана заштите тајних података примењују у свакодневним радним активностима.

5. Евалуација и унапређење

- Након спроведене обуке, прикупити повратне информације од учесника.
- Редовно ажурирати програм обуке на основу нових прописа и најбољих пракси.
- Дефинисати показатеље успешности обуке, као што су:
  - Проценат запослених који успешно пролазе тестирање након обуке.
  - Број идентификованих пропуста у руковању тајним подацима пре и после обуке.
  - Степен примене научених мера у пракси.

Додатни ресурси

- **Обрасци и модели одлука**: За имплементацију Закона о тајности података.
- **Приручници**: За додатно усавршавање и разумевање принципа заштите тајних података.

- **Онлајн консултације**: За додатну подршку, заказивање путем е-поште.

Интеграцијом ових корака, организације могу успоставити ефикасан програм обуке који осигурава да запослени правилно рукују тајним подацима и придржавају се свих релевантних прописа.

Допринос организације настанку штетног догађаја са тајним подацима често је резултат пропуста који се јављају на системском, оперативном или едукативном нивоу. Организације које не успоставе целовит и функционалан систем заштите тајних података у складу са законским обавезама, излажу се значајним безбедносним ризицима и потенцијалним правним последицама.

Најчешћи **системски пропусти** укључују одсуство званично усвојеног Плана заштите тајних података, непостављање руковаоца тајних података, као организационе јединице или лица одговорног за руковођење системом заштите, као и недостатак јасно дефинисаних унутрашњих аката и процедура за руковање и управљање тајним подацима. Уз то, чест је и недостатак документације о примени мера заштите тајних података. Лоша техничка и физичка инфраструктура — као што су просторије без контроле приступа, непрописно складиштење папирних или електронских података — додатно повећава ризик од инцидената.

Превентивне мере се у многим организацијама – органима јавне власти или правним лицима, недовољно примењују или се формално спроводе без суштинске контроле, како унутрашње тако и спољашне. Неуспостављање планова управљања ризиком, изостанак редовних процена безбедносних претњи и непостојање доследне персоналне безбедности, која обухвата како безбедносне провере лица која приступају тајним подацима, тако и поседовање одговарајућих сертификата за приступ тајним подацима, представљају озбиљне пропусте. Поред тога, коришћење неакредитованих или лоше одржаваних информационо-комуникационих система за рад са тајним подацима који не поседују адекватне криптографске мере, као ни политике ажурирања и техничке контроле, знатно умањује ниво заштите.

Недовољна обученост запослених је чест фактор ризика. Организације често не организују обавезне почетне обуке при пријему у радни однос, не спроводе периодичне обуке у складу са променом прописа или технолошким новинама, нити практичне вежбе симулације инцидената. Изостанак специјализованих едукација за лица са посебним приступом (руковаоци, унутрашња контрола, лица за процену ризика) доводи до тога да постоји озбиљан дисбаланс у знању и компетенцијама. Невођење евиденције о похађању и садржају обука за рад са

тајним подацима додатно онемогућава управљање кадровским капацитетима и контролу стручности.

Реакција на инциденте је често неадекватна због непостојања јасно дефинисаних унутрашњих процедура за пријаву, реаговање, истраживање и санирање инцидената у раду са тајним подацима. У пракси, пропушта се дубинска анализа узрока инцидената, не формирају се комисије за процену штете, а евиденција инцидената се не води систематично. Непријављивање инцидената надлежним државним органима, као и одсуство предузимања мера за ублажавање последица, угрожава интегритет система заштите и ствара ризик од понављања истих пропуста.

Одговорност често није јасно утврђена ни на личном ни на функционалном нивоу. Унутрашњи акти не предвиђају механизме за утврђивање дисциплинске, прекршајне или кривичне одговорности у случају кршења правила о заштити тајних података. Без јасно дефинисаног система санкција и контролних механизама, пропусти остају несанкционисани, што охрабрује небезбедно понашање и повећава ризик од поновног настанка инцидената.

Толерисање културе небезбедног поступања са тајним подацима представља дубоко укорењен проблем. Овакво окружење се карактерише занемаривањем процедура, рутинским заобилажењем правила, недовољном свешћу о ризицима, као и одсуством система за анонимно пријављивање пропуста и неправилности. Запослени у таквом систему не осећају личну одговорност, што доводи до пада безбедносне културе и повећане учесталости инцидената.

Решења за ове проблеме морају бити системска и доследна. Кључне мере укључују: успостављање јасно дефинисаног и функционалног система заштите тајних података, увођење редовних и обавезних обука, имплементацију процедура за реаговање и анализу инцидената, те промовисање културе одговорности и поштовања правила. Лидерство у области безбедности и транспарентност у поступању морају бити подржани механизмима контроле, ревизије и извештавања како би систем функционисао ефикасно и одрживо.

Област пропуста	Кључни проблеми
Системска организација	Недостаје план заштите тајних података, руковалац тајних података, одговорна лица, процедуре, техничка/физичка заштита
Превентивне мере	Нема процене ризика, сертификата за приступ тајним подацима, акредитованих ИКТ система за рад са тајним подацима
Обука и едукација	Недовољно или формално спровођене обуке, без евиденције и специјализације
Реакција на инциденте	Нема поступка за пријаву и анализу инцидената, непријављивање надлежнима
Одговорност	Непостојање механизама за дисциплинску, прекршајну или кривичну одговорност, несанкционисани пропусти
Безбедносна култура	Толерише се небезбедно понашање, занемарују се процедуре, нема система за пријаве (негативан контекст „цинкарење“)

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/3945/Neophodni_koraci_za_dobijanje_sertifikata_PL.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. **Акредитација икт система** подразумева да 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
4. **Активирање containment мера**: Ове мере подразумевају брзу реакцију како би се инцидент изолово и спречило даље ширење оштећења.
5. **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.
6. **Апсолутне сметње** (непосредни разлог за ускраћивање сертификата) - Ово су здравствени проблеми који аутоматски дисквалификују особу, јер представљају трајан или тежак ризик по безбедност.
7. **Архивска грађа** јесте целина докумената или записа насталих или примљених деловањем и радом субјеката у изворном или репродукованом облику документа, без обзира на форму и формат бележења, као и прописане евиденције о њему.
8. **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.
9. **Accountability („одговорност и праћење поступања")** – свако лице које рукује тајним подацима мора бити у потпуности одговорно за своје поступке у вези са тим подацима, а орган је у обавези да обезбеди систем надзора, праћења и евидентирања активности.
10. **Безбедносна акредитација** - 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.
11. **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.

12. **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.
13. **Безбедносна зона II степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО”.
14. **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.
15. **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.
16. **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).
17. **Безбедносна сметња** представља чињеницу која онемогућава издавање сертификата.
18. **Безбедносне процедуре** су прописана правила за поступање лица у раду са тајним подацима.
19. **Безбедносни брифинг** представља упознавање са прописима којима се уређује тајност података и последицама неовлашћеног приступа и коришћења тајних података.
20. **Безбедносни инцидент** дешава се када постоји стварни или потенцијални ризик за штићене податке и даље категорисан као кривично дело или прекршај.
21. **Безбедносни ризик** је стварна могућност нарушавања безбедности тајних података.
22. **Безбедносни упитник** је саставни део документације у поступку издавања сертификата за приступ тајним подацима.
23. **Безбедност** означава стање неког субјекта (појединца, групе људи, заједнице, институције) које карактерише одсуство невоља, брига, несрећа, опасности и других зла.

24. **Блокада приступа:** За спречавање даљих оштећења, неопходно је ограничити приступ угроженим подацима и предузети техничке мере као што су lock-out и повлачење докумената.
25. **Водич за поступање у случају инцидента са тајним подацима** представља кључни инструмент за адекватно управљање ситуацијама које угрожавају безбедност и интегритет заштићених података у оквиру органа јавне власти и правних лица.
26. **Губитак поверења** - Недостатак адекватне заштите тајних података може довести до значајног губитка поверења у органе јавне власти.
27. **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.
28. **Дебрифинг** подразумева упознавање са прописима и обавезама по престанку потребе за приступом тајним подацима по различитим основама.
29. **Директива 488/2001/ЕЦ Европског парламента и Савета** односи се на заштиту класификованих информација које се стварају и обрађују у Европској унији, и представља правни оквир за регулисање безбедности и размене класификованих података између држава чланица и институција ЕУ. Ова директива поставља стандарде који се односе на обраду класификованих информација у државама чланицама, као и на поступке везане за безбедност, комуникацију и размену тих информација. Директива прописује правила за приступ класификованим информацијама, што подразумева да особе које имају приступ класификованим подацима морају проћи безбедносне провере.
30. **Документ** је сваки носач податка (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.
31. **Доношење формалне одлуке о тајности** - Орган јавне власти је у обавези да донесе генеричну или појединачну писмену одлуку о одређивању степена тајности података, уз процену утицаја и потенцијалне штете по интересе Републике Србије у случају откривања, злоупотребе или уништења података. Тајност податка, под условима и на начин утврђен законом о тајности података, одређује овлашћено лице.
32. **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.
33. **Евиденције** подразумевају да 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.
34. **Евиденцију корисника тајних података** је евиденција коју води руковалац тајним подацима у органу јавне власти.

35. **Етички аспекти безбедносних провера медицинских података** укључују заштиту приватности, избегавање дискриминације, осигурање информисаног пристанка, јасне и праведне циљеве, као и минимизацију интервенције.
36. **Жалба** је правно средство у управном поступку које се може изјавити против управног акта тј. против првостепеног решења.
37. **Зависност од информационо-комуникационих технологија (ИТ)** - подразумева прекомерну употребу дигиталних алата, као што су мобилни телефони, рачунари, друштвене мреже или видео игре, која може довести до 16 поремећаја концентрације, смањене продуктивности или чак психолошких проблема.
38. **Зависност од коцке (патаљије)** - може бити проблем који утиче на појединца у различитим аспектима живота, укључујући и његов радни учинак и понашање у ситуацијама које захтевају висок ниво одговорности и пажње, као што је рад са класификованим информацијама.
39. **Зависност од секса или сексуална зависност**, која се карактерише прекомерном и неконтролисаном потребом за сексуалним активностима која може бити психолошки и физички штетна, може се разматрати као фактор у безбедносним проверама за приступ класификованим информацијама, али као и код других зависности, њен утицај зависи од озбиљности и последица које она има на појединца.
40. **Заштита података** је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације.
41. **Злоупотреба информација** - Неовлашћени приступ тајним подацима може довести до извоза осетљивих информација и коришћења од стране странака које имају непријатељске намере према Србији.
42. **Злоупотреба тајних података** - Лице које злоупотреби тајне податке, било да их дели, продаје или на неки други начин користи против националне безбедности, може бити осуђено на казне затвора.
43. **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.
44. **Идентификација категорија података** - Подаци се анализирају како би се утврдило да ли испуњавају услове за означавање као тајни, укључујући прописима предвиђене категорије података, као и процену могућег утицаја на националну безбедност, јавни интерес, територијални интегритет и економске интересе. У овом кораку се такође разматра и општи значај података, као и последице које би њихово откривање могло имати на рад органа јавне власти.
45. **Изјава** чини саставни део документације на основу које је издат сертификат за приступ тајним подацима, односно дозвола.

46. **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.
47. **Инсајдер** (енг. insider - "неко унутра") је назив за особу која је припадник неке друштвене групе због чега располаже одређеним сазнањима недоступним широј јавности.
48. **Интегритет** значи очуваност изворног садржаја и комплетности података;
49. **Интерна контрола** представља мере пажње усмерене на спречавање грешака, прекомерних трошкова и преваре, проверава и обезбеђује поузданост информација.
50. **Информанти** су лица која случајно и пригодно сазнају за планирана или извршена кривична дела и њихове учиниоце.
51. **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.
52. **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.
53. **Информациона безбедност тајних података** обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних информација које се обрађују у комуникационо-информационим системима – КИС.
54. **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.
55. **ISO/IEC 27001** је међународни стандард за управљање безбедношћу информација. Детално описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ISMS) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.
56. **Јавни подаци** су концепт у коме одређени подаци треба да буду слободно доступни свима на коришћење и поновну употребу, без ауторских или било каквих других ограничења.
57. **Кемз (Компромитација електромагнетним зрачењем)-** представља шири концепт који обухвата техничке и организационе мере за спречавање цурења података путем електромагнетних емисија.

58. **КЕМЗ (Компромитација електромагнетним зрачењем)** представља шири концепт који обухвата техничке и организационе мере за спречавање цурења података путем електромагнетних емисија.
59. **Класификација инцидената** - У складу са одредбама Закона о тајности података („Сл. гласник РС“, бр. 72/2009), инциденти у систему заштите тајних података класификују се према степену ризика по заштићене интересе и врсти повреде закона. У најширем смислу, свака компромитација штићених података подразумева неовлашћен приступ, откривање, измену, уништавање или губитак података, што представља повреду основних принципа заштите и може довести до озбиљних последица по јавне органе, правна лица или појединце.
60. **Компромитација тајног податка** представља умишљајно, нехатно или немарно откривање тајних података непозваним и неовлашћеним лицима.
61. **Компромитација штићених података у најширем смислу** (тајних података, личних података, банкарске тајне, пореске тајне, пословне и професионалне тајне) настаје када дође до неовлашћеног откривања, приступа, измене, уништења или губитка података, чиме се угрожава њихова поверљивост, интегритет или доступност. Такви догађаји могу проузроковати озбиљну штету по орган јавне власти, правно лице, организацију или појединца.
62. **Компромитујуће електромагнетно зрачење (КЕМЗ)** представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података.
63. **Контролна листа у случају инцидента** - Органи јавне власти и правна лица се охрабрују да примењују унапред дефинисану листу за проверу, као алат за брзо и ефикасно реаговање у случају инцидента.
64. **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.
65. **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.
66. **Кривично дело (Кривична одговорност)**: Инцидент који је довео или могао довести до компромитације тајних података, укључујући: • неовлашћено саопштавање, предаја или омогућавање приступа тајним подацима, • губитак, уништење или откривање докумената који садрже тајне податке, • прибављање тајних података без одобрења.

67. **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.
68. **Криптографски производ** је софтвер или уређај путем кога се врши криптозаштита.
69. **Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима.
70. **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.
71. **Листа "ПОТРЕБНО ПОДЕЛИТИ СА"** представља међународни принцип рада са тајним подацима који подразумева списак органа јавне власти који међусобно размењују тајне податке.
72. **Лични податак** је сваки податак који се односи на физичко лице чији је идентитет непосредно или посредно одређен или одредив-посебно на основу ознаке идентитета. Лични податак је свака информација која се односи на физичко лице које се у неком тренутку може идентификовати; то је карактеристична особина сваке појединачне особе.
73. **Лојалност** је значење изведено преко синонима: оданост, верност, исправност, поданичка верност, честитост, часност, привржености, поверљивост, постојаност, непроменљивост, искреност,поштење.
74. **Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.
75. **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.
76. **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.
77. **НАТО стандард С-М (2002) 49** подразумева да безбедносне провере обухватају различите аспекте кандидата, укључујући: • Кривичну историју. • Психолошке процене. • Медицинске процене.
78. **Недопуштена измена или уништавање тајних података**- Лица која униште, измене или на неки начин ометају очување тајних података, као и лица која не предузму прописане мере заштите података, могу бити кривично санкционисана.
79. **Неовлашћено откривање тајних података**- Лице које без овлашћења открије тајне податке или их користи у незаконите сврхе, може бити кривично гоњено.

80. **Неповољна историја у раду са тајним подацима** – Раније повреде правила о заштити тајних података или неодговорно поступање са поверљивим информацијама (пословна тајна, професионална тајна...)
81. **Непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.
82. **Непоузданост власничке структуре** – Ако се утврди да су власници или оснивачи правних лица повезани са ризичним субјектима, страним утицајем или криминалним групама.
83. **Непоузданост и нестабилност** – Процена да кандидат није довољно одговоран, финансијски стабилан (дугови, честе промене радних места), или да има друге личне карактеристике које га чине подложним притиску или уцени.
84. **Обавеза обавештавања** - Сва лица која на било који начин раде са тајним подацима имају неодложну обавезу да пријаве сваки безбедносни инцидент или сумњу на повреду мера заштите. Обавештавање се врши непосредно надређеном, овлашћеном лицу за заштиту тајних података или руководиоцу органа. У зависности од тежине и природе инцидента, обавештавају се и Канцеларија Савета за националну безбедност и заштиту тајних података, службе безбедности (БИА или ВБА у складу са надлежностима) или надлежно тужилаштво.
85. **Обезбеђење** је планска примена и коришћење оперативно-тактичких метода, мера, радњи, средства и снага ради заштите од угрожавања одређених личности, људи, масовних скупова, имовине, отвореног-затвореног простора, фабричких хала, магацина или других објеката.
86. **Обрада података** је генерално, "прикупљање и употреба података ради стварања смислене информације".
87. **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.
88. **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.
89. **Одлука о одређивању руковаоца тајним подацима у органу јавне власти** је одлука којом се одређује се руковалац тајним подацима у органу јавне власти.
90. **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.

91. **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.
92. **Означавање података -** Подаци добијају јасну ознаку која укључује степен тајности, начин престанка тајности, податке о овлашћеном лицу, датум означавања, назив органа који је донео одлуку и правну основу.
93. **Означавање степена тајности** је означавање тајног податка ознакама: "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО", "ПОВЕРЉИВО" или "ИНТЕРНО".
94. **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.
95. **Организационе мере заштите** представљају организацију заштите процеса рада и функционисања информационо-комуникационог система у редовним околностима и ванредним ситуацијама.
96. **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.
97. **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.
98. **Патролирање** је услуга обезбеђења коју врше службеници обезбеђења крећући се у одређено време између више међусобно раздвојених места/објеката.
99. **Периметар је део физичке безбедности** који се мора поставити око објеката у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.
100. **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.
101. **План заштите тајних података** у органу јавне власти – је основни стуб организационе безбедности у сваком органу јавне власти. Он омогућава правилно управљање тајним подацима и осигурава њихову заштиту, што је од кључног значаја за очување националне безбедности. Иако сам План није директно прописан Законом о тајности података, он се сматра

имплицитно обавезним као део комплетног система заштите тајних података, који мора бити у складу са важећим законима и прописима.

102. **План поступања у вандредним ситуацијама** обухвата процедуре и мере које треба предузети у случају напада, злоупотребе или другиј вандредних ситуација које угрожавају безбедност података.
103. **Повреда радне дисциплине (Дисциплинска одговорност)**: Инцидент који не доводи до компромитације тајних података, али представља незаконито или несавесно поступање у вршењу службене дужности.
104. **Податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и сувереност, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове.
105. **Пословна тајна** је податак који може да има економску вредност. Ова врста података није опште позната нити лако доступна трећим лицима. Банкарска тајна је пример пословне тајне, али њена специфичност јесте да иста прелази у више категорија (професионална тајна, лични подаци).
106. **Поступци због повреда радне дисциплине:** Одговорна лица која су прекршила процедуре могу бити предмет дисциплинских мера, као што су опомена, суспензија или отказ.
107. **Правне импликације** - Када дође до кршења процедура означавања и заштите тајних података, могу се покренути и правни поступци против одговорних лица.
108. **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;
109. **Правовремено, транспарентно и систематизовано поступање у случају инцидента** представља један од основних стубова система заштите тајних података. Овакве процедуре морају бити део Плана заштите тајних података, укључујући и евиденцију свих пријављених инцидената, анализа узрока и извештавање према надлежним институцијама.
110. **Праћење стања сертификата** обухвата праћење издатих сертификата за физичка и правна лица, укључујући проверу ваљаности сертификата у контексту њиховог приступа тајним подацима.
111. **Прекршај (Прекршајна одговорност)**: Инцидент који није довео до компромитације тајних података, али указује на пропусте у примени прописаних мера заштите.
112. **Прекршај** је безбедносни инцидент који не доводи до губитка, компромитовања или сумње на безбедносни инцидент.

113. **Прекршајни поступци:** Уколико је дошло до прекршаја у смислу неправилног чувања или поступања са тајним подацима, могу се изрећи новчане казне или друге мере као што су упозорење или јавна опомена.
114. **Провера медицинских података** је кључан аспект безбедносне провере јер омогућава процену да ли кандидат има менталне, неуролошке или друге здравствене сметње које могу утицати на његову способност да поуздано, свесно и одговорно рукује тајним подацима и информацијама.
115. **Провера медицинских података** је кључан аспект безбедносне провере јер омогућава процену да ли кандидат има менталне, неуролошке или друге здравствене сметње које могу утицати на његову способност да поуздано, свесно и одговорно рукује тајним подацима и информацијама. Провера медицинских података је неопходна ради заштите националне безбедности, тајних података и стабилности лица које раде са тајним подацима. Неопходно је осигурати да ниједна особа са тешким психофизичким поремећајима не добије приступ тајним подацима јер би то могло довести до озбиљних безбедносних ризика.
116. **Професионална тајна** је податак који професионалац у контакту са клијентом сазна о личном или породичном животу клијента, а што не сме бити доступно другим особама. Професионална тајна у себи садржи лични податак, односно личне податке, који су повезани са правилима струке.
117. **Процедура за означавање и одређивање степена тајности података** представља кључни корак у заштити осетљивих информација, докумената и података, као и очувању интереса Републике Србије. Ова процедура има за циљ да обезбеди безбедност података, уз транспарентност и одговорност органа јавне власти. Као тајни податак може се одредити податак од интереса за Републику Србију чијим би откривањем неовлашћеном лицу настала штета, ако је потреба заштите интереса Републике Србије претежнија од интереса за слободан приступ информацијама од јавног значаја.
118. **Процена околности настанка безбедносног инцидента у раду са тајним подацима**, као и његова правна квалификација, један је од најважнијих корака у обради и одређивању даљег поступања у складу са прописима. У зависности од врсте инцидента, различито ће се реаговати надлежни органи и применити одговарајући правни механизми.
119. **Процена претње за безбедност тајног податка (самопроцена)** - по Закону о тајности података представља безбедносну процену која се примењује у раду са тајним подацима. Процена претње за безбедност тајног податка или самопроцена није само идентификација неправилности, већ и континуиран процес унапређења. Комбинација редовне процене, обуке, технолошких решења, унутрашње контроле и надзора осигурава највиши ниво заштите.
120. **Процена ризика** је одређивање квантитативних и квалитативних вредности ризика који се односе на конкретну ситуацију и признато претње (назива опасност).

121. **Процена утицаја и ризика од инцидента у раду са тајним подацима важан** је корак у разумевању степена угрожавања који је наступио. То подразумева не само процену настанка материјалне штете, већ и потенцијалне последице по националну безбедност, права лица или организацију. Када се процењује да ли је инцидент могао имати међународне импликације, важно је узети у обзир степен осетљивости података, као и могућност да се повреда изазове преко граница.
122. **Рад са правним лицима** односни се на управу и сарадњу са правним лицима код поверљивих набавки, посебно у области индустријске безбедности, који укључују безбедност информација и технологија у производним и сервисним процесима.
123. **Радна тачка за рад са тајним подацима** представља функционални одређени део радног простора унутар органа јавне власти који је посебно организован ради пријема, обраде, приступа и чувања тајних података у органу јавне власти. Радна тачка не представља званично успостављену административну, односно безбедносну зону, већ служи као привремено решење за рад са тајним подацима у контролисаним и безбедним условима, до успостављања зона у складу са Уредбом о посебним мерама физичкотехничке заштите тајних података.
124. **Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
125. **Ревизија и ажурирање -** Ознаке тајности се периодично преиспитују и ревидирају како би се утврдило да ли је потребно задржати, променити или укинути степен тајности, због временског ограничења, престанка тајности утврђивањем датума, наступањем одређеног догађаја и истеком рока.
126. **Регистарски систем** представља уређен систем који мора да буде реализован у складу са прописима и стандардима из области ЗТП.
127. **Релативне сметње** (процена појединачног случаја) - Ово су стања која не морају аутоматски водити дисквалификацији, али могу представљати безбедносни ризик у зависности од тежине, учесталости симптома и начина лечења.
128. **Решење** представља управни акт надлежног органа којим је решена управна ствар која је била предмет управног поступка.
129. **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;
130. **Руковалац тајним податком** је физичко лице или организациона јединица органа јавне власти, који предузима мере заштите тајних података у складу са одредбама овог закона.
131. **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.

132. **Сајбер безбедност** представља примену технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.
133. **Сајбер претња** укључује крађу, шпијунажу, насиље и саботажу свега што је повезано са технологијом, виртуелном стварношћу, рачунарима, уређајима или интернетом.
134. **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“.
135. **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.
136. **Систем мониторинга и ревизије** је систем за праћење и ревизију који осигурава да се све мере заштите примењују на адекватан начин.
137. **Скривање података** – Лице намерно или ненамерно не пријави све релевантне информације у сврху вршења безбедносне провере (непријављивање контаката са страним држављанима, скривање радног или криминалног досијеа,скривање медицинских података, лажирање информација о образовању..).
138. **Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије.
139. **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;
140. **Страни утицај** – Чести контакти или породичне везе са страним држављанима који се могу сматрати безбедносним ризиком.
141. **Стручни надзор у систему заштите тајних података** представља процес стручне процене и верификације примене Закона о тајности података код органа јавне власти, са циљем осигурања усклађености прописа и ефикасности мера заштите. Овај процес омогућава идентификацију потенцијалних ризика и слабости, пружајући стручне препоруке за унапређење система заштите тајних података.
142. **Судски поступци -** Ако се утврди да је поступак означавања или обраде података био незаконит, могу се покренути цивилни поступци, где се може захтевати одговорност за штету коју су органи јавне власти или њихови запослени нанели.
143. **Security breaches/кршење безбедности** представља неовлашћени приступ информацијама на мрежама, серверима или уређајима,

заобилажење сигурности на тим системима, што на крају резултира отицањем или компромитацијом података.

144. **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.
145. **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.
146. **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.
147. **Тајни податак означен степеном тајности "ПОВЕРЉИВО"** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по интересе Републике Србије.
148. **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.
149. **Тајност** је својство које значи да податак није доступан неовлашћеним лицима.
150. **Техничка заштита** је обезбеђење лица и имовине које се врши техничким средствима и уређајима, њиховим планирањем, пројектовањем, уградњом и одржавањем.
151. **Техничке мере заштите** представљају обезбеђење и заштиту података и информација и других елемената информационо-комуникационог система, који се остварују применом посебних техничко-технолошких процеса рада и/или спровођењем физичко-манипулативних мера заштите у било којој процедури у оквиру рада ИКТ система.
152. **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 информационо-телекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера крипто-заштите.
153. **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.
154. **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.

155. **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).
156. **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.
157. **Унутрашња контрола** је процес установљен и спровођен од стране руководиоца органа јавне власти, организационе јединице или овлашћеног појединца.
158. **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.
159. **Усаглашеност са стандардима безбедности** представља обавезу органа да се усагласи са националним и међународним стандардима у области информационе безбедности, посебно у области безбедности ИТ система који обрађују тајне податке.
160. **Физичка безбедност/сигурност** представља примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима се налазе или чувају штићени подаци (информације) које захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.
161. **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;
162. **Физичко-техничка заштита** је обезбеђење лица и имовине применом физичке заштите и коришћењем средстава техничке заштите.
163. **Финансијска нестабилност** – Велики дугови, лоша финансијска ситуација или нерегуларно пословање, покретање ликвидације односно стечаја правних лица.
164. **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.
165. **Шифра** је пресликавање (трансформација, правило) којим се тајна порука пресликава у неразумљив низ знакова (слова, бројеве...)
166. **Шпијун** - (ухода, доушник, достављач, потказивач, вребач, жбир...)

167. **Шпијунажа** је прикривена или недозвољена пракса шпијунирања за потребе стране владе, организације, ентитета или особе ради добијања поверљивих информација ради војне, политичке, стратешке или финансијске користи.
168. **Штета** је нарушавање интереса Републике Србије настало као последица неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последица друге радње обраде тајних података и страних тајних података.
169. **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

- Одлука о одређивању тајних података у органу јавне власти
- Одлука о одређивању руковаоца тајним подацима
- Одлука о одређивању унутрашње контроле у органу јавне власти
- Листа „Потребно да зна“
- Листа „Потребно поделити са“
- План заштите података за вандредне и хитне случајеве
- Упутство за рад са тајним подацима

Обрасци и упутство за попуњавање безбедносног упитника

- Образац безбедносног упитника за физичка лица
- Образац безбедносног упитника за правна лица
- Упутство за попуњавање безбедносног упитника
- Изјава

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

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

Модели одлука

- Модел одлуке о овлашћеном лицу за одређивање тајности података
- Модел одлуке о одређивању Административне зоне
- Модел одлуке о одређивању Безбедносне зоне
- Модел одлуке о промени степена тајности
- Модел одлуке о опозиву тајности – периодична процена
- Модел одлуке о престанку тајности истеком рока
- Модел извештаја приликом достављања извештаја о раду са тајним подацима
- Модел Акта о информационој безбедности
- Евиденције за рад са тајним подацима

Модели образаца

- Образац безбедносне напомене приликом достављања тајног податка другој држави или међународној организацији
- Образац о копији документа
- Образац о означавању докумената који садржи тајне податке степена тајности ДТ, СП, П и И
- 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 (SEENSA), као и у оквиру Иницијативе „6S'' 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.

Издавач
Институт за политичке студије, Београд
Канцеларија Савета за националну безбедност и заштиту тајних података.
ISBN 978-86-7419-417-1.