Предраг Обрадовић

www.nsa.gov.rs

ПОСЕБНЕ МЕРЕ ФИЗИЧКО-ТЕХНИЧКЕ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

– СКРИПТА –

Београд, 2024. година

НАПОМЕНЕ

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

Ова скрипта је креирана како би корисницима тајних података помогла да боље спознају и приближе тему која се односи на Посебне мере физичко-техничке заштите и представља основ за даље усавршавање.
Циљ овог радног материјала намењен је подизању безбедносне свести и културе, а у сврху заштите националне безбедности Републике Србије.

САДРЖАЈ:

УВОДНА РАЗМАТРАЊА

МЕЂУНАРОДНИ СПОРАЗУМИ

Ратификовани међународни споразуми сматрају се делом националног законодавства.

Република Србија је закључила 16 споразума са 14 држава и 2. међународне организације у области размене и заштите тајних података и то са:

Мађарска – потписан 2023. г. (ратификован)

Велико Војводство Луксембург - потписан 2020. г. (ратификован)

Република Француска - потписан 2018. г. (ратификован)

Република Кипар - потписан 2017. г. (ратификован)

Румунија - потписан 2017. г. (ратификован)

Република Пољска - потписан 2015. г. (ратификован)

Руска Федерација - потписан 2014. г. (ратификован)

Краљевина Шпанија – потписан 2014. г. (ратификован)

Република Северна Македонија - потписан 2014. г. (ратификован)

Босна и Херцеговина - потписан 2013. г. (ратификован)

Република Словенија- потписан 2013. г. (ратификован)

Чешка Република - потписан 2013. г. (ратификован)

Република Бугарска – потписан 2011. г. (ратификован)

Словачка Република - потписан 2011. г. (ратификован)

Европска Унија – потписан 2011. г. (ратификован)

НАТО– потписан 2011. г. (ратификован)

ПРОПИСИ КОЈИ СУ ПОВЕЗАНИ СА ФИЗИЧКО-ТЕХНИЧКОМ ЗАШТИТОМ

Прописи који уређују рад са тајним подацима

- ✓ Закон о тајности података („Службени гласник РС“, број 104/09)
- ✓ Уредба о посебним мерама физичко-техничке заштите тајних података („Службени гласник РС“, број 97/2011)
- ✓ Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС“, број 53/2011

Прописи који уређују информациону безбедност

- ✓ Закон о информационој безбедности („Службени гласник РС“, број 6/2016, 94/2017 и 77/2019)
- ✓ Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја („Службени гласник РС“, број 94/2016)

Остали прописи

- ✓ Закон о заштити од пожара („Службени гласник РС“, број 111/2009 и 20/2015, 87/2018 и 87/2018-др. закони)
- ✓ Уредба о одређивању послова безбедносне заштите одређених лица и објеката („Службени гласник РС“, број 72/2010 и 64/2013)
- ✓ Закон о детективској делтности („Службени гласник РС“, број 104/2013 и 87/2018)
- ✓ Правилник о просторно-техничким условима за обављање детективске делатности („Службени гласник РС“, број 37/2019)
- ✓ Закон о Народној банци Србије („Службени гласник РС“, број 72/2003, 55/2004, 85/2005 - др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018)
- ✓ Закон о банкама („Службени гласник РС“, број 107/2005, 91/2010 и 14/2015)
- ✓ Закон о приватном обезбеђењу („Службени гласник РС“, број 104/2013, 42/2015 и 87/2018)
- ✓ Уредба о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама („Службени гласник РС“, број 9/2021)
- ✓ Правилник о начину вршења послова техничке заштите и коришћења техничких средстава („Службени гласник РС“, број 91/2019)

ФИЗИЧКА БЕЗБЕДНОСТ

Физичка безбедност подразумева примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима се налазе или чувају тајни подаци које захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења. Физичка безбедност у суштини представља комбинацију безбедносних процедура и техничких стандарда који се заснивају на препорукама, процени и пракси.

КРИТЕРИЈУМИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Орган јавне власти, у складу са Законом о тајности података и прописима донетим на основу овог закона, успоставља систем поступака и мера заштите тајних података према следећим критеријумима:

1)степену тајности[1];
2)природи документа у коме је садржан тајни податак[2];
3)процени претње за безбедност тајног податка[3].

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 едукација за рад са тајним подацима у органу јавне власти
10. Успоставље 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

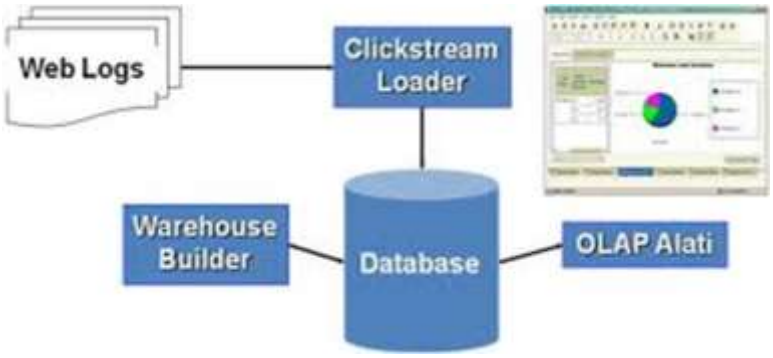
[1] Нпр: није исто да ли се ради о тајном податку степена тајности „ИНТЕРНО“ или је у питању тајни податак степена тајности „ПОВЕРЉИВО“, „СТРОГО ПОВЕРЉИВО“ или „ДРЖАВНА ТАЈНА“.
[2] Нпр: није исто да ли је носач података папир или се тајни податак налази у еклектронском или неком другом облику.
[3] Нпр: није исто да ли се објекат у коме се чувају тајни подаци налази негде на ауто-путу где је брисан простор или је уз неку полицијску станицу где се у већ примењене одређене мере физичко-техничке заштите.

ОРГАНИЗАЦИЈА

- **Руковалац тајним подацима**
- **Одлука о одређивању ТП**
- **Листа „Потребно да зна“[4]**
- **План рада са тајним подацима**
- **План за ванредне и хитне ситуације**
- **Мере заштите тајних података**
- **ИКТ системи (Акт о безбедности ИКТ система од посебног значја)**
- **Остало...**

Аспекти заштите података

- Регистарски систем
- Персоналну безбедност
- Административну безбедност
- **Физичку и техничку безбедност**
- Информатичку безбедност
- Индустријску безбедност (поверљиве набавке везане за државу)



[4] Први кораци у имплементцији Закона о тајности података у органу јавне власти подразумевају доношење Одлуке о одређивању тајних података, Одлуку о одређивању руковаоца тајним подацима и Листу „Потребно да зна“, као и да ли постоји Одлука о одређивању унутрашње контроле.

О СИСТЕМУ ФИЗИЧКО-ТЕХНИЧКОГ ОБЕЗБЕЂЕЊА

Систем ФТО подразумева физичко, техничко и противпожарно обезбеђење, заштиту на раду, послове одбране и цивилне заштите, мере које се предузимају на плану благовременог спречавања зараза и епидемија, као и управљање и руковођење кризним ситуацијама на нивоу заштићеног објекта.
Основни задатак система ФТО предузећа је обезбеђење имовине и пословање предузећа и заштита лица.

ОБЛИЦИ ОБЕЗБЕЂЕЊА

- ФИЗИЧКО – ангажовање лица на пословима ФТО;
- ТЕХНИЧКО, које подразумева:
  - **механичко** – применом направа и уређаја који омогућавају заштиту одређеног објекта;
  - **електронско** – коришћење уређаја који најављују или спречавју приступ у затворени простор или улаз у објекат под заштитом.

Физичко обезбеђење се може спроводити на четири основна начина:

- на улазно-излазним капијама;
- формирањем стражарских (чуварских) места на угроженим или значајним деловима предузећа;
- обилажењем круга предузећа или одређених његових делова – патрола;
- комбинацијом два или више наведених начина.

Физичка заштита - је обезбеђивање активношћу физичких лица - непосредних извршилаца службе ФТО, без претежне употребе техничких средстава, са физичком снагом, мерама и средствима принуде и физичке заштите објеката, имовине и лица у транспорту од уништавања, оштећења, крађе, повреда физичког и психичког интегритета, приватности и личних слобода и права, као и других облика угрожавања.

Врсте физичке заштите

- **Спољно обезбеђење** – подразумева стражарску службу, пратњу вредности и појачану патролну делатност у непосредној околини предузећа;
- **Унутрашње обезбеђење** – подразумева непосредну заштиту објеката, постројења, уређаја, опреме, инсталација и лица која бораве у предузећу; преглед и контролу алармних и других безбедносних уређаја у објекту; обезбеђивање улаза у предузеће и режима кретања и боравка свих лица у њему; контрола пропусница или других личних докумената радника предузећа и издавање сталних или привремених пропусница; преглед транспортних и других возила која улазе у предузеће; преглед поштанских и других пошиљки пре уношења у предузеће.

На основу горе наведеног долазимо до закључка да облици угрожавања безбедности неког штићеног објекта могу бити:

1. **Унутрашњи** (настали изнутра) – деловањем запослених или привремено ангажованих лица тзв. инсајдери;
2. **Спољни** (иницирани и настали споља) – деловањем лица изван предузећа;
3. **Комбиновани** (комбинованог порекла).

Техничка заштита – је стварање техничких услова за спречавање противправних радњи и непосредна употреба техничких средстава за обезбеђење објекта и имовине, ствари и лица у транспорту.

Под системом техничке заштите подразумевају се:

а) системи за физичко спречавање недопуштеног приступа објекту:

- специјалне ограде; рампе; барикаде; противпровална врата и други механички или електромеханички системи техничке заштите;
- све врсте брава са серијским бројем или кодом;
- непробојна стакла и сличне грађевинске конструкције;
- опрема за похрањивање и чување предмета и докумената (касе, трезори и слично).

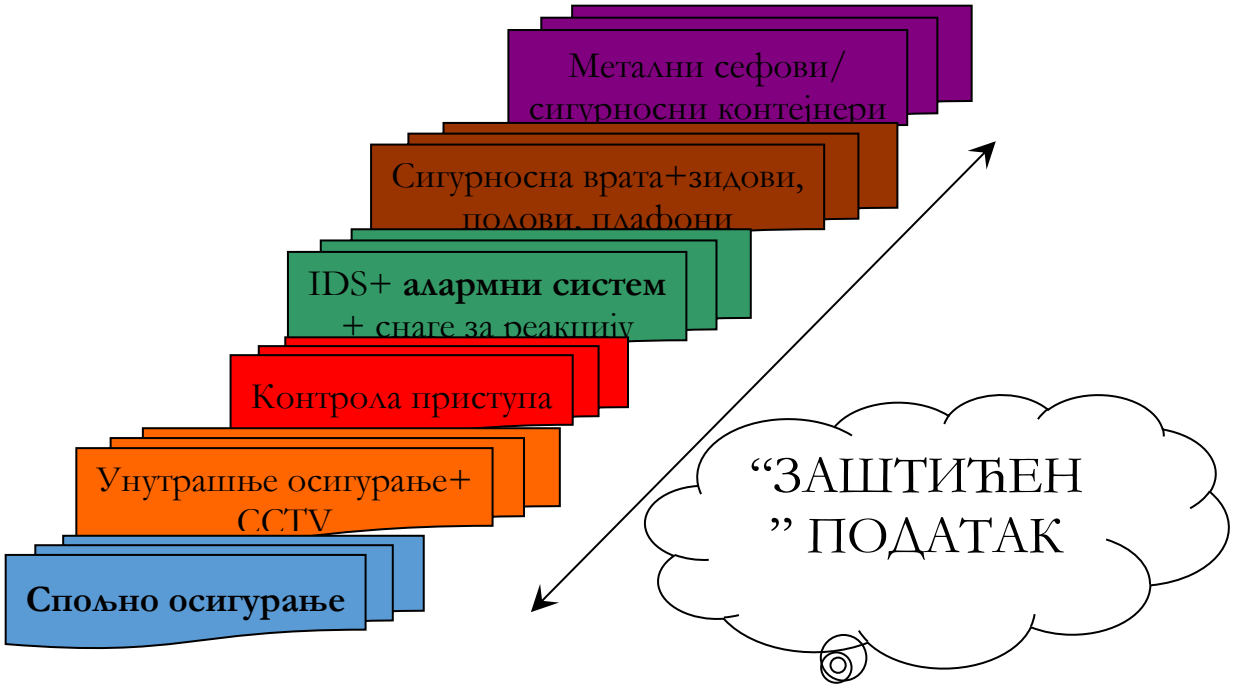
б) електронски безбедносни системи:

- алармни противпровални системи;
- систем затворене телевизије;
- системи за контролу приступа;
- системи за контролу обиласка објекта;
- противпожарни системи;
- остали електронски системи у функцији заштите имовине и лица.

Конкретни ефекти техничке заштите су:

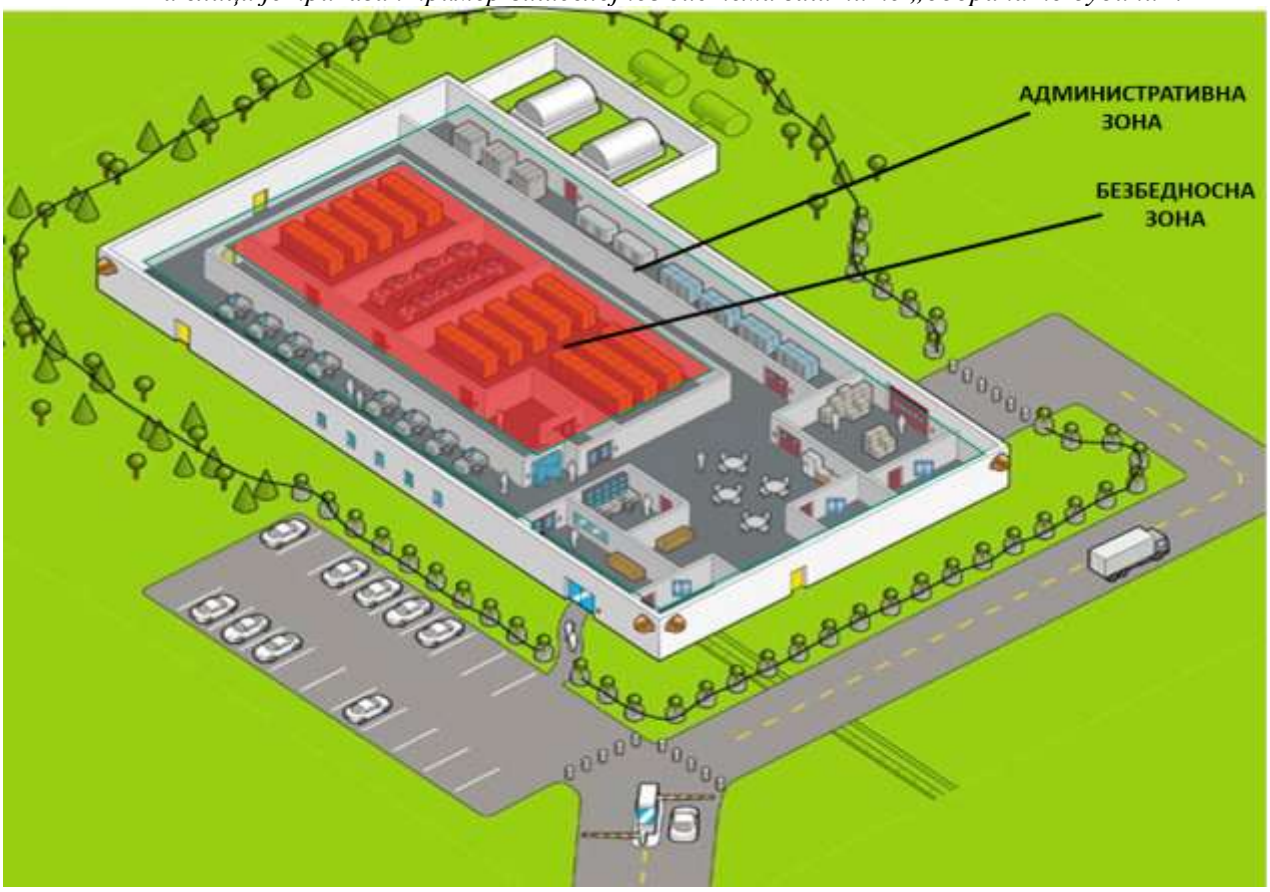
- **Спречавање** уласка у рестриктивни простор или просторије;
- **Детекција** (алармирање) неовлашћењног приступа;
- **Процена** догађаја;
- **Неутрализација** појаве (интервенција службе ФТО или полиције).

ВИШЕСЛОЈНИ СИСТЕМ ЗАШТИТЕ-ОДБРАНА ПО ДУБИНИ



За заштиту ТП примењује се вишеслојни систем заштите „одбрана по дубини“, уз коришћење одговарајуће комбинације комплементарних мера физичког и техничког обезбеђења које пружају степен заштите у складу са значајем и осетљивошћу тајног података
Одбрана по дубини треба да буде процес који је координиран са другим мерама безбедности (персоналном, административном безбедношћу и информационом гаранцијом).

На слици је приказан пример вишеслојног система заштите „одбрана по дубини“.



Плафони, зидови и подови

Плафони, зидови и подови морају бити израђени од армираног бетона или чврстог незапаљивог материјала. У случају да су просторије међусобно повезане размаком између плафона и крова, морају бити одвојени чврстим незапаљивим материјалом.

Заштита од директног увида у просторију

Ако се просторија/соба у којој се налазе штићени подаци може видети споља када су врата отворена, преграде или завесе морају бити инсталиране, како би се онемогућио директан увид споља у просторију у којој се налазе штићени подаци.

Улаз

У принципу мора постојати само један улаз.
Расвета (ноћна светла) на улазу/излазу врата мора да функционише чак и у случају нестанка струје.
У случају да није могуће унети/изнети опрему и инструменте на тај улаз, може се направити улаз за отпрему/пријем.
По потреби могу постојати и врата за случај опасности која се могу отворити само изнутра.

Врата и браве

Врата за улаз, улаз за отпрему/пријем или излаз у случају опасности морају бити челичнау принципу. Код двокрилних врата на спојним деловима морају бити астрагали (конвексна лајсна или дрвена трака преко површине или преградне плоче, обично полукружног попречног пресека). Уколико је потребно поставити прозоре – морају бити затворени са спољним или унутрашњим металним решеткама.
Просторија се не сме видети кроз прозоре.
Улазна врата и врата за отпрему/пријем морају бити двоструко закључана са 3 механичке комбиноване браве (више од 1000 комбинација) и бравом на кључ.
Као алтернативна мера, међутим, може се користити и дигитални уређај за закључавање као нпр уређај за биометријску аутентификацију уместо механичке комбиноване браве.
Механизам за евакуацију у случају ванредних ситација мора бити инсталиран, тако да се може отварати само изнутра.

Прозори

Прозор се у принципу не сме инсталирати.
Када је неизбежна уградња прозора, они морају бити ограничени на минимум и опремљени гвозденим шипкама пречника 13мм или више и интервалима од 10 цм или више, у складу са СРПС ЕН Стандардима.
Прозорско стакло мора бити непрозирно са слојем жичане мреже или једноставно непрозирно, са заштитом од провале.

Отвори/вентилација/канал

Да бисте спречили улазак, осматрање или прислушкивање, канале, плафонске прозоре, одводе, тунели и остали отвори морају бити затворени жичаном мрежом или гвозденим шипкама пречника од 13 mm или више, са интервалима мањим од 10 cm, у складу са SRPS EN стандардима.

Алармни систем

Мора постојати аутоматски алармни систем који детектује отварање/затварање врата и неовлашћене упаде.
Алармни систем мора бити директно повезан са сигурносним контролним центром и тако подешен, да функционише и у случају нестанка електричне енергије.
Повезивање алармног система (ожичење) се не сме лако прекинути, тако да се систем мора алармира ти када се искључи електрична енергија или прекине ожичење.

Периметар

Периметар се мора поставити на око објектата у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.
Према околностима, потребна је ограда висине од 2 метра или више, прекривена бодљикавом жицом или сензорима који регују на контакт. Ова ограда би требала бити или на бетонским армираним или на челичним стубовима.
Периметарска ограда мора бити постављена око сигурносних објеката или читавог простора укључујући објекте.

Периферне контролне области

Да би се спречио неовлашћени приступ безбедносним објектима, изван периметра, периферне контролне области морају бити одређене и приступ тим подручјима је потребно контролисан.

Сигурносни контејнери/КАСЕ

Тајни подаци морају се складиштити у следећим сигурносним касама/контејнерима у зависности од степена тајности:

- за ДРЖАВНУ ТАЈНУ (ДТ), каса/сеф који се закључава са три положаја точкића, комбинована брава,
- за СТРОГО ПОВЕРЉИВО (СП), челична каса/сеф која се закључава са комбинованом бравом,
- за ПОВЕРЉИВО (П), челична кутија која се може закључати са комбинованом бравом за бирање; и
- за ИНТЕРНО (И), челичну кутију која се може закључати.

ЗАКОН О ТАЈНОСТИ ПОДАТАКА

У складу са чл. 6. Закона о тајности података тајни подаци се чувају и користе у складу са мерама заштите које су прописане овим законом, прописом донесеним на основу овог закона и међународним споразумом.
Лице које користи тајни податак или лице које се упознало са његовом садржином дужно је да тај податак чува без обзира на начин на који је за такав податак сазнало.

Врсте мера заштите

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. Чланом 31. Закона о тајности података одређено је да ОЈВ примењеује опште и посебне мере заштите у складу са законом и прописом донетим на основу закона, ради заштите тајних података који се налазе у његовом поседу.

Опште мере заштите тајних података у складу са чл. 32. ст. 2. т. 8. Закона о тајности података обухватају мере физичко-техничке заштите тајног податка, укључујући и уградњу и постављање техничких средстава заштите, утврђивање безбедносне зоне и заштиту ван безбедносне зоне;

Посебне мере заштите тајних података које се односе на посебне мере физичко-техничке заштите тајних података прописане су Уредбом о посебним мерама физичко-техничке заштите тајних података.

ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

УРЕДБА О БЛИЖЕМ УРЕЂЕЊУ МЕРА ЗАШТИТЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

На основу Закона о информационој безбедности донета је Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, где је чланом 13. одређена физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему.

Оператор ИКТ система дужан је да спречи неовлашћен физички приступ објектима, просторима, просторијама односно безбедносним зонама у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему.

У случају када посебним прописима није предвиђена обавеза успостављања безбедносних зона, оператор ИКТ система може да предвиди мере физичко-техничке заштите просторија у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему, као што су уградња алармних уређаја, контрола уласка уз обавезно ношење видљиве идентификације за све време боравка и друге мере којима се обезбеђује физичко-техничка заштита.

Оператор ИКТ система дужан је да предвиди и примени мере физичке заштите у случају елементарних непогода, злонамерних напада, несрећа или намерног уништавања објеката, просторија, средстава и докумената ИКТ система.

УРЕДБА О ОДРЕЂИВАЊУ ПОСЛОВА БЕЗБЕДНОСНЕ ЗАШТИТЕ ОДРЕЂЕНИХ ЛИЦА И ОБЈЕКАТА

Под пословима безбедносне заштите, у смислу ове уредбе подразумевају се:

– мере контраобавештајне заштите;
– превентивно-безбедносне мере;
– мере превентивно техничке заштите;
– мере физичке заштите;
– мере превентивно медицинске заштите.

Мере превентивно-техничке заштите представљају скуп послова, задатака и активности који се предузимају ради откривања и уклањања минско-експлозивних, запаљивих, радиоактивних и других опасних материја, установљавања и отклањања техничких неисправности на уређајима и инсталацијама и спречавања тајног или насилног уласка у објекте и просторије, као и функционисања заштићеног система веза.

Мере физичке заштите представљају скуп послова, задатака и активности који се предузимају ради обезбеђења одређених лица и објеката и обухватају:
– непосредну физичку заштиту одређених лица;
– физичку заштиту одређених објеката које лице користи стално или повремено;
– физичка заштита безбедносно осетљивих тачака на правцима кретања;
– регулисање саобраћаја и обезбеђење кретања возила под пратњом.

Послове безбедносне заштите одређених лица и објеката у земљи и иностранству непосредно врше органи Републике Србије који су надлежни за безбедносну заштиту.

ЗАКОН О НАРОДНОЈ БАНЦИ СРБИЈЕ

У складу са чланом 82. Закона о Народној банци Србије организација рада Народне банке Србије ближе се уређује Статутом и унутрашњим општим актима Народне банке Србије, а нарочито:

1) унутрашња организација Народне банке Србије и систематизација радних места у Народној банци Србије;

2) права, обавезе и одговорности руководилаца;
3) права, обавезе и одговорности запослених у обављању послова и задатака;
4) зараде и накнаде функционера Народне банке Србије и запослених;
5) **заштита података означених одређеним степеном тајности (у даљем тексту: тајни подаци) и безбедност информацијама у Народној банци Србије;**
6) управљање документима у Народној банци Србије.

Такође чланом 86а наведеног закона, као тајни подаци настали у пословању Народне банке Србије нарочито се одређују подаци који се односе на:

1) управљање девизним резервама;
2) преговоре са организацијама и институцијама из члана 11. овог закона;
3) издавање новчаница и кованог новца и управљање токовима готовине;
4) појединачне податке и показатеље пословања субјеката над којима Народна банка Србије врши контролу, односно надзорну функцију.

Као тајни подаци настали у пословању Народне банке Србије могу се законом или унутрашњим општим актом Народне банке Србије одредити и други подаци чијим би откривањем неовлашћеним лицима могла наступити штета по остваривање циљева и обављање функција Народне банке Србије.

ЗАКОН О БАНКАМА

У Закону о банкама, чланом 9б који се односи на тајност података, одређено је да подаци који се односе на контролу бонитета и законитости пословања банке и на реструктуирање банке, као и документи који садрже такве податке, а које запослени у Народној банци Србије, агенцији надлежној за осигурање депозита (у даљем тексту: Агенција), министарству надлежном за послове финансија или банци и друга лица на било који начин сазнају у обављању послова у вези са овом контролом, односно реструктурирањем – одређују се и штите се као тајни подаци са ознаком степена тајности „СТРОГО ПОВЕРЉИВО“, „ПОВЕРЉИВО“ или „ИНЕТРНО“, у складу са законом којим се уређује тајност података.

ЗАКОН О ПРИВАТНОМ ОБЕЗБЕЂЕЊУ

Законом о приватном обезбеђења уређују се обавезно обезбеђење и заштита одређених објеката, послови и рад правних и физичких лица у области приватног обезбеђења, услови за њихово лиценцирање, начин вршења послова и остваривање надзора над њиховим радом.
Неки од појмова који се користе у овом закону имају следеће значење:

17) **самозаштитна делатност** је делатност обезбеђења лица, имовине и пословања које организација обавља за сопствене потребе;

19) **штићени простор** је објекат или простор на којем се врше услуге обезбеђења;

20) **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;

21) **физичко-техничка заштита** је обезбеђење лица и имовине применом физичке заштите и коришћењем средстава техничке заштите;

22) **техничка заштита** је обезбеђење лица и имовине које се врши техничким средствима и уређајима, њиховим планирањем, пројектовањем, уградњом и одржавањем.

Минималне техничке услове код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама (поште, штедионице, мењачнице, трезори и др) у којима се, у складу са овим законом, обављају послови приватног обезбеђења утврђује Влада.
Ближи начин вршења послова техничке заштите и коришћења техничких средстава утврђује министар.

УРЕДБА О МИНИМАЛНИМ ТЕХНИЧКИМ УСЛОВИМА КОД ОБАВЕЗНЕ УГРАДЊЕ СИСТЕМА ТЕХНИЧКЕ ЗАШТИТЕ У БАНКАМА И ДРУГИМ ФИНАНСИЈСКИМ ОРГАНИЗАЦИЈАМА

Уредбом о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама утврђују се минимални технички услови код обавезне уградње система техничке заштите у банкама, њиховим пословницама, платним институцијама, пословницама јавног поштанског оператора и другим финансијским организацијама.

Одредбе ове уредбе не примењују се на пословнице банака и финансијских организација које се налазе у објектима које обезбеђују организационе јединице војске, полиције или правосудне страже или код којих су минимални услови за техничку заштиту уређени посебним законом или прописом донетим на основу закона.

Техничка заштита се у смислу ове уредбе спроводи у складу са законом на основу акта о процени ризика у заштити лица, имовине и пословања, који се периодично ажурира у складу са потребама и новим околностима, а најмање на сваке три године.

Банке и финансијске организације код којих на основу акта о процени ризика постоји **изразито велики ниво ризика,** дужни су да користе уређаје, опрему и системе техничке заштите, који минимално омогућавају:

1) сигнализацију неовлашћеног уласка у штићени простор и дојаву контролном центру,
2) праћење кретања у штићеном простору и појединачно штићеним просторијама (контрола приступа и видео обезбеђење) уз видео запис, који се чува најмање 30 дана,
3) заштиту појединачних вредности помоћу система електрохемијске заштите (кофери, контејнери, касе, трезори и др.),
4) интегрисану заштиту с најмање једним локалним надзорним местом (контролна соба) и системом везе са службеницима обезбеђења на штићеном објекту,
5) писане процедуре за случајеве наступања ризика.

Банке и финансијске организације код којих на основу акта о процени ризика постоји **велики ниво ризика**, дужни су да користе уређаје, опрему и системе техничке заштите, који минимално омогућавају:

1) сигнализацију неовлашћеног уласка у штићени простор и дојаву контролном центру,
2) праћење кретања у штићеном простору (контрола пролаза и видео обезбеђење) уз видео запис, који се чува најмање 30 дана,
3) интегралну заштиту с најмање једним локалним надзорним местом (контролна соба) и системом везе са контролним центром.

Банке и финансијске организације код којих на основу акта о процени ризика постоји **умерено велики ниво ризика**, дужне су да користе уређаје, опрему и системе техничке заштите, који минимално омогућавају:

1) праћење кретања око штићеног простора (видео обезбеђење) уз видео запис, који се чува најмање 30 дана,
2) сигнализирање неовлашћеног приступа у штићени простор и дојаву контролном центру.

Банке и финансијске организације код којих на основу акта о процени ризика постоји **мали или занемарљив ниво ризика**, дужне су да користе системе техничке заштите, који минимално омогућавају:

1) физичко спречавање недозвољеног уласка лица у штићени објекат и простор који му припада,
2) сигнализирање неовлашћеног приступа у штићени простор и дојаву контролном центру.

- Правилник о начину вршења послова техничке заштите и коришћења техничких средстава -

Средства и уређаји техничке заштите у смислу Правилника о начину вршења послова техничке заштите и коришћења техничких средстава су:

1) механичка средства, елементи, уређаји или конструкције које за рад не користе електричну енергију, а намењени су за физичко спречавање недозвољеног уласка лица или предмета у штићени објекат и простор који му припада, односно за заштиту лица, имовине и пословања (противбалистичка стакла, противпровалне фолије за стаклене површине, трокраке баријере, сигурносне кабине, опрема за смештај, чување и пренос вредности, и др.);

2) електронска и електро-механичка средства и уређаји (противпровални и противпрепадни алармни системи са активним и пасивним јављачима, уређаји и опрема за контролу приступа, системи којима се обавља стални надзор над штићеним објектом с једног места, интегрални системи заштите са најмање једним локалним надзорним местом, уређаји и опрема видео обезбеђења, и др.);

3) противдиверзиона и противсаботажна средства и уређаји (детектори метала, детектори експлозива и других опасних материја, рендгенски уређаји за преглед пртљага, огледала за преглед подножја возила, уређаји и опрема за електрохемијску заштиту новца и других вредности, и др.);

4) средства и уређаји за глобално позиционирање лица и покретних добара (ГПС сателитско праћење) који су намењени за заштиту лица, имовине и пословања или су у функцији њихове заштите.

Системи техничке заштите, у смислу овог правилника, састоје се од:

1) средства и уређаји техничке заштите на штићеном објекту или простору (разни детектори алармних стања, камере видео обезбеђења и други периферни уређаји и средства техничке заштите);

2) спојених путева за пренос сигнала алармних стања, видео обезбеђења и пренос података између елемената система техничке заштите;

3) једне или више контролних соба или техничких центара на објекту заштите или спојеним путевима, ако се планира њихово успостављање;

4) контролног центра.

С*редствима, уређајима и системима техничке заштите,* може се вршити мониторинг на даљину (из контролног центра, контролне собе или техничког центра).

Противпровални системи планирају се, пројектују и уграђују на начин да се детектори смештају на места која покривају улазе и друге идентификоване критичне тачке штићеног објекта (прозори, стаклени зидови, рек собе, просторије са вредном робом и др.), односно на опрему или уређаје за чување новца и вредности (касе, сефови, трезори, банкомати и др.), централе, резервна напајања и друге уређаје за дојаву аларма на тешко доступним местима,

каблове заштићене од спољних утицаја и алармне сирене или светла, ако се постављају на видним, а тешко доступним местима.

Противпрепадни системи пројектују се, планирају и уграђују на скривеним али лако доступним местима, тако да службеник обезбеђења или корисник услуга може да их благовремено неометано активира.

Уређаји и средства видео обезбеђења који се користе у техничкој заштити морају задовољавати основне захтеве у смислу квалитета, функционалности, минималне резолуције, функционалности у ноћним условима, као и друге захтеве према плану система техничке заштите, а у складу са важећим техничким стандардима.
Средства и уређаји видео обезбеђења којима се поред мониторинга врши и снимање штићеног објекта или простора морају имати дигитални запис и довољан капацитет меморије за сачињавање записа у трајању од најмање 30 дана, у моду континуираног снимања 24/7/ или у моду снимања детекцијом кретања, а према плану система техничке заштите, да имају могућност преноса података на преносни медијум у формату читљивом на рачунару, уз потврду одговарајућег воденог жига (watermark) у складу са важећим техничким стандардима.

ЗАКОН О ДЕТЕКТИВСКОЈ ДЕЛАТНОСТИ

- Правилник о просторно-техничким условима за обављање детективске делатности-

На основу Закона о детективској делатности донет је Правилник о просторно-техничким условима за обављање детективске делатности. Чл. 3. наведеног правилника одређено је да у пословном простору, правно лице и предузетник за детективску делатност, у складу са прописима о приватном обезбеђењу, треба да обезбеди постављање техничких средстава за контролу приступа (механичких или електронских), као и противпровалног система и да обезбеди енергетски прикључак за непрекидно и алтернативно напајање електричном енергијом. У делу пословног простора намењеном за рад детектива, ради смештаја и чувања предмета у раду и збирки података и других евиденција, мора се налазити **метална каса или сеф**, који треба да буду опремљени сигурносним механичким или нумеричким бравама, које обезбеђују противпровалну сигурност.

УРЕДБА О ПОСЕБНИМ МЕРАМА ФИЗИЧКО-ТЕХНИЧКЕ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

УРЕДБА О ПОСЕБНИМ МЕРАМА ФИЗИЧКО-ТЕХНИЧКЕ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Опремљеност просторија

Просторије у којима се чувају, користе, обрађују и уништавају тајни подаци обезбеђују се противпровалним и противпожарним системом.

Просторија је по правилу опремљена:

1) једним од безбедносних механизама на улазним вратима, са могућношћу евиденције података о уласку у простор (приступним читачем кодова, картица, тастатуре и слично или биометријским системом), како би се приступ таквим просторијама могао ограничити, надзирати и евидентирати;
2) опремом за безбедно чување предмета и докумената;
3) енергетским прикључком на непрекидно и алтернативно (агрегатско) напајање;
4) сигурносним механичким системом за закључавање са ограниченим бројем кључева, без могућности умножавања или томе одговарајућим одвојеним аутоматизованим и мануелним решењима.

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 ИКТ система

Просторије у којима се постављају телефонске централе и друга телекомуникациона опрема за обједињавање целокупног информационо - телекомуникационог 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.

Просторије у којима се постављају сервери и елекомуникациона опрема морају задовољавати **SRPS**, односно одговарајуће **ISO стандарде**.

Опрема за обраду тајних података

Фотокопир апарат, телефакс и другу опрему неопходну за обраду тајних података, може употребљавати само лице које има одговарајући сертификат за приступ тајним подацима. Наведена опрема, има исти степен тајности као и подаци који се обрађују и чувају на њој.

Опрема у којој се чувају тајни подаци

Безбедносно техничка опрема, односно одговарајућа средства техничке заштите у којој се чувају тајни подаци, је:
1) противпожарна метална каса са уграђеном бравом за степен тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО”;
2) канцеларијски или метални ормар за степен тајности „ИНТЕРНО”.

Каса или просторија у којој се та каса налази, опремљене су системом јављања и мора испуњавати одговарајуће **SRPS/EN техничке стандарде**.

Означавање опреме за чување тајних података

Означавање касе, односно ормара, врши се тако што се на њиховој спољној страни у горњем левом углу ставља етикета или налепница прикладне величине са ознаком великог штампаног слова, и то:
1) „ДТ” за степен тајности „ДРЖАВНА ТАЈНА”;
2) „СП” за степен тајности „СТРОГО ПОВЕРЉИВО”;
3) „П” за степен тајности „ПОВЕРЉИВО”;
4) „И” за степен тајности „ИНТЕРНО”.

Ако се у каси чувају тајни подаци различитог степена тајности, ознака тајности мора одговарати највишем степену тајности података који се у њима чувају.

Поступање са кључевима

Са комбинацијом за отварање брава на касама могу бити упознати само запослени које одреди руководилац органа јавне власти.

<u>Комбинације за отварање брава се мењају</u>:

1) одмах након постављања;
2) у случају откривања или сумње у откривање комбинације;
3) периодично, после шест месеци од постављења;
4) након прераспоређивања или престанка радног односа запосленог који је био упознат са постављеном комбинацијом;
5) у другим оправданим случајевима, када то одлучи руководилац органа јавне власти или лице које он овласти.

Писани запис појединачне комбинације за отварање брава и кључеви за браву чувају се у непровидној коверти, у каси, код руководиоца органа јавне власти или лица које он овласти.

Простори са рестриктивним приступом

Руководилац органа јавне власти, на основу процене могућег нарушавања безбедности тајних података одређује административну зону, безбедносне зоне, одговарајућу безбедносно техничку опрему, као и мере обезбеђења безбедносних зона.
Безбедносне зоне могу бити I или II степена.

Администартивна зона

У административној зони обрађују се и чувају тајни подаци степена тајности „ИНТЕРНО".
За административну зону одређује се простор или просторија која се може надзирати (улаз и излаз и кретање лица и возила).
На улазу у административну зону мора бити истакнуто обавештење о надзору приступа и кретању у њој.

Безбедносна зона

У безбедносној зони I или II степена обрађују се и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО".
Безбедносне зоне, по правилу, морају бити видно означене натписом „БЕЗБЕДНОСНА ЗОНА I СТЕПЕНА", односно „БЕЗБЕДНОСНА ЗОНА II СТЕПЕНА", уз додатна обавештења повезана са безбедносним мерама које се спроводе у тој зони.
Изузетно, када то захтевају посебне оправдане околности, руководилац органа јавне власти може одредити да се безбедносне зоне не означавају на начин предвиђен уредбом.

Безбедносна зона I степена

Самим уласком у ову зону сматра се да је остварен приступ тајним подацима.

Посебне физичко-техничке мере заштите тајних података у безбедносној зони I степена, обухватају:

1) надзор којим се обезбеђује потпуна контрола и евиденција улаза и излаза;
2) вођење евиденције о приступу тајним подацима;
3) забрану уношења механичких, електронских и магнетно-оптичких средстава и делова средстава, којима би се могао неовлашћено снимити, однети или пренети тајни податак;
4) непосредно и непрекидно физичко обезбеђење, које се, у складу са проценом, може допунити или заменити електронским системом за противпровално обезбеђење, чији је алармни систем повезан са одговарајућом јединицом за интервенцију;
5) непрекидно техничко обезбеђење са резервним напајањем, којим се остварује потпуни надзор безбедносне зоне, као замена непрекидном физичком обезбеђењу;
6) прегледање простора или просторије по завршеном радном времену.

Простор или просторије безбедносне зоне I степена морају испуњавати одговарајуће SRPS/EN техничке стандарде.

Безбедносна зона II степена

Улазак и кретање у овој зони не сматра се приступом тајним подацима.

Посебне физичко-техничке мере заштите тајних података у безбедносној зони II степена, обухватају:

1) надзор којим се обезбеђује потпуна контрола и евиденција улаза и излаза;
2) организацију рада која обезбеђује запосленима приступ само оним тајним подацима који су им потребни за извршавање радних задатака и до оног степена тајности за који имају сертификат;
3) надзор који обезбеђује да друга лица која имају дозволу за приступ тајним подацима улазе у ову зону само у пратњи запосленог;
4) забрану уношења механичких, електронских и магнетно-оптичких средстава и делова средстава, којима би се могао неовлашћено снимити, однети или пренети тајни податак, без одобрења овлашћеног лица;
5) физичко или противпровално обезбеђење простора или просторије, као и њихово повремено прегледање по завршеном радном времену.

Улазак лица у Безбедносну зону

За улазак у безбедносну зону I или II степена запослени у органу јавне власти користи безбедносну пропусницу која може бити у писаној форми или у облику магнетне картице са идентификационим подацима. Приступ зонама мора бити у складу са сертификатом за приступ одговарајућем степену тајних података који запослени поседује.
За улазак другог лица у безбедносну зону издаје се посебна безбедносна пропусница у писаној форми. Друго лице се обавештава да се његово кретање надзире и евидентира и при уласку и кретању у безбедносној зони, мора имати на видљивом месту закачену безбедносну пропусницу.

Безбедносну пропусницу издаје руководилац органа јавне власти или лице које он овласти. О издатим безбедносним пропусницама води се евиденција.

Противприслушни преглед

У свим просторима, односно просторијама безбедносне зоне I или II степена мора бити обављен противприслушни преглед, и то:

1) приликом одређивања безбедносне зоне;
2) код сваког насилног упада или неовлашћеног приступа у зону;
3) после распоређивања на друго радно место које не подразумава приступ тајним подацима или престанка радног односа запосленог који је руковао тајним подацима;
4) после извођења било које врсте грађевинских или радова на телекомуникационој опреми;
5) сваких шест месеци.
Заштита од прислушкивања других простора, односно просторија или информационих и телекомуникационих капацитета путем којих се преносе тајни подаци врши се у складу са проценом.

Преглед врши орган који је, у складу са прописом који уређује одређивање послова безбедносне заштите одређених лица и објеката, надлежан за обављање послова контраобавештајне заштите.

У зависности од процене, могу се спровести и друге мере заштите тајних података, које подразумевају одређивање безбедносног појаса, постављање ограде са осветљењем око објекта и слично.

Обрада тајног података изван безбедносне зоне

Тајни подаци могу се обрађивати изван безбедносних зона, ако је простор или подручје у којем се обрађују физички или технички обезбеђен, а приступ до њега под надзором. Лице које обрађује тајни податак изван безбедносних зона мора имати тајни податак цело време под надзором. По окончаној обради, тајни податак се враћа у безбедносну зону.

Када се тајни податак степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО" мора обрађивати изван простора органа јавне власти, руководилац органа јавне власти или лице које он овласти утврђује мере за заштиту тајног податка које морају бити у складу са мерама заштите прописаним за одговарајућу безбедносну зону.

Свако изношење или уношење тајног податка степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО" изван безбедносне зоне, односно у безбедносну зону се евидентира.

Лице које преузима тајни податак за обраду изван безбедносних зона, потврђује то својеручним потписом.

Припрема за слање тајног податка

Тајни податак означен степеном тајности „ДРЖАВНА ТАЈНА", доставља се на коришћење изван безбедносне зоне у две затворене коверте које морају бити у затвореном коферу, кутији или торби, са затварањем на кључ или са шифрованом комбинацијом.
Тајни податак означен степеном тајности „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО" изван безбедносне зоне, доставља се, по правилу, у две затворене коверте.
Спољна затворена коверта је од тврдог, непровидног, непропусног материјала, на којој је означен орган коме се доставља тајни податак.
Унутрашња затворена коверта, мора имати ознаку степена тајности податка, број и датум акта и податке о примаоцу и пошиљаоцу.

Достављање тајног податка

Овлашћено лице које је одредило степен тајности податка доставља тајни податак кориснику који има сертификат за приступ тајним подацима најмање оног степена тајности податка који се доставља.

Тајни податак се доставља на коришћење кориснику, преко лица које преноси тајне податке (у даљем тексу: курир).
Курир мора поседовати сертификат за приступ тајним подацима одговарајућег степена тајности.
На захтев лица којем предаје или од кога преузима тајни податак, курир је дужан да покаже курирско уверење.
Образац уверења, одштампан је уз ову уредбу и чини њен саставни део као Прилог 2.
Уколико се процени да може доћи до нарушавања безбедности доставе тајног податка, достављање се може обезбедити ангажовањем полицијског службеника или припадника војне полиције, како би се спречио неовлашћени приступ, оштећење или уништење тајног податка.

Достављање тајног податка унутар безбедносне зоне

Тајни податак означен степеном тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО" унутар безбедносне зоне, доставља се на коришћење у затвореној, непровидној коверти, на којој су назначени подаци о примаоцу тог документа.

Достављање тајног податка ван безбедносне зоне

Тајни податак са ознаком степена тајности „ДРЖАВНА ТАЈНА", ван безбедносне зоне, доставља се на коришћење преко најмање два курира, а документ означен степеном тајности „СТРОГО ПОВЕРЉИВО" или „ПОВЕРЉИВО", доставља један курир.

Тајни податак са ознаком степена тајности „ИНТЕРНО" може се достављати преко курира или путем поште, препорученом пошиљком са повратницом. Изузетно, достављање тајних података страној држави или међународној организацији може се вршити и путем дипломатске поште.

На документу којим се тајни податак доставља другој држави или међународној организацији мора се налазити следећа безбедносна напомена:
„Овај документ и сви садржани прилози сматрају се тајним подацима означеним степеном тајности _____ (навести степен тајности), власништво су _____ (навести назив органа јавне власти), и могу се користити само у сврху за коју су достављени. Прималац документа водиће бригу о заштити тајности података садржаних у документу у складу са прописима Републике Србије о заштити тајних података. Не сме се мењати степен тајности означен на овом документу и никоме није дозвољен приступ подацима садржаним у овом документу ако нема сертификат, односно дозволу за приступ тајним подацима степена тајности којим је означен овај документ. Документ и његов садржај не сме се без одобрења Републике Србије објављивати, умножавати, давати на коришћење другом органу или трећој страни, односно користити у друге сврхе осим оних због којих је достављен.
Република Србија задржава право на информисање о коришћењу достављеног документа и података које документ садржи, а прималац документа се обавезује да ће о уништењу документа обавестити Републику Србију."
Ако се страној држави или међународној организацији достављају системи, уређаји и предмети који имају одређени степен тајности, уз њих се доставља и посебан акт који садржи безбедносну напомену из става 1. овог члана.

Пријем тајног податка

Примопредаја тајног податка врши се у посебној просторији коју одреди руководилац органа јавне власти коме се тајни податак доставља на коришћење;
Корисник тајног податка потврђује пријем тог податка потписом на потврди, односно у доставној књизи, уписивањем датума и времена пријема;
Образац потврде, одштампан је уз ову уредбу и чини њен саставни део као Прилог 1.

Чување тајног податка

Тајни податак може се чувати у писаној или електронској форми (магнетни или оптички медиј, дискета, УСБ меморија, смарт картица, компакт диск, микрофилм, видео и аудио запис). Чување и руковање тајним подацима врши се у складу са актом, односно одлуком, којом се уређује чување и руковање тајним подацима.

Актом, односно одлуком, зависно од процене, броја докумената која садрже тајне податке, степена тајности података, непосредног окружења објекта и карактеристика објекта у којем ти подаци настају, чувају или се користе, ширег окружења објекта, као и броја запослених који имају дозволу за приступ тајним подацима, ближе се одређују мере заштите простора, односно просторије, у којем се чувају тајни подаци, ради спречавања од насилног упада или неовлашћеног приступа, употребе или уништавања тајних података.

Акт, односно одлуку, доноси руководилац органа јавне власти у чијем раду настају тајни подаци, односно који чува или користи тајне податке. Наведени акт, односно одлука, ажурира се најмање једном у шест месеци, а ефикасност утврђених мера проверава се најмање једном годишње.

Умножавање, превођење или сачињавање извода тајног податка

Корисник тајног податка степена тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО” може умножити или превести документ, односно сачинити извод из документа, ако постоји:

1) захтев за умножавање, превођење или сачињавање извода тајног податка са предлогом броја примерака;

2) сагласност, по правилу у писаној форми, од стране овлашћеног лица које је одредило степен тајности податка, уз одређивање броја примерака који ће се умножити, превести или броја извода који ће се сачинити.

Број умножених примерака, превода или извода из документа који садржи тајни податак, одређује се по потреби;

Умножавање, превођење или сачињавање извода тајног податка врши лице које има сертификат за приступ тајним подацима, која није мањег степена тајности од степена тајности тог податка;

Мере заштите одређене за оригинални документ примењују се и на умножене примерке, преводе или изводе из тог документа.

Уништавање тајних података

Тајни подаци, копије, радни нацрти, белешке, као и подаци који су физички оштећени и не могу се даље користити, осим тајних података стране државе и међународне организације, уништавају се на начин да се не могу препознати и обновити (хемијским разлагањем, спаљивањем, дробљењем и др).

У складу са наведеним, *руководилац органа јавне власти образује комисију за уништавање тајних података.*

Комисију чине најмање три лица којима је издат сертификат за приступ тајним подацима најмање оног степена тајности података који се уништавају.

О уништавању података, *води се записник, који потписују сви чланови комисије*.

Записник садржи податке о броју и датуму акта којим је одређено уништавање тајног податка броју, датуму и степену тајног податка који се уништава и начину њиховог уништавања. *Записник чува се трајно*.

О уништавању тајних података степена тајности „ДРЖАВНА ТАЈНА”, „СТРОГО ПОВЕРЉИВО” и „ПОВЕРЉИВО”, писаним путем се обавештава овлашћено лице које је одредило степен тајности податка.

На уништавање докумената који садрже тајне податке стране државе или међународне организације примењују се прописи државе или међународне организације у којој је тајни податак настао, односно међународног споразума.

НА КРАЈУ

Продори и компромитовања

Губитак тајног податка или информације, чак и привремен, ван безбедносног подручја, треба сматрати компромитовањем.

Губитак тајног податка или информације, чак и привремен, унутар безбедносног подручја, заједно са оним документма, која се не могу лоцирати, треба сматрати продором, док кривична истрага не покаже другачије.

О сваком продору и компромитовању, потребно је хитно обавестити надлежне полицијске органе или службе безбедности, ради предузимања даљих одговарајућих мера.

Препоруке

Потребно је успоставити технолошке капацитете за обраду и заштиту података, набављањем одређене опреме и имплементацијом одговарајућих стандарда, SRPS/СРПС ISO/IAC 27001, ISO 14001 и слично, односно успостављање ISMS.

Потребно је успоставити систем надлежности да је сасвим јасно ко шта ради и ко за шта одговара. Нпр. **Синергија** - Правници би требали бити носиоци правне проблематике и тумачења прописа, безбедњаци би требали бити носиоци активности документовања одређених догађаја, ИТ служба би требала бити носилац одређених процедура, али све три структуре би требале радити као тим, вођен менаџментом (руководством) организације.

У циљу константног подизања безбедносне свести и културе када су у питању тајни подаци неопходно је успоставити систем едукција на више нивоа.

Резиме

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 информационо - телекомуникационог 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.

Уместо закључка

ЧАРОБНИ ШТАПИЋ ИЛИ ПРИГОДНИ МАГИЈСКИ РИТУАЛ НЕ ПОСТОЈИ...
ИСКУСТВА СА ПРЕТХОДНИХ РАДНИХ МЕСТА СУ ДОБРА, АЛИ НИСУ ДОВОЉНА...

ЧОВЕК

ЈЕ НАЈСЛАБИЈА КАРИКА СВАКОГ СИСТЕМА . . .

ЕДУКУЈТЕ СЕ . . .

ЗАШТИТИМО НАЦИОНАЛНУ БЕЗБЕДНОСТ И ТАЈНЕ ПОДАТКЕ РЕПУБЛИКЕ СРБИЈЕ

ЛИТЕРАТУРА

- Закон о тајности података („Службени гласник РС“, број 104/09)
- Закон о информационој безбедности („Службени гласник РС“, број 6/2016, 94/2017 и 77/2019)
- Закон о Народној банци Србије („Службени гласник РС“, број 72/2003, 55/2004, 85/2005 - др. закон, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – одлука УС и 44/2018)
- Закон о банкама („Службени гласник РС“, број 107/2005, 91/2010 и 14/2015)
- Закон о приватном обезбеђењу („Службени гласник РС“, број 104/2013, 42/2015 и 87/2018)
- Закон о детективској делтности („Службени гласник РС“, број 104/2013 и 87/2018)
- Уредба о посебним мерама физичко-техничке заштите тајних података („Службени гласник РС“, број 97/2011)
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја („Службени гласник РС“, број 94/2016)
- Уредба о одређивању послова безбедносне заштите одређених лица и објеката („Службени гласник РС“, број 72/2010 и 64/2013)
- Уредба о минималним техничким условима код обавезне уградње система техничке заштите у банкама и другим финансијским организацијама („Службени гласник РС“, број 9/2021)
- Правилник о начину вршења послова техничке заштите и коришћења техничких средстава („Службени гласник РС“, број 91/2019)
- Правилник о просторно-техничким условима за обављање детективске делатности („Службени гласник РС“, број 37/2019)
- Проф. др Горан Матић - Систем заштите тајних података података – приручник (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf)
- Проф. др Горан Матић - Основе обраде и заштите података – приручник https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf
- Проф. др Горан Матић - Основи физичко-техничког обезбеђења – приручник за едукацију непосредних извршилаца приватног обезбеђења лица и имовине, *Београд 2006. године*
- Сајт Канцеларије Савета за националну безбедност и заштиту тајних података nsa.gov.rs