# ИНФОРМАЦИОНА БЕЗБЕДНОСТ У ИКТ СИТЕМИМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

– СКРИПТА –

**Проф.др Горан Д. Матић**

**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 информациону безбедност у ИКТ системима за рад са тајним подацима 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

## ПРОПИСИ КОЈИ УРЕЂУЈУ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ

- ✓ 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), нови Закон о ИБ у припреми
- ✓ Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Службени гласник РС“, број 97/2011)
- ✓ Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја („Службени гласник РС“, број 94/2016)
- ✓ Уредба о ближем садржају акта о безбедности ИКТ од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја („Службени гласник РС”, број 94/16)
- ✓ Акциони план за реализацију стратегије развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године („Службени гласник РС”, број 30/18)
- ✓ Уредба о криптобезбедности и заштити од КЕМЗ („Сл. гласник РС", број 57/19)

## ИНФОРМАЦИОНА БЕЗБЕДНОСТ- НАДЛЕЖНОСТИ

- Надлежни орган за безбедносну акредитацију икт система (SAA) – није одређен
- Надлежни орган за информациону безбедност (IAA) – Министарство информисања и телекомуникација
- Надлежни орган за криптобезбедност и КЕМЗ (CAA, CDA И TA) – Министарство одбране

## ПРОБЛЕМИ У ПРАКСИ

- ➢ Орган надлежан за акредитацију ИКТ система – није одређен
- ➢ Повезивање икт система
- ➢ Безбедносна свест о заштити података у ИКТ системима
- ➢ Обука
- ➢ Примена мера заштите од КЕМЗ (организационе мере)

# СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

# ИНФОРМАЦИОНА БЕЗБЕДНОСТ


*Слика 1.* Систем заштите тајних података-елементи

Систем заштите тајних података, као вишеслојни систем заштите, служи циљу обезбеђења и усаглашеност са законским и институционалним захтевима, реализовања концепта заштите националне безбедности и успостављање међународне сарадње, као и високих стандарда квалитета корпоративног управљања и адекватног понашања, али и осигурања стварне одговорности и доброг система 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.

# ИНФОРМАЦИОНА БЕЗБЕДНОСТ

# ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Безбедност на мрежи, односно онлајн безбедност је актуелна тема која изазива пажњу многих субјеката, а нарочито је значајна за кориснике и провајдере информационе технологије (IT).

Појам 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.

Представља праксу заштите информација ублажавањем ризика и представља део управљања ризиком (INFOSEC)....

## ШТА ЧИНИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ

1. ЦИЉЕВИ

   - очување поверљивости, интегритета и доступности информација
   - заштита информација и инф.система од неовлашћеног приступа, коришћења, откривања, ометања, модификације или уништења у циљу обезбеђивања поверљивости, интегритета и доступности
   - осигуравају да само овлашћени корисници (поверљивост) имају приступ тачним и потпуним информацијама (интегритет) када је то потребно (доступност)
   - заштита интелектуалне својине организације
   - управљање ризицима и трошковима информационог ризика за пословање
   - обезбеђивање да су инф.ризици и контроле у равнотежи
   - заштита информација, инф.система или база података од неовлашћеног приступа, оштећења, крађе или уништења

2. МЕРЕ

   - скуп активности и радњи које предузимају државни органи, јавна предузећа, компаније и правна лица ради заштите одређених информација

3. АКТИВНОСТИ

   - идентификација информација и сродних средстава, потенцијалних претњи, рањивости и утицаја
   - процена ризика
   - доношење одлука о третирању ризика (избегавању, ублажавању, расподели или прихватању)
   - избор и дизајн безбедносних контрола и спровођење
   - надгледање активности и прилагођавање променама....

## САЈБЕР БЕЗБЕДНОСТ

**Сајбер безбедност** се може представити као примена технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.

Циљ сајбер безбедности јесте да се смањи ризик од сајбер напада и заштити од неовлашћеног искоришћавања система, мреже и технологије.

## ЕЛЕКТРОНСКА УПРАВА

**Електронска управа или е-управа** (енгл. e-administration) је термин чије дефиниције варирају од употребе информатичке технологије како би се олакшао промет информација и савладале физичке препреке традиционалних система до коришћења технологије како би се повећала доступност и олакшало извршење јавних служби у корист грађана, привредника, као и запослених у тим службама.

Устаљено виђење ствари иза ових дефиниција је да је е-управа заправо аутоматизација, односно компјутеризација постојећег „папир система“, која ће довести до нових стилова управљања, нових начина расправљања и одређивања стратегија, обављања послова, као и организовања и достављања информација.

**Развој е-управе у Републици Србији** подразумева успостављање ефикасне и кориснички оријентисане управе у дигиталном окружењу, која је интероперабилна како између различитих нивоа јавне управе у Србији, тако и са јавном управом држава чланица ЕУ.

Међутим, пут од стадијума на коме се тренутно налази еУправа у Србији, до наведеног жељеног стања, представља распон жељене промене, који подразумева јасно дефинисање циљева Програма, као и мера за постизање тих циљева, са јасно уочљивим узрочно последичним везама.

На основу претходних реченица уочљиво је да сам развој подразумева концепцију и примену електронског пословања које користе сви (запослени у јавној управи, грађани, пословни људи, запослени људи у приватним објектима итд.).

Развојем е-управе омогућава се ефикаснија услуга према становништву, смањење трошкова, једноставније обављање послова уз добру организацију, сузбијање корупције и ефикаснији однос са привредним објектима.

Такође боља функционалност приступа подацима помаже развоју еУправе у Србији јер су грађани у прилици да лако провере тачност својих података и да се по потреби обрате надлежној институцији како би се ти подаци исправили.

**Закон о информационој безбедности**

Овим законом су уређене мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

**ИКТ системи од посебног значаја су системи који се користе:**

- у обављању послова у органима јавне власти;
- за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

## ИНФОРМАЦИОНА БЕЗБЕДНОСТ У Р. СРБИЈИ

Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са употребом информационо-комуникационих технологија, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.
**(Стратегија развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године)**

## ИНФОРМАЦИОНА БЕЗБЕДНОСТ

- Безбедност локације (“сајта”)
- Безбедност ресурса
- Безбедност комуникацијске мреже
- Безбедност сервиса
- Безбедност приватности - личних података.

У рачунарским мрежама се у циљу спречавања евентуалних напада и могућих оштећења података примењују одређени сигурносни сервиси, од којих су најзначајнији:

- Аутентификација (authentication);
- Тајност података (data confidiality);
- Непорицање порука (nonrepudation);
- Интегритет података (data integrity);
- Контрола приступа (access control) и
- Расположивост ресурса (resource availability)

Ради повећања IT безбедности органи јавне власти, предузећа, односно компанија обично се примењује шест категорија безбедносних мера.

Избор мера зависиће од потребног нивоа безбедности
- опште безбедносне политике и процедуре,
- софтвер за заштиту од вируса,
- дигитални потписи,
- шифровање,
- заштитни зидови (firewall) и
- прокси сервери

## ОПШТЕ БЕЗБЕДНОСНЕ ПОЛИТИКЕ И ПОСТУПЦИ

- Честа промена приступних лозинки
- Ограничавање употребе система
- Ограничавање приступа подацима
- Успостављање контроле физичког приступа
- Подела одговорности
- Шифровање (енкрипција) података
- Успостављање процедуралне контроле
- Провођење едукативних програма
- Инспекција активности унутар система
- Бележење свих трансакција и активности корисника

## УРЕДБА О БЛИЖЕМ УРЕЂЕЊУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

- Ближе уређење мера заштите ИКТ система
- Послови и одговорност запослених
- Заштита информационих добара
- Средства и имовина за надзор над пословним процесима
- Управљање ризицима
- Постизање безбедности рада на даљину и мобилних уређаја
- Образовање, обуке и едукације + одговорност
- Заштита после промене радног места (уговор о поверљивости, клаузула забране конкуретности…)
- Класификовање података
- Заштита носача података
- Ограничење приступа и овлашћен приступ
- Мере криптозаштите…

## УРЕДБА О БЛИЖЕМ САДРЖАЈУ АКТА О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА, НАЧИНУ ПРОВЕРЕ И САДРЖАЈУ ИЗВЕШТАЈА ПРОВЕРЕ БЕЗБЕДНОСТИ ИКТ СИСТЕМА

Садржина акта о безбедности ИКТ система:

- мере заштите
- принципи
- начини и процедуре постизања нивоа безбедности
- овлашћења и одговорности
- Ресурси
  КОМПАТИБИЛНО СА ISO/SRPS 27001

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

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.

## БЕЗБЕДНОСНИ РЕЖИМИ ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

Безбедносни режими ИКТ система за рад са тајним подацима односе се на различите нивое организације и примене мера заштите, како би се осигурала поверљивост, интегритет и доступност података у складу са њиховим степеном осетљивости. Ови режими дефинишу како корисници и системи могу приступати, обрађивати и складиштити податке.

Систем ради у једном од следећих безбедносних режима:

1) „НЕСЕЛЕКТИВНИ”;

2) „СЕЛЕКТИВНИ”;

3) „СА ВИШЕ НИВОА”.

Руководилац органа јавне власти, односно одговорно лице у правном лицу посебним актом одређује безбедносни режим рада система.

У систему који ради у безбедносном режиму „НЕСЕЛЕКТИВНИ”, сва лица која имају приступ том систему морају да имају сертификат за приступ тајним подацима највишег степена тајности података који се обрађују у систему и имају приступ свим тајним подацима који се обрађују у систему.

У систему који ради у безбедносном режиму „СЕЛЕКТИВНИ”, сва лица која имају приступ том систему морају да имају сертификат за приступ тајним подацима највишег степена тајности података који се обрађују у систему и могу приступати само одређеним тајним подацима.

У систему који ради у безбедносном режиму „СА ВИШЕ НИВОА”, лица која имају приступ том систему не морају да имају сертификат за приступ тајним подацима највишег степена тајности података који се обрађују у систему и имају приступ само одређеним тајним подацима који се обрађују у систему.

Тајни податак не сме се преносити кроз систем изван безбедносних зона без примене метода и средстава криптозаштите, који су одобрени од стране органа надлежног за спровођење послова у области криптозаштите.

Приватна информационо-телекомуникациона средства и преносиви документи (лични рачунари, преносиви рачунари, дискете, меморијски модули и др.) не могу се користити за обраду ТП.

Ако се тајном податку степена тајности „ДРЖАВНА ТАЈНА” или „СТРОГО ПОВЕРЉИВО” промени или укине степен тајности, документу на којем је тај податак био записан у електронском облику, не може се променити или укинути степен тајности.

Ако се тајном податку степена тајности „ПОВЕРЉИВО” или „ИНТЕРНО” промени или укине степен тајности, документу на којем је тај податак био записан у електронском облику, може се променити или укинути степен тајности, само кад је тај податак избрисан на начин да га је немогуће обновити софтверским алатом.

Ова документа морају се уништити након истека рока њихове употребе или након истека рока употребе система у којем су се користили, у складу са прописом којим се утврђују посебне мере физичко-техничке заштите тајних података.

Технички застарела или оштећена документа на којима су чувани тајни подаци уништавају се, у складу са прописом којим се утврђују посебне мере физичко-техничке заштите тајних података.

Коришћење аутоматизованих информационо-телекомуникационих средстава која раде без присуства оператера заснива се на процени ризика безбедности система, коју врши руководилац органа јавне власти, односно одговорно лице у правном лицу.

Проверу спровођења нивоа безбедности врши орган јавне власти или правно лице, односно овлашћено лице за управљање безбедношћу система.

# УПРАВЉАЊЕ РИЗИКОМ БЕЗБЕДНОСТИ ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

# УПРАВЉАЊЕ РИЗИКОМ БЕЗБЕДНОСТИ ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

Управљање ризиком безбедности ИКТ система за рад са тајним подацима је кључни процес који има за циљ идентификацију, процену, смањење и контролу ризика који могу угрожавати заштиту осетљивих података. Ови подаци могу бити од изузетне важности за националну безбедност, корпоративне интересе или личну приватност, тако да је неопходно обезбедити њихову заштиту на највишем нивоу.

### 1. Идентификација ризика

Први корак у управљању ризиком је идентификација потенцијалних претњи и рањивости система који обрађују тајне податке. Овај процес подразумева анализу свих аспеката ИКТ система који могу бити угрожени, као што су:

- **Претње изнутра**: Неовлашћени приступ или злоупотреба приступа од стране запослених или других овлашћених особа.
- **Претње споља**: Напади из спољашњих извора, као што су хакери, сајбер напади (нпр. DDoS напади, вируси, ransomware), или физички напади на инфраструктуру.
- **Природне катастрофе**: Оштета система услед природних догађаја као што су земљотреси, поплаве, или пожари.
- **Људске грешке**: Неправилно поступање са подацима, као што су грешке у конфигурацији, заборављени подаци или неадекватно уништавање информација.

### 2. Процена ризика

Након што су идентификовани ризици, потребно је проценити њихову озбиљност и вероватноћу. Процена ризика подразумева две кључне компоненте:

#### 2.1. Вредновање последица

- **Финансијске последице**: Губитак или крађа података може довести до значајне финансијске штете, укључујући казне, трошкове опоравка и потенцијалне тужбе.
- **Репутацијске последице**: Ризик од губитка поверења корисника или јавности, посебно ако дође до компромитације осетљивих података.
- **Правне последице**: Кршење закона или прописа о заштити тајних података, заштити података о личности, који може довести до правних санкција.
- **Безбедносне последице**: Ризик од националне или корпоративне безбедности ако се тајни подаци користе противно интересима државе, органа јавне власти или правног лица.

#### 2.2. Процена вероватноће

- Процена вероватноће да ће се неки ризик остварити заснива се на историјским подацима о претњама, доступним безбедносним статистикама и проценама тренутних унутрашњих и спољашњих ризика.

### 3. Стратегије управљања ризиком

Након процене ризика, треба усвојити стратегије које ће минимизирати утицај потенцијалних претњи. Ове стратегије могу бити:

1. **Избегавање ризика**: Промена процеса или процедура да би се елиминисали високо ризични аспекти.
2. **Смањење ризика**: Примена мера безбедности које смањују вероватноћу да ће се ризик остварити. То може укључивати техничке и оперативне мере као што су криптовање, контрола приступа и безбедносне политике.
3. **Преношење ризика**: Пренос одређених ризика на треће стране (нпр. осигурање или аутсорсинг безбедности).
4. **Прихватање ризика**: Ако су последице минималне или ако је трошак спречавања ризика већи од потенцијалних губитака, компаније могу одлучити да прихвате одређени ризик.

### 4. Мере за смањење ризика

Ефикасно управљање ризицима захтева имплементацију специфичних мера које ће заштитити ИКТ систем и тајне податке. То укључује:

#### 4.1. Техничке мере

- **Шифровање података**: Сви подаци који се чувају или преносе морају бити шифровани како би се спречила њихова неовлашћена употреба.
- **Аутентификација и ауторизација**: Употреба снажних метода аутентификације (нпр. двофакторска аутентификација) и контрола приступа како би се осигурало да само овлашћени корисници могу приступити осетљивим подацима.
- **Мониторинг и детекција**: Применом система за мониторинг који ће детектовати неовлашћене активности, као што су упади или неовлашћени приступи.
- **Резервне копије и опоравак**: Стварање редовних резервних копија података и дефинисање процедура за опоравак података у случају неуспеха система.

#### 4.2. Оперативне мере

- **Политике и процедуре**: Успостављање и примена строгих безбедносних политика, укључујући процедуре за руковање тајним подацима, едукацију запослених и сталну ревизију система.
- **Обучавање особља**: Стално обучавање запослених о безбедносним претњама, процедурама и одговорностима.
- **Физичка безбедност**: Осигурање физичког приступа рачунарима и серверима који чувају тајне податке, укључујући контроле на улазима у зграде, серверске просторије и слично.

#### 4.3. Управљање инцидентима

- **Одговор на инциденте**: Развити план за одговор на безбедносне инциденте (нпр. напад на сајбер безбедност, откривање угрожених података), који ће брзо деловати да би се минимизирале последице.

- **Континуирано усавршавање**: Након инцидента, треба анализирати узроке и предузети мере да се будући инциденти спрече.

**5. Мониторинг и континуирано побољшање**

Управљање ризиком није једнократан процес, већ континуиран циклус који захтева стално праћење и унапређење. Редовне безбедносне ревизије, процене нових претњи и одржавање система су од пресудног значаја за одржавање високог нивоа безбедности.

- **Ревизија ризика**: Стално праћење нових ризика и прилагођавање безбедносних мера на основу нових претњи и технологија.
- **Тестирање система**: Регуларни тестови, као што су *penetration* тестови, како би се идентификовале могуће рањивости.
- **Ажурирање безбедносних мера**: Применом нових безбедносних алата и метода како би се одржала заштита на високом нивоу.

Управљање ризиком безбедности ИКТ система за рад са тајним подацима је кључно за осигурање сигурности информација. Постављање адекватних мера за идентификацију, процену, смањење и праћење ризика осигурава да се подаци обрађују и складиште на сигуран начин, смањујући ризик од њихове компромитације. Правилно управљање овим ризицима помаже у заштити података, у складу са правним прописима и организационим потребама.

# АКРЕДИТАЦИЈА ИКТ СИСТЕМА

# АКРЕДИТАЦИЈА ИКТ СИСТЕМА

Безбедносна акредитација ИКТ система је поступак којим се осигурава усклађеност ИКТ система с мерама и стандардима информационе безбедности и информационе гаранције, дефинисане прописанима законском и подзаконском регулативом из подручја рада са тајним подацима и информационе безбедности, у сврху остваривања безбедносних циљева и потребног нивоа заштите тајности, целовитости и расположивости тајних података и пратећих услуга и ресурса. Овим се поступком утврђује се да ли је достигнут потребни ниво заштите, како се наведени ниво заштите одржава, као и оспособљеност тела надлежнога за управљање безбедношћу ИКТ система за који се безбебедносна акредитација спроводи.

Безбедносну акредитацију националних ИКТ система спроводе национални безбедносни органи (National Security Authority - NSA), који у најчешћем броју случајева обављају и фунцију Тела за акредитацију (Security Accreditation Authority - SAA). У колико NSA, односно SAA орган нема развијене капацитете за TEMPEST и крипто сертификацију, оно акредитацију спроводи у сарадњи са другим националним телом које је добило надлежност TA, CAA, CDA, и IAA тела.

Безбедносна акредитација ИКТ система осигурава усклађеност с прописаним мерама и стандардима информационе безбедности и заштите тајних података, због чега тела и правне особе утврђују Безбедносне циљеве и потребни ниво заштите тајних података, као и пратећих услуга и ресурса.

Основ безбедносне акредитације ИКТ система чине:

- Ревизија процене безбедносног ризика ИКТ система за рад са тајним подацима,
- Процена безбедносне документације,
- Провера и утврђивање примене безбедносних мера и њиховог одржавања, и
- утврђивање преосталог ризика и провера управљања безбедносним ризиком.

Државни орган, орган државне управе, орган јединице локалне самоуправе и друго правно лице којем је поверено вршење јавних овлашћења, као и правно и физичко лице које у вршењу законом утврђених послова, односно извршавању уговореног посла користи тајне податке, а који планирају да користе комуникационо-информационе системе и процесе за тајне податке, дужни су да од SAA тела прибаве Сертификат за ІКТ системе и процесе.

Уз захтев за сертификовање ИКТ система и процеса за тајне податке (у даљем тексту: систем) орган, односно правно или физичко лице прилаже Процену могућег угрожавања безбедности тајних података од упада у систем и употребе и уништавања тајних података који су обрађени и чувани у систему, тј. Процена ризика безбедности система (report of risk assesment proces). Процена ризика безбедности система односи се на утврђивање ризика, процену ризика који се не могу избећи, процену рањивости система, претње и могуће поседице реализације појединих претњи, укључујући и ризике у вези са окружењем у којем се систем користи. Процена ризика безбедности система врши се периодично, у складу са поступцима за процену ризика предвиђеним планом за процену ризика система.

Треба нагласити да је у Уредби о посебним мерама заштите тајних података у информационо-телекомуникационим системима, "Службени гласник РС", број 53/2011, наведено да се Процена ризика безбедности система врши се за систем у коме се обрађују, преносе и чувају тајни подаци степена тајности "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО" и "ПОВЕРЉИВО".

Према нормативним актима Републике Србије, за систем у коме се обрађују тајни подаци који су означени степеном тајности "ИНТЕРНО", није потребно да се спроводи сертификација, већ орган јавне власти, односно правно лице обезбеђује одржавање одговарајућег нивоа безбедности тајних података (поверљивости, целовитости, аутентичности или доступности), у складу са прописима којима се уређује информациона безбедност.

## 1. Процес акредитације ИКТ система

Акредитација ИКТ система подразумева формалну процену који се систем користи за обраду тајних података. Процес акредитације осигурава да систем испуњава безбедносне стандарде који су утврђени за заштиту података у складу са важећим законима, прописима и спецификацијама.

### 1.1. Кораци у процесу акредитације

1. **Процена потреба**:
    - Одређивање врсте тајних података који ће се обрађивати, степен тајности, као и специфични безбедносни захтеви.
2. **Дефинисање безбедносних мера**:
    - Разрада техничких и организационих мера заштите (шифровање, аутентификација, контрола приступа, физичка безбедност, итд.).
3. **Процена ризика**:
    - Извођење процене ризика како би се идентификовале потенцијалне претње и слабости у систему. Ова фаза подразумева тестирање система, процену рањивости и припрему одговарајућих мера за смањење ризика.
4. **Ревизија и верификација**:
    - Независна ревизија система од стране акредитованих стручњака или тела која ће проверити да ли систем испуњава прописане стандарде и безбедносне захтеве.
5. **Издавање акредитације**:
    - Након успешне процене и провере, орган акредитације издаје службену акредитацију која потврђује да систем испуњава све релевантне безбедносне стандарде.

### 1.2. Међународни стандарди и прописани захтеви

- **ISO/IEC 27001**: Стандард за управљање безбедношћу информација који поставља захтеве за успостављање, имплементацију, одржавање и континуирано унапређење система управљања безбедношћу информација.
- **Common Criteria (CC)**: Међународни стандард за евалуацију и сертификацију безбедности ИТ система.

- **NIST SP 800-53**: Стандарди и смернице за безбедност информационих технологија који се користе у Сједињеним Америчким Државама, али су широко примењивани и у другим земљама.
- **TEMPEST:** Стандард који регулише заштиту од компромитованих еманација и електромагнетног зрачења које може бити пресретнуто током рада са тајним подацима.

## 2. Улога акредитације у контексту тајних података

Акредитација ИКТ система за рад са тајним подацима има важну улогу у обезбеђивању да се системи користе на сигуран и поуздан начин.

### 2.1. Осигурање поузданости система

Акредитовани системи морају бити константно тестирани, ажурирани и евалуирани како би се осигурало да задовољавају актуелне захтеве за безбедност података. Ово укључује:

- Редовну ревизију система.
- Процену нових претњи и унапређење мера заштите.
- Праксу сталне едукације и обуке особља које рукује системом.

### 2.2. Прописи и усаглашеност

Тиме што добија акредитацију, ИКТ систем доказује своју усаглашеност са релевантним прописима који регулишу заштиту тајних података. Ово је важно јер правне и регулаторне инстанце захтевају да сви системи који раде са тајним подацима буду у складу са прописаним безбедносним и правним оквирима.

### 2.3. Поверење јавности и корисника

Акредитација такође повећава поверење јавности, корисника и других заинтересованих страна, јер осигурава да је систем у складу са највишим безбедносним стандардима. Ово је посебно важно када се ради о тајним подацима који могу бити од значаја за националну безбедност.

## 3. Обновљива акредитација и континуирано одржавање безбедности

Након што је ИКТ систем акредитован, потребно је стално одржавати висок ниво безбедности:

- **Редовне ревизије и процене безбедности**: За безбедност система је потребно да се периодично спроводе ревизије како би се утврдило да ли су све мере и процедуре у складу са новим претњама и технологијама.
- **Ажурирање система**: Редовно ажурирање безбедносних алата, система и процедура како би се смањили нови ризици.
- **Обновљена акредитација**: У зависности од захтева, акредитација може бити ограничена на одређени период, након чега се процес акредитације мора поновити.

Акредитација ИКТ система за рад са тајним подацима је кључна за осигурање да системи који обрађују тајне податке буду безбедни, поуздани и у складу са важећим стандардима и прописима. Поред самог процеса акредитације, важан је и континуирани надзор и одржавање безбедности система како би се осигурала заштита података у сваком тренутку.

## СРПСКИ СТАНДАРД

- SRPS ISO/IEC 27001:2014, Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација – Захтеви
- Уредба о посебним мерама заштите тајних података у информационо-телекомуникационим системима (ЗТП)
- Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја (ЗИБ + ЗЗЛП)

## SRPS ISO 27001

- **ISO/IEC 27001** је међународни стандард за управљање безбедношћу информација .
- Детаљно 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.
- Већина организација има бројне контроле безбедности информација.
- Међутим, без система управљања безбедношћу информација (ISMS), контроле имају тенденцију да буду донекле неорганизоване и неповезане, пошто се често примењују као тачна решења за специфичне ситуације или једноставно као ствар конвенције.
- Контроле безбедности које раде обично се баве одређеним аспектима информационе технологије (IT) или посебно безбедности података; остављајући не-ИТ информациона средства (као што су папирологија и власничка знања) мање заштићена у целини.
- Планирањем континуитета пословања и физичком безбедношћу може се управљати сасвим независно од ИТ или информационе безбедности, док се у пракси људских ресурса може мало помињати потреба да се дефинишу и доделе улоге и одговорности у области безбедности информација у целој организацији.

ISO/IEC 27001 захтева да менаџмент:

- Систематски испита ризике по безбедност информација организације, узимајући у обзир претње, рањивости и утицаје;
- Дизајнира и примени кохерентан и свеобухватан скуп контрола безбедности информација и/или других облика третмана ризика (као што је избегавање ризика или пренос ризика) како би се адресирали они ризици који се сматрају неприхватљивим; и

- Усвоји свеобухватни процес управљања како бисте осигурали да контроле безбедности информација настављају да испуњавају потребе организације за безбедност информација на сталној основи.

## СТАНДАРДИ ISO/IAC 17799

- политику безбедности;
- организовање информатичке безбедности;
- управљање ресурсима;
- безбедност људских ресурса;
- физичку заштиту;
- управљање радом и комуникацијама;
- контролу приступа;
- набављање, развој и одржавање информатичких система, управљање безбедосним инцидентима;
- управљање континуитетом пословања и усаглашеност за законском регулативом.

# ИНФОРМАЦИОНА ГАРАНЦИЈА (ИГ)

# ИНФОРМАЦИОНА ГАРАНЦИЈА (ИГ)

ИГ треба да обезбеди:

- поверљивост
- интегритет
- расположивост
- аутентификација
- непорецивост

Имплементација система информационе гаранције (ИГ) доприноси побољшању безбедности података, смањењу ризика, повећању продуктивности и ефикасности, те јачању угледа и кредибилитета.

Специфичне предности укључују:

1.Појачана безбедност података:

- ✓ Минимизирање ризика од неовлашћеног приступа, коришћења, откривања, оштећења, модификације или уништења информација.
- ✓ Заштита приватности и поверљивости података клијената, запослених и других заинтересованих страна.
- ✓ Усклађивање са законским и прописима о заштити података, као што су Закон о заштити тајних података, Закон о заштити података о личности и ISO 27001.

2. Смањени трошкови и финансијски губици:

- ✓ Спречавање трошкова везаних за санирање последица безбедносних инцидената, као што су губитак података, прекид рада и оштећење угледа.
- ✓ Смањење трошкова везаних за судске спорове и казне.
- ✓ Повећање поузданости и стабилности пословања, што доводи до дугорочних финансијских уштеда.

3. Побољшана продуктивност и ефикасност:

- ✓ Обезбеђивање доступности информација неопходних за рад запослених.
- ✓ Смањење губитка времена и ресурса због проблема са безбедношћу.
- ✓ Повећање поверења запослених у информациони систем и побољшање радне атмосфере.

4. Усавршено управљање ризиком:

- ✓ Идентификација, процена и управљање ризицима по информацијску безбедност.
- ✓ Обезбеђивање плана за суочавање са безбедносним инцидентима и минимизирање њихових последица.
- ✓ Повећање отпорности организације на кибернетичке нападе и друге претеће.

5. Јачи углед и кредибилитет:

- ✓ Демонстрација посвећености организације заштити података и приватности својих клијената и партнера.
- ✓ Повећање поверења клијената и изградња чврших пословних односа.
- ✓ Давање компаративне предности на тржишту.

6. Олакшано усклађивање са прописима:

- ✓ Усклађивање са релевантним законима и прописима о заштити тајних података, али и прописа који покривају покривају заштиту података о личности и ISO 27001.
- ✓ Смањење ризика од санкција и казни.
- ✓ Поједностављење процеса аудита и контроле.

7. Побољшан континуитет пословања:

- ✓ Обезбеђивање доступности и функционалности информационих система и података у свим околностима.
- ✓ Минимизирање прекида рада и губитка прихода у случају безбедносних инцидената.
- ✓ Повећање отпорности органа јавне власти или правног лица на непредвиђене ситуације.

8.Подигнута свест о безбедности:

- ✓ Подизање свести запослених о ризицима по информацијску безбедност и начинима заштите података.
- ✓ Промена културе безбедности у организацији и стварање одговорнијег приступа информационим ресурсима.
- ✓ Допринос општем побољшању безбедносног окружења.

9. Побољшано доношење одлука:

- ✓ Обезбеђивање тачних и ажурних информација потребних за доношење информисаних пословних одлука.
- ✓ Смањење ризика од доношења лоших одлука због нетачних или непотпуних информација.
- ✓ Повећање ефикасности и продуктивности организације.

10. Олакшано планирање и буџетирање

- ✓ Имплементација система информационе гаранције (ИГ) не само да побољшава безбедност података и смањује ризике, већ доприноси и олакшаном планирању и буџетирању у оквиру информационог система.

Предности у планирању и буџетирању:

- *Проактивно управљање ризиком:* Идентификација и процена ризика по безбедност података омогућава проактивно планирање и алокацију ресурса за њихово ублажавање. То доводи до смањења трошкова везаних за санирање последица безбедносних инцидената у будућности.
- *Транспарентност трошкова:* Јасно дефинисане политике и процедуре ИГ-а доприносе транспарентности трошкова везаних за безбедност података. То олакшава буџетирање и планирање ИТ инвестиција, те доводи до ефикаснијег коришћења ресурса.

- *Предвидивост трошкова:* Проактивно управљање ризиком и транспарентност трошкова омогућавају предвидивост трошкова везаних за безбедност података. То олакшава планирање дугорочних ИТ стратегија и инвестиција.
- *Оптимизација ресурса:* Ефикасно управљање ризиком и транспарентност трошкова доприносе оптимизацији коришћења ИТ ресурса. То доводи до уштеда у трошковима и побољшања ефикасности ИТ операција.
- *Планирање за раст:* Добро имплементиран ИГ систем олакшава планирање за раст и скалирање ИТ инфраструктуре. То обезбеђује да је информациони систем спреман да подржи будуће потребе органа јавне власти или правног лица без компромитовања безбедности података.

**Примери:**

- *Планирање имплементације нових технологија:* ИГ систем може се користити за процену ризика везаних за имплементацију нових технологија и дефинисање буџета за мере заштите података.
- *Планирање за опоравак од хаварија:* ИГ систем може се користити за дефинисање плана опоравка од хаварија и буџета за неопходне ресурсе.
- *Планирање редовног одржавања и ажурирања софтвера:* ИГ систем може се користити за дефинисање распореда редовног одржавања и ажурирања софтвера, те буџета за те активности.

Имплементација система информационе гаранције не само да побољшава безбедност података, већ доприноси и олакшаном планирању, буџетирању и управљању ИТ ресурсима. То доводи до смањења трошкова, побољшања ефикасности и повећања отпорности органа јавне власти или правног лица на претеће нападе.

## 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

Уз претходно наведене мере заштите ИКТ система за рад са тајним подацима, важно је истакнути следеће:

**Усаглашеност са прописима:**

- Организације које рукују тајним подацима морају се придржавати релевантних прописа и стандарда о заштити тајних података, али и прописа који покривају заштиту података о личности и ISO 27001.
- Имплементација система управљања информационом безбедношћу (ISMS) може знатно допринети усклађености са прописима и побољшању укупне безбедности ИКТ система.

Улога људи:

- Чак и уз најснажније технолошке мере заштите, људски фактор остаје кључни елемент у заштити тајних података.
- Неопходно је континуирано едуковати запослене о ризицима по безбедност података и обезбедити им потребна знања и вештине за правилно руковање тим подацима.

**Планирање за будућност:**

- Претње ИКТ системима се стално мењају и развијају, стога је неопходно да се мере заштите континуирано ажурирају и прилагођавају.
- Важно је пратити најновије трендове у кибернетичкој безбедности и имплементирати нове технологије и решења за заштиту како би се очувао висок ниво безбедности тајних података.

**Сарадња:**

- Размена информација о претњама и искуствима у вези са заштитом тајних података са другим организацијама и стручњацима може значајно допринети побољшању укупне безбедности.

**Улагање у заштиту:**

- Заштита тајних података не представља трошак, већ инвестицију у будућност.
- Губитак или оштећење тајних података може довести до озбиљних финансијских губитака, штете угледу и других негативних последица.

**Заштита ИКТ система са тајним подацима је сложен и континуиран процес који захтева преданост, стручност и тимски рад. Имплементацијом свеобухватног приступа који укључује технолошка решења, организационе мере, едукацију корисника и сарадњу са другим заинтересованим странама, органи јавне власти и правна лица могу значајно побољшати безбедност својих тајних података и обезбедити дугорочну заштиту.**

# ЗНАЧЕЊЕ ПОЈЕДИНИХ ТЕРМИНА

**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 .

**ИКТ систем** (информационо-комуникациони систем) је технолошко-организациона целина која обухвата:

- електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
- уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
- податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- организациону структуру путем које се управља ИКТ системом;
- све типове системског и апликативног софтвера и софтверске развојне алате.

**Оператор ИКТ система** је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

**Тајност** је својство које значи да податак није доступан неовлашћеним лицима.

**Интегритет** значи очуваност изворног садржаја и комплетности податка.

**Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан.

**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.

**Непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

**Ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система.

**Мере заштите ИКТ** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.

**Информациона добра** обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично .

## 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)
- 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)
- Проф. др Горан Д. Матић - Систем заштите тајних података података – приручник (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_TP-skripta.pdf)
- Проф. др Горан Д. Матић - Основе обраде и заштите података – приручник (https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf)
- Сајт Канцеларије Савета за националну безбедност и заштиту тајних података (nsa.gov.rs)