ИНФОРМАЦИОНА БЕЗБЕДНОСТ У ИКТ СИТЕМИМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

– СКРИПТА –

Проф.др Горан Д. Матић

Београд, 2025. 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 овлашћни 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 (избегавњу, 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).

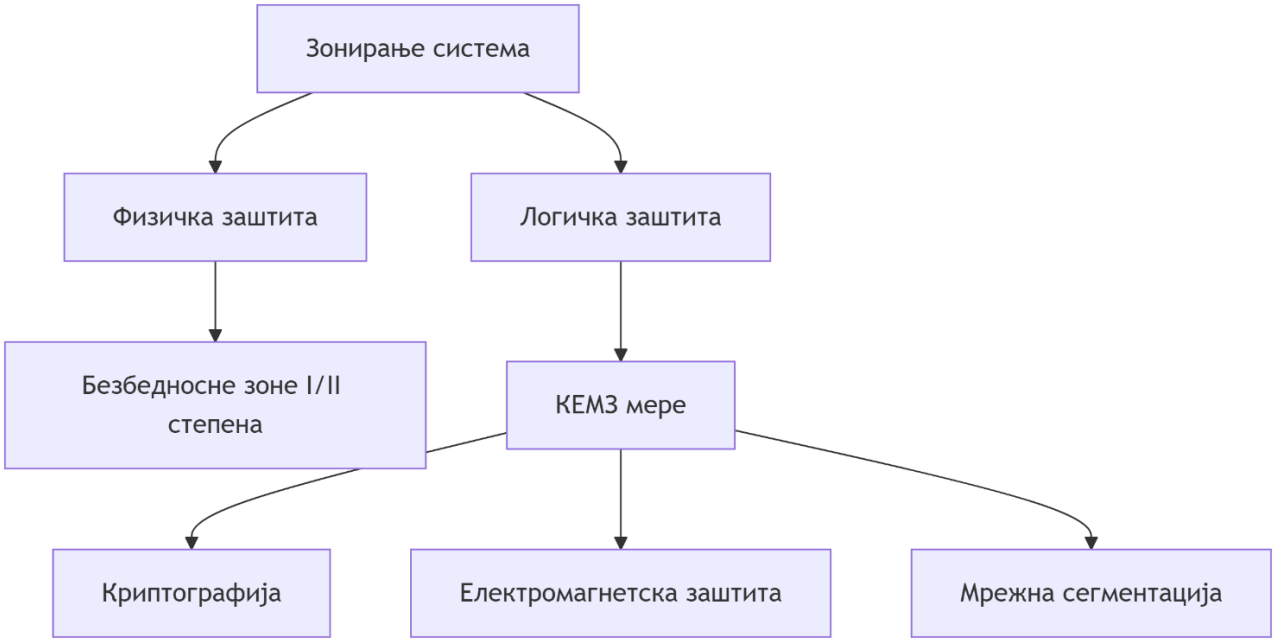
Према резултатима мерења спроведених уз помоћ одговарајуће опреме за зонирање објеката и мерења електромагнетног зрачења одређују се безбедносне зоне у објектима у којима се обрађују тајни подаци. У ствари, то значи одређивање просторија према степену заштите од електромагнетног зрачења.

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.

ЗОНИРАЊЕ ПРОСТОРА И СИСТЕМА – БЕЗБЕДНОСНЕ И АДМИНИСТРАТИВНЕ ЗОНЕ У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА И СИСТЕМИМА ЗА ОБРАДУ ТАЈНИХ ПОДАТАКА

Зонирање информационо-комуникационих система од посебног значаја и система за обраду тајних података представља један од темељних елемената техничко-организационе заштите у оквиру система националне безбедности. Оно подразумева јасну поделу простора на административне и безбедносне зоне различитог степена, у складу са прописима који регулишу тајност података, информациону безбедност и физичко-техничке мере заштите. Примена стандарда као што је SRPS ISO/IEC 27001, увођење КЕМЗ концепта (криптографија, електромагнетска, мрежна и заштита приступа), као и процена потребе за TEMPEST мерама, кључни су за обезбеђење интегритета, поверљивости и доступности података. У складу са законском регулативом и техничким смерницама, зонирање омогућава систематичну контролу приступа, управљање ризицима и акредитацију ИКТ система у којима се рукује тајним подацима и другим поверљивим информацијама, што представља предуслов за сигуран и одржив рад органа јавне власти у окружењу повећаних сајбер и хибридних претњи.



СЛИЧНОСТИ И РАЗЛИКЕ ИЗМЕЂУ „КЛАСИЧНОГ“ ЗОНИРАЊА И ЗОНИРАЊА ИКТ СИСТЕМА, У ОДНОСУ НА РАД СА ТАЈНИМ ПОДАЦИМА

Сличности:

- И једно и друго зонирање служе као механизми контроле приступа тајним подацима – физичке и организационе мере примењују се ради заштите поверљивости, интегритета и доступности података.
- Оба модела користе класификацију простора у административне и безбедносне зоне (I и II степена), са јасно дефинисаним условима за приступ и боравак.
- У оба случаја потребна је евиденција приступа, контрола уноса/износа материјала или опреме, као и редовне провере и интерна контрола.
- Прописане мере заштите морају бити документоване, проверљиве и засноване на процени ризика.

Разлике:

- Класично зонирање се односи превасходно на физичко руковање и чување папирних докумената, док зонирање ИКТ система укључује и логичке (дигиталне) и мрежне аспекте, као и криптографску и електромагнетску заштиту.
- У зонирању ИКТ система примењује се **КЕМЗ концепт** (криптографија, електромагнетска, мрежна и приступна заштита), који нема еквивалент у класичном моделу.
- За разлику од папирног система, где је приступ физички ограничен простором, у ИКТ окружењу је потребна **технолошка сегментација система** (властити VLAN-ови, DMZ, IDS/IPS, firewall итд.).
- У зонирању ИКТ система се разматра и примена **TEMPEST мера**, које се односе на заштиту од електромагнетног зрачења и прислушкивања, што није примењиво у класичном зонирању.
- Док класични систем зависи претежно од физичких мера (брава, обезбеђење, видео надзор), ИКТ системи захтевају и **софтверске, мрежне и хардверске контроле**, као и примену стандарда као што је SRPS ISO/IEC 27001.

„КЛАСИЧНО“ ЗОНИРАЊЕ VS. ЗОНИРАЊЕ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Критеријум	**Класично зонирање (папирни документи)**	**Зонирање ИКТ система од посебног значаја**
Сврха	Контрола физичког приступа тајним документима	Контрола приступа, обраде и преноса тајних података у ИКТ окружењу
Типови зона	Административна, безбедносна зона I и II степена	Идентичне зоне, али примењене у ИКТ инфраструктури
Средства заштите	Браве, видео надзор, дежурне службе, контрола уноса/износа	Мрежне сегментације, IDS/IPS, firewall-и, VLAN, криптографија, логови
Контрола приступа	Физичка: обезбеђење, легитимације, дневници улаза	Дигитална: аутентикација, ауторизација, логовање приступа
Фокус безбедности	Простор и физички документи	Информације у дигиталном облику и инфраструктура
КЕМЗ мере	Не примењују се	Примењују се (криптографија, електромагнетска, мрежна и приступна заштита)
TEMPEST мере	Није примењиво	Примењује се по процени ризика у зонама I степена
Правни основ	Закон о тајности података, Уредба о физичко-техничкој заштити	Закон о тајности података, Закон о информационој безбедности, Уредба о посебним мерама заштите тајних података у ИКТ системима
Акредитација	Није увек обавезна	Обавезна за ИКТ системе који рукују тајним подацима
Документација	План физичке заштите, опис зона, евиденција приступа	+ Изјава о примени стандарда, опис КЕМЗ мера, процена ризика, ев. TEMPEST извештај
Примери мера	Закључавање просторија, службеници обезбеђења	DMZ зоне, изоловане мреже, криптографија, HSM, PKI, изолација каблова

"Напомена: *Зонирање није циљ већ процес - захтева континуирано ажурирање према новим претњама."*

1. Правни основ зонирања

Назив прописа	Примена
Закон о тајности података („Сл. гласник РС“, бр. 104/2009)	Прописује обавезу примене мера заштите тајних података, укључујући физичко-техничке и организационе мере.
Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016...95/2021)**	Дефинише појам ИКТ система од посебног значаја и уводи обавезу примене мера заштите, процене ризика и акредитације.
Уредба о посебним мерама заштите тајних података у ИКТ системима („Сл. гласник РС“, бр. 89/2013)	Прописује техничке, логичке и физичке мере заштите података у ИКТ окружењу. Обавезује на процену ризика и примену стандарда.
Уредба о посебним мерама физичко-техничке заштите тајних података	Одређује класификацију зона: административна, безбедносна зона I и II степена.
Препоруке КСНБиЗТП за акредитацију ИКТ система – чл. 87 Закона о тајности података	Прецизира поступак и техничке услове за акредитацију ИКТ система који обрађују тајне податке.
SRPS ISO/IEC 27001:2014	Једини нормативно прихваћен стандард за испуњавање организационих и техничких мера у административним и другим зонама.

2. Типови зона и њихово одређивање

Зона	Примена
Административна зона	Обрада интерних, општих и неосетљивих података, укључујући комуникацију запослених, логистику и подршку.
Безбедносна зона II степена	Простор или просторија у којој се обрађују и чувају тајни подаци степени тајности: „ПОВЕРЉИВО“, „СТРОГО ПОВЕРЉИВО“ и „ДРЖАВНА ТАЈНА“, али улазак и кретање у овој зони не сматра се приступом тајним подацима.
Безбедносна зона I степена	Простор или просторија у којој се обрађују и чувају тајни подаци из зоне II степена. Улазак у ову зону сматра се оствареним приступом тајним подацима.

3. КЕМЗ концепт у заштити ИКТ система

Компонента	Опис
К – Криптографија	Енкрипција података у преносу и складиштењу, крипто-модули, хардверски безбедносни модули (HSM), PKI инфраструктура.
Е – Електромагнетска заштита	Екранизација, размак између ИКТ и електроенергетских инсталација, изолација кабловских токова ради спречавања електромагнетних сметњи и цурења информација.
М – Мрежна заштита	Дизајн мрежа са демилитаризованим зонама (DMZ), VLAN сегментација, IDS/IPS системи, firewall-и, физичка изолација мрежа.
З – Заштита приступа	Аутентикација корисника, евиденција приступа, биометријски системи, видео надзор, контроле улога и дозвола.

4. Физичко-техничке мере по зонама

Зона	Мере
Административна	Закључавање простора, картице, видео надзор, уређена евиденција приступа.
II степен	Ојачана контрола улаза, дежурна служба, алармни систем, надзор 24/7, имплементација КЕМЗ мера.
I степен	Све мере из II степена + два нивоа контроле улаза, провера уноса/износа опреме, ограничен број овлашћеног особља, контрола докумената и интерних процедура.

5. TEMPEST мере – статус у Србији

Ставка	Стање
Лабораторија	Не постоји званична TEMPEST лабораторија.
Сертификација опреме	Није успостављен национални списак сертификиране опреме.
Обавезност	Није прописана као обавезна мера, али може бити услов за акредитацију у зони I степена.
Препорука	Навести у документацији одсуство примене TEMPEST мера са образложењем (нпр. недостатак инфраструктуре) и применити компензационе мере.

6. Обавезна документација (за акредитацију КСНБ и ЗТП)

- Општи опис просторија и зона;
- Табела примењених физичко-техничких мера;
- Изјава о примени стандарда SRPS ISO/IEC 27001;
- Описи примењених КЕМЗ мера;
- Процена ризика по систему и простору;
- Извештај о мерењу електромагнетног зрачења (ако постоји);
- Навођење одсуства TEMPEST мера уз образложење;
- Потписано лице задужено за систем заштите.

Зонирање ИКТ система од посебног значаја и система за обраду тајних података мора бити засновано на јасно дефинисаном законском и техничком оквиру, који обухвата:

- примену релевантних закона и подзаконских аката који прописују физичко-техничку и организациону заштиту тајних података;
- стандарде SRPS ISO/IEC 27001 као основ за информациону безбедност у свим зонама;
- КЕМЗ концепт као кључни модел за безбедносно зонирање и заштиту ИКТ система;
- TEMPEST мере као предуслов за највише нивое тајности, примењиве у складу са резултатима процене ризика;
- строгу контролу приступа, редовне безбедносне провере, евиденцију и интерне контроле.

Овај оквир обезбеђује свеобухватну и сигурну заштиту података и ИКТ инфраструктуре у условима повећаних претњи и сложености савремених информационих система.

Напомена: *"Зонирање није само технички захтев – то је стратешки оквир за одржавање суверенитета државе у дигиталном добу."*

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.

ОСНОВНИ ПРИНЦИПИ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

ОСНОВНИ ПРИНЦИПИ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Информациона безбедност у раду са тајним подацима представља један од кључних концепата у заштити националних интереса, корпоративних ресурса и институционалне стабилности. Обрада и чување тајних података захтева примену вишеструких мера заштите – техничких, организационих и правних – у складу са важећим законским оквиром Републике Србије. Пре свега, Закон о тајности података („Сл. гласник РС”, бр. 104/2009 и 36/2011) дефинише врсте и степене тајних података, поступке одређивања, означавања, руковања и приступа, док Закон о информационој безбедности („Сл. гласник РС”, бр. 6/2016, 94/2017 и 77/2019) уређује мере заштите ИКТ система, укључујући и системе од посебног значаја, у којима се често обрађују тајни или осетљиви подаци. ИКТ системи од посебног значаја, како су дефинисани наведеним законом, обухватају критичне инфраструктуре, државне органе, правна лица која обављају делатност од јавног значаја, као и пружаоце електронских услуга. Уколико такви системи обрађују тајне податке, обавезна је примена појачаних безбедносних мера, укључујући процену ризика, имплементацију техничких и организационих мера, стални надзор, инцидентно обавештавање, као и сарадњу са надлежним телима као што су Канцеларија Савета за националну безбедност и заштиту тајних података и Канцеларија за информационе технологије. Такође, пре пуштања у рад, ИКТ системи од посебног значаја морају проћи процедуру безбедносне акредитације која потврђује да систем испуњава све прописане безбедносне стандарде и захтеве за обраду тајних података.

Савремени информациони системи који обрађују тајне податке морају бити пројектовани тако да буду отпорни на различите врсте безбедносних претњи – сајбер нападе, унутрашње компромитације, техничке кварове или физичке упаде. У ту сврху примењују се принципи као што су вишеслојна одбрана (Defense in Depth), концепт нултог поверења (Zero Trust), приступ с најмањим привилегијама (Least Privilege), шифровање података, микросегментација, као и континуирано праћење и евидентирање активности. Интеграција ових мера и принципа, уз придржавање релевантних стандарда као што су ISO/IEC 27001, ISO/IEC 15408, NIST Cybersecurity Framework, ENISA препоруке и CIS Controls, представља основ за постизање високог степена поверљивости, интегритета и доступности података. Ово је кључно не само за безбедно доношење одлука у области националне безбедности, већ и за очување поверења у институције и инфраструктуру Републике Србије, као и за усклађеност са међународним стандардима и обавезама у оквиру ЕУ и НАТО Партнерства за мир, као и билатералне међународне сарадње у области размене тајних података.

Савремени приступи информационој безбедности заснивају се на примени више комплементарних принципа који, заједно, обезбеђују снажан и отпоран систем. Ови принципи нису само техничке мере, већ и темељне безбедносне политике које се интегришу у све нивое управљања подацима – од пројектовања система до свакодневног руковања тајним подацима и осетљивим информацијама.

- **Defense in Depth (Одбрана у дубини):** Вишеслојна заштита система, где сваки слој (физички, мрежни, апликативни) представља додатну баријеру, смањујући шансу да један пробој угрози целину.
  Пример: Комбинација firewall-a, IDS/IPS система и антивирусне заштите на крајњим уређајима.
- **Security by Design (Безбедност по дизајну):** Безбедносни захтеви се уграђују у саму архитектуру система од почетка, уместо да се додају накнадно.
  Пример: Систем за електронско гласање који од старта укључује криптографску заштиту, аутентификацију и логовање.
- **Need to Know (Потребно да зна или за сазнањем):** Приступ поверљивим подацима имају само лица којима су ти подаци нужни за конкретне задатке, чиме се смањује ризик од злоупотребе.
- **Zero Trust (Нулта толеранција или Политика неповерења):** Не постоји аутоматско поверење – сваки захтев за приступ се верификује, без обзира да ли долази из интерне мреже или са удаљене локације.
  Пример: Коришћење континуиране аутентификације и контекстуалних политика приступа унутар великих организација.
- **Least Privilege (Најмање привилегија):** Корисници добијају само она права која су им неопходна за рад, без додатних привилегија које могу бити злоупотребљене.
- **Data Encryption (Шифровање података):** Подаци морају бити заштићени и током преноса и у мировању, чиме се обезбеђује поверљивост чак и у случају физичког компромитовања система.
- **Secure Communication (Безбедна комуникација):** Пренос осетљивих информација врши се искључиво преко проверених и шифрованих канала, као што су VPN, TLS или енд-то-енд енкриптоване апликације.
- **Audit & Logging (Аудит и логовање):** Све активности које укључују тајне податке морају бити евидентиране, анализиране и редовно прегледане како би се благовремено открile злоупотребе или пропусти.
- **Access Controls (Контрола приступа):** Напредни механизми као што су двофакторска аутентификација, биометрија или адаптивне контроле приступа смањују ризик од неовлашћеног уласка у систем.
- **Data Integrity (Интегритет података):** Очување тачности и непромењености података током њихове обраде и складиштења обезбеђује поузданост система.
- **Segmentation (Сегментација):** Раздвајање мрежних ресурса ограничава потенцијално ширење напада и унапређује контролу приступа између различитих делова инфраструктуре.
- **Continuous Monitoring (Континуирано праћење):** Системи се стално надгледају како би се на време уочиле безбедносне претње и брзо предузеле мере.

Интеграција ових принципа у информационе системе значајно повећава ниво безбедности тајних података. Организације које доследно примењују Zero Trust модел и друге безбедносне мере могу боље одговорити на савремене претње и обезбедити поуздану заштиту својих критичних информација.

Пример из праксе: Компанија Google је 2011. године имплементирала Zero Trust модел (BeyondCorp) након сајбер напада који је компромитовао осетљиве податке. Овим приступом елиминисали су класични периметарски модел безбедности и успоставили динамичке контроле приступа за све запослене, без обзира на њихову локацију.

ПРИНЦИП DEFENSE IN DEPTH – ВИШЕСЛОЈНА ОДБРАНА

Defense in Depth (Вишеслојна одбрана) је концепт у информационој безбедности који подразумева имплементацију више независних слојева заштите унутар ИКТ система и процеса. Циљ оваквог приступа је да се повећа укупна отпорност система, тако да компромитовање једног слоја не доведе до потпуног урушавања безбедности. Ова стратегија следи логичку претпоставку: ***"не ослањај се на један механизам заштите."***

Основна начела:

1. **Редудантност и дубина:** Више баријера функционише као резервни механизми.
2. **Хетерогеност мера:** Различити типови мера спречавају да један вектор напада угрози све слојеве.
3. **Време и детекција:** Нападачима се отежава и продужава време упада, дајући тимовима за реаговање више времена за откривање и одговор.

Нивои примене:

1. Физички ниво

Ово је први и често занемарен слој заштите. Циљ је спречавање неовлашћеног физичког приступа просторијама или хардверу у ком се чувају тајни подаци.

Примери:

- Контрола приступа просторијама (ID картице, биометрија).
- Видео-надзор, алармни системи.
- Чување сервера у заштићеним просторијама (rack сервери са бравама).
- Анти-тампер уређаји на хардверу.

2. Мрежни ниво

Обухвата механизме који штите комуникационе канале и мрежну инфраструктуру.

Примери:

- **Firewall** – ограничавање саобраћаја према политичким правилима.

- **IDS/IPS (Intrusion Detection/Prevention Systems)** – откривање и спречавање упада.
- VPN тунели за безбедну комуникацију.
- VLAN сегментација за изолацију критичних делова мреже.

3. Апликативни и системски ниво

Овај ниво обезбеђује заштиту самих апликација и оперативног система који приступа или обрађује тајне податке.

Примери:

- Шифровање података у мировању (at rest) и у преносу (in transit).
- Аутентификација са више фактора (MFA).
- Заштита од SQL инјекција и XSS напада.
- Правилна контрола приступа на основу улога (RBAC/ABAC).
- Безбедно програмирање и редовно ажурирање софтвера.

4. Организациони и процесни ниво

Безбедност није само техничко, већ и управљачко питање. Овај ниво подразумева уређење политика, процедура и људских ресурса.

Примери:

- Обука особља за препознавање социјалног инжењеринга.
- Политике најмањих привилегија (Least Privilege).
- Процедуре за инцидентно реаговање и опоравак.
- Унутрашња контрола и редовне ревизије.

ПРИМЕНА У ЗАШТИТИ ТАЈНИХ ПОДАТАКА

У раду са тајним подацима, **Defense in Depth** се примењује обавезно и системски. Закон о тајности података и Закон о информационој безбедности не предвиђају само техничке мере, већ и организационе, као и физичке мере које треба да раде заједно.

Пример из праксе (војни или државни систем):

- Просторија за приступ тајним подацима има контролу уласка са биометријом и надзорним камерама.
- Сервери су изоловани и приступачни само преко VPN тунела уз двофакторску аутентификацију.
- Подаци су шифровани, а активности запослених се логују и прате.

- Инцидентни одговор се активира аутоматски у случају сумње на компромитацију било ког слоја.

Вишеслојна одбрана је основни стуб модерне информационе безбедности, посебно у системима који обрађују тајне или строго поверљиве податке. Њен значај расте у контексту све софистицираних претњи и хибридних напада. Имплементација Defense in Depth приступа захтева сарадњу ИТ сектора, безбедносних служби и руководства – уз поштовање домаћег правног оквира и међународних стандарда.

SECURITY BY DESIGN – БЕЗБЕДНОСТ УГРАЂЕНА У ДИЗАЈН

Security by Design је приступ развоју информационих система који подразумева уградњу безбедносних захтева и контрола у све фазе животног циклуса система – од иницијалног планирања и пројектовања, преко развоја и тестирања, до имплементације, одржавања и повлачења из употребе. Циљ овог приступа је спречавање рањивости пре него што систем постане оперативан, уместо накнадног "додавања" безбедности као засебног слоја.

Кључни елементи приступа:

1. **Threat Modeling – Моделовање претњи** - Рана идентификација и анализа потенцијалних безбедносних претњи, рангирање ризика и дефинисање мера заштите већ у фази дизајна.

Примери:

- STRIDE модел (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege).
- Анализа нападачких путева и злоупотреба (attack trees, misuse cases).

2. Secure Coding Practices – Безбедне праксе програмирања - Примена стандарда и смерница за избегавање уобичајених програмерских грешака које доводе до безбедносних рањивости.

Примери:

Избегавање директне интерполације корисничког уноса.

- Коришћење функција за валидацију и филтрирање података.
- Управљање меморијом и ресурсима (посебно у C/C++ окружењима).

3. Принципи најмањих привилегија и сегментације - Сваки део система и сваки корисник имају само оне привилегије које су им апсолутно неопходне, чиме се смањује обим потенцијалне компромитације.

4. Интегрисано тестирање безбедности - Безбедносно тестирање се укључује у процес развоја (DevSecOps), што укључује:

- Статичку анализу кода (SAST).
- Динамичку анализу апликација (DAST).
- Пентестове и fuzz тестирање током развоја.

5. Усаглашеност са стандардима - Примена признатих индустријских стандарда и оквира као што су:

- **OWASP Top 10** – најчешће рањивости веб апликација.
- **NIST SP 800-160** – системски инжењеринг за безбедност.
- **ISO/IEC 27034** – апликативна безбедност.

Пример примене у пракси - Развој веб апликације у оквиру државне институције која обрађује тајне податке**:**

- Још у фази пројектовања идентификоване су претње попут XSS, CSRF и SQL инјекција.
- Развојни тим користи безбедносне библиотеке за аутентификацију и шифровање.
- Уведене су континуиране провере кода кроз Git репозиторијуме.
- Кориснички унос се валидира на серверу и клијенту.
- Коришћени су OWASP смернице и алати (*ZAP, Dependency-Check*).

Значај за заштиту тајних података - У системима у којима се обрађују тајни или строго поверљиви подаци (нпр. у системима од посебног значаја према Закону о информационој безбедности), принцип *Security by Design* није препорука – већ нужност. Он осигурава да ниједна компонента не буде "слаба карика" и смањује ослањање на спољне заштитне мере, јер је сам систем пројектован тако да одолева претњама.
Security by Design поставља безбедност као основни грађевински елемент система, а не као накнадну обавезу. У контексту савремених сајбер претњи и обраде тајних података, овај приступ представља стандард добре праксе у складу са домаћим и међународним правилима и значајно унапређује укупну дигиталну отпорност организација.

НУЛТО ПОВЕРЕЊЕ (ZERO TRUST) – СУШТИНСКА ПАРАДИГМА БЕЗБЕДНОСТИ

Zero Trust модел представља модеран приступ заштити тајних података елиминацијом подразумеваног поверења и захтева континуирану верификацију идентитета и приступа. Насупрот традиционалним безбедносним моделима, који претпостављају да су корисници унутар мреже поуздани, Zero Trust обезбеђује динамичку контролу приступа, независно од физичке локације или корисничког статуса.

КЉУЧНИ ПРИНЦИПИ НУЛТО ПОВЕРЕЊЕ (ZERO TRUST) МОДЕЛА

Zero Trust модел представља оквир који елиминише подразумевано поверење и обезбеђује строг приступ подацима кроз континуирану верификацију. Основни принципи овог модела укључују:

1. **Никада не веруј, увек проверавај** – Сваки захтев за приступ мора бити аутентификован и верификован, без обзира на локацију корисника или претходни статус. Ово укључује употребу **вишеструке аутентификације (MFA)** за сваку сесију, динамичке политике приступа и периодичну ревизију корисничких дозвола.
2. **Минимални приступ (PoLP – Principle of Least Privilege)** – Корисници и системи добијају само она овлашћења која су им апсолутно неопходна за обављање конкретних задатака. Ово спречава прекомерно дељење ресурса и умањује ризик од злоупотребе приступа у случају компромитације налога.
3. **Континуирано праћење и анализа** – Све корисничке активности се надгледају у реалном времену ради откривања сумњивих образаца и потенцијалних безбедносних претњи. Коришћење **SIEM платформи као што су Splunk и Microsoft Sentinel** омогућава прикупљање и анализу логова како би се брзо детектовале аномалије и спречиле потенцијалне компромитације.
4. **Шифровање података у свим фазама** – Тајни подаци морају бити заштићени и у мировању и током преноса. Ово подразумева коришћење **AES-256 за складиштење и TLS 1.3 за пренос**, чиме се осигурава да чак и у случају пресретања комуникације или компромитације система, подаци остају неупотребљиви за неовлашћене стране.
5. **Сигурни комуникациони канали** – Сва комуникација мора се одвијати преко безбедних платформи и протокола. Коришћење **VPN-а, шифрованих е-порука (PGP, S/MIME)**, као и специјализованих алата за размену осетљивих информација, смањује ризик од пресретања или манипулације подацима током преноса.

Zero Trust модел значајно унапређује безбедносне механизме организације, омогућавајући динамичку контролу приступа и континуирану валидацију активности. Правилном имплементацијом ових принципа, ризик од неовлашћеног приступа и сајбер напада се своди на минимум, чиме се обезбеђује максимална заштита тајних података.

ZERO TRUST VS. ТРАДИЦИОНАЛНИ БЕЗБЕДНОСНИ МОДЕЛИ У РАДУ СА ТАЈНИМ ПОДАЦИМА

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

ПРИНЦИП NEED TO KNOW КАО КЛАСИЧНИ МОДЕЛ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Дефиниција и основна карактеристика - Need to Know (NTK – "Потребно да зна") представља један од најстаријих и најстрожих принципа заштите тајних података, традиционално примењиван у војним, обавештајним и државним институцијама. Овај модел се заснива на концепту да корисник сме приступити поверљивим информацијама **само ако му је то неопходно за обављање службених дужности**, што значи да приступ није заснован на статусу или положају, већ искључиво на стварној потреби.

Основни механизми примене

1. **Строга контрола приступа** – Приступ тајним подацима је ограничен и строго дефинисан, уз ревизију дозвола на периодичној основи.
2. **Додела привилегија на минималном нивоу** – Корисницима се омогућава само оно знање и ресурси који су директно релевантни за њихову улогу.
3. **Сегментација информација** – Подаци су подељени у засебне категорије и ниво приступа зависи од посебних дозвола.

4. **Континуирано праћење приступа** – Приступ поверљивим подацима се бележи и анализира ради спречавања неовлашћеног откривања или злоупотребе.

Предности и изазови примене

- ✓ **Смањује ризик од неовлашћеног откривања** – Ограниченим приступом подацима смањује се могућност цурења информација.
- ✓ **Прецизно дефинише улоге и одговорности** – Свако има приступ само ономе што му је неопходно, без вишка информација које би могле бити злоупотребљене.
- ▼ **Може отежати сарадњу** – Због строгих ограничења, понекад је потребно додатно време да се обезбеди приступ за радне задатке.
- ▼ **Захтева строгу административну контролу** – Имплементација NTK модела захтева доследно управљање и ажурирање приступа.

Примери из праксе

- **Војне операције** – Оперативци имају приступ само специфичним информацијама неопходним за њихове задатке, чиме се спречава цурење осетљивих података.
- **Корпоративна безбедност** – Компаније примењују NTK модел да ограниче приступ стратегијским плановима и осетљивим пословним подацима.
- **Обавештајне службе** – Оперативни агенти добијају само делове информација релевантне за њихову мисију, без ширег контекста.

Need to Know модел остаје један од најпоузданијих приступа заштити тајних података. Иако његова строга примена може изазвати оперативне изазове, његова способност да минимизује ризик од неовлашћеног приступа чини га незаменљивим у критичним безбедносним ситуацијама.

Кључни елементи Need to Know принципа - Need to Know (NTK) модел функционише кроз низ строгих безбедносних механизама који осигуравају да приступ осетљивим подацима имају само овлашћени корисници са оправданом потребом. Основни елементи овог принципа укључују:

1. Хијерархијски приступ

- Приступ подацима се додељује на основу формалне класификације, као што су **"Поверљиво", "Строго поверљиво", "Државна тајна"**.
- Корисници морају имати **експлицитно одобрење**, попут безбедносног сертификата или дозволе, да би приступили одређеном степену тајности.
- Виши степени тајности захтевају додатне мере безбедности, као што су двофакторска аутентификација или биометријска провера.

2. Контрола приступа на основу улога (RBAC – Role-Based Access Control)

- Права приступа се додељују **према улози у организацији** (нпр. аналитичар, руководилац, аудитор), што смањује ризик од неовлашћеног приступа.

- **Примери примене:**
    - **Војни официр** има приступ само подацима везаним за његову јединицу, док му подаци других одељења нису доступни.
    - **Државни службеник у министарству финансија** не може видети документе министарства одбране, чиме се спречава неовлашћено откривање осетљивих информација.
- RBAC модел минимизује изложеност поверљивих података и примењује се уз **регуларне ревизије** приступних права.

3. Статичке листе приступа

- За сваки скуп тајних података креирају се **фиксне листе овлашћених лица**, којима је приступ строго ограничен.
- Свака **промена приступа** захтева **формални процес ревизије**, који може укључивати додатне провере од стране безбедносних служби.
- Овај приступ је посебно користан у високо осетљивим окружењима, као што су **војне базе и истраживачки институти**.

4. Физичка и процедурална заштита

- Тајни документи се складиште у **сефовима**, безбедним серверима или просторијама са ограниченим приступом.
- Сви приступи се **евидентирају** – ручно (нпр. вођење дневника) или путем **аутоматизованих система логовања**, како би се пратио сваки покушај приступа поверљивим подацима.
- Коришћење **сигурносних мера** као што су видео-надзор, алармни системи и приступни кодови осигурава додатну заштиту.

Need to Know принцип остаје један од најефикаснијих модела заштите тајних података. Његова примена осигурава да се информације деле **само са овлашћеним особама**, минимизујући ризик од неовлашћеног откривања или злоупотребе.

Пример из праксе – Примена Need to Know модела у банкарском сектору

Међународна банка је 2022. године имплементирала **Need to Know + Zero Trust** приступ за управљање осетљивим финансијским подацима.

- **Контрола приступа на основу улога (RBAC):** Само запослени у сектору финансијских истрага имају увид у сумњиве трансакције, док запослени у другим секторима немају приступ.
- **Динамичка анализа ризика:** Ако запослени покуша да приступи поверљивим подацима ван радног времена или са нерегистрованог уређаја, систем **аутоматски блокира** приступ и шаље упозорење безбедносном тиму.

- **Микро-сегментација:** Чак и овлашћени запослени могу приступити **само одређеним деловима финансијских података**, без могућности прегледа целокупног клијентског портфолија.
- **Шифровани пренос информација:** Интерне комуникације користе **PGP шифроване е-поруке**, чиме се осигурава да подаци остају безбедни чак и ако дође до компромитације мрежног система.

Овим приступом, банка је значајно смањила ризик од **унутрашњих злоупотреба**, цурења осетљивих података и сајбер напада.

УЛОГА NEED TO KNOW У ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Need to Know принцип представља један од најзначајнијих концепата у информационој безбедности, обезбеђујући строг контролисани приступ поверљивим подацима. Његова примена значајно смањује ризик од инсајдерских претњи, неовлашћеног откривања информација и кршења правних прописа.

1. Ограничавање експозиције података

- **Минимизира ризик од инсајдерских претњи** – Чак и ако корисник има легитимни приступ једном делу система, он нема аутоматски увид у све податке. Ово спречава злоупотребу интерних информација.
- **Смањује површину напада** – Ограничен приступ значи да потенцијални нападач не може лако компромитовати све системе и податке.

Пример из праксе: У обавештајној агенцији, агент који ради на пројекту **„Алфа“** нема никакву информацију о пројекту **„Бета“**, чиме се спречава ширење осетљивих података ван дозвољених граница.

2. Спречавање „цурења или преливања“ информација

- **Ограничава непотребно дељење осетљивих података** – Подаци се деле само са особама којима су неопходни за обављање конкретног задатка.
- **Спречава случајна цурења** – На пример, особа која није овлашћена не може случајно добити приступ поверљивим документима.

Пример из праксе: У великим корпорацијама, приступ финансијским подацима је строго ограничен. Финансијски аналитичар може видети само податке који се односе на његов сектор, али нема приступ широј стратегији компаније.

3. Комплајенс и правни оквири

- ✓ **Need to Know је често законски прописан за рад са државним тајнама** – У многим земљама овај принцип је обавезан за институције које управљају поверљивим подацима.
- ✓ **Користи се у различитим стандардима информационе безбедности**, као што су:
- **ISO 27001** – Глобални стандард за информациону безбедност.
- **NISPOM (Национални индустријски безбедносни програм за САД)** – Регулише рад са осетљивим подацима у војно-индустријском комплексу.

Пример из праксе: У владиним агенцијама, запослени са **безбедносним дозволама** имају приступ подацима само у оквиру својих операција, спречавајући неовлашћено дељење државних тајни.

4. Комбинација са другим моделима

Need to Know се често комбинује са другим безбедносним приступима ради још боље контроле приступа:

- **Мандаторна контрола приступа (MAC)** – Систем аутоматски одлучује ко сме да приступи одређеним подацима на основу дефинисаних правила.
- **Zero Trust модел** – Need to Know дефинише основна приступна правила, док Zero Trust уводи **континуирану верификацију** корисничких активности.

Пример из праксе: Технолошке компаније које користе **Zero Trust** приступ комбинују Need to Know модел са аутоматизованим праћењем корисничке активности. Ако се детектује неуобичајено понашање, систем може **привремено блокирати** приступ и затражити додатну аутентификацију.

Need to Know остаје један од најстрожих и најефикаснијих модела информационе безбедности. Његова примена значајно смањује ризик од злоупотреба, инсајдерских претњи и неовлашћеног приступа осетљивим подацима. Уз савремене технологије попут Zero Trust и динамичке контроле приступа, овај принцип постаје још ефикаснији у заштити критичних информација.

NEED TO KNOW VS. ZERO TRUST: КОМПАРАТИВНА АНАЛИЗА

Критеријум	**Need to Know (NTK)**	**Zero Trust (ZT)**
Основа приступа	Формална дозвола и улога	Континуирана верификација
Флексибилност	Статички (ретке промене)	Динамички (адаптивни приступ)
Фокус	Заштита од инсајдерских ризика	Заштита од спољних и унутрашњих претњи
Технологија	Физичке контроле, RBAC	MFA, SIEM, микросегментација
Примена	Војна, државна управа	Корпоративне и cloud средине

СЛАБОСТИ NEED TO KNOW МОДЕЛА

Иако је Need to Know дуго био основни модел заштите тајних података, његова примена у модерним информационо-комуникационим системима има одређене недостатке.

1. Ограничена примена у динамичким ИКТ срединама

✓ **Захтева ручне измене приступа**, што може бити споро и неефикасно у великим системима.
✓ **Није погодан за cloud и remote-work окружења**, где су приступи подацима флексибилнији.

Пример: У модерним корпоративним мрежама, запослени често морају сарађивати на различитим пројектима, али строг Need to Know модел отежава брзу размену података, захтевајући ручне промене дозвола.

2. Не открива злонамерне активности

✓ Ако корисник има приступ тајним подацима, Need to Know систем **не анализира његове намере или понашање**.
✓ **Инсајдерске претње** остају велики проблем – овлашћени корисници могу злоупотребити своје привилегије без система који их надгледа у реалном времену.

Пример: Током хакерског напада на **OPM (U.S. Office of Personnel Management) 2015.**, злонамерни актер је искористио **легитимне креденцијале** да украде милионе досијеа. Need to Know није спречио цурење јер је нападач већ имао овлашћење за приступ. **Zero Trust би захтевао додатну верификацију и анализу понашања**, чиме би овај напад био откривен раније.

3. Високи трошкови имплементације

✓ Захтева **детаљну административну контролу** и **регуларне ревизије** приступа.
✓ Велике организације морају одржавати сложене системе приступа, што повећава оперативне трошкове.

Пример: Институције које управљају поверљивим подацима морају редовно ажурирати **листу овлашћених корисника**, што захтева време, ресурсе и високу тачност у управљању подацима.

ДА ЛИ ЈЕ NEED TO KNOW И ДАЉЕ РЕЛЕВАНТАН?

✓ **Да**, за **врло строго контролисане средине**, као што су **нуклеарни објекти, обавештајне службе и војне институције**, где је ризик од компромитације изузетно висок.
▼ **Не**, као **једина заштита** у дигиталном окружењу – потребна је **комбинација са Zero Trust моделом** како би се обезбедила динамичка заштита података.

Идеалан сценарио:

- **Need to Know** дефинише ко сме да приступи подацима.
- **Zero Trust** проверава **да ли је приступ легитиман у сваком тренутку**, анализирајући корисничке активности, уређаје и локацију.

Овај **комбиновани приступ** осигурава и хијерархијску контролу и флексибилну динамичку заштиту, што је кључно за рад са тајним подацима у 21. веку.

NEED TO KNOW VS. ZERO TRUST: СЛИЧНОСТИ И РАЗЛИКЕ

Need to Know и **Zero Trust** су два принципа безбедности који се примењују у раду са тајним подацима, али имају различите приступе и циљеве.

Сличности

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

Разлике

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

Примена у информационим системима

- **Need to Know** се користи у **класичним безбедносним структурама**, као што су војне и државне институције, где се приступ подацима, односно тајним подацима заснива на хијерархији и улогама.
- **Zero Trust** је погодан за **модерне ИКТ системе**, посебно у cloud окружењима (*AWS, Azure*), где се приступ подацима мора динамички контролисати и верификовати.

Референца: *NIST SP 800-207 дефинише Zero Trust архитектуру и препоручује њену примену у критичним инфраструктурама.*

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

ИМПЛЕМЕНТАЦИЈА ZERO TRUST МОДЕЛА У РАДУ СА ТАЈНИМ ПОДАЦИМА

Zero Trust модел обезбеђује максималну контролу приступа тајним подацима, елиминишући ризик од неовлашћеног приступа кроз принцип „никада не веруј, увек проверавај“. Његова примена подразумева следеће кључне кораке:

1. Строга контрола приступа

- ✓ **Дефинисање правила приступа** – Коришћење **Azure AD Conditional Access** омогућава динамичку контролу приступа на основу корисничких атрибута као што су локација, уређај и ризик сесије.
- ✓ **Примена мултифакторске аутентификације (MFA)** – Безбедност се повећава коришћењем **FIDO2 стандарда и хардверских токена као што је YubiKey**, чиме се елиминишу слабости класичних лозинки.

2. Шифровање података

Коришћење криптографије за заштиту поверљивих информација –

- **AES-256** се користи за складиштење тајних података.
- **TLS 1.3** обезбеђује безбедан пренос.
- **Пост-квантни алгоритми** се примењују у системима који желе дугорочну заштиту од криптографских пробоја.

3. Сигурни комуникациони канали

- **Избегавање јавних мрежа** – Коришћење VPN-а као што су **WireGuard и IPsec** обезбеђује безбедан тунел за размену осетљивих информација.
- **Шифроване поруке и е-пошта** – Коришћење **PGP или S/MIME** спречава неовлашћено пресретање комуникације.

4. Континуирано праћење и анализа

- **Примена система детекције упада (IDS)** – Алат као што је **Snort или Suricata** анализира мрежни саобраћај ради откривања сумњивих активности.
- **SIEM (Security Information and Event Management)** – Коришћење **IBM QRadar или Splunk** омогућава прикупљање и анализу безбедносних инцидената у реалном времену.

5. Едукација запослених

- **Обучавање за препознавање сајбер претњи** – Фишинг и социјални инжењеринг остају међу највећим претњама, па платформе као што је **KnowBe4** помажу у редовним симулацијама напада.
- **Политике безбедног руковања тајним подацима** – Запослени морају бити свесни ризика и следити прописане процедуре.

Зашто је Zero Trust идеалан модел за заштиту тајних података? - Zero Trust не само да елиминише ризик од неовлашћеног приступа, већ обезбеђује **континуирану верификацију идентитета и анализу корисничких активности**, чиме се спречавају потенцијални напади.

Комбинација са Need to Know принципом

- **Need to Know** дефинише ко сме да приступи подацима.
- **Zero Trust** осигурава да се сваки приступ проверава у реалном времену.

Овај **вишеслојни приступ** је посебно критичан за организације које управљају **најосетљивијим информацијама**, као што су **обавештајне службе, финансијске институције и војне организације**.

LEAST PRIVILEGE – НАЈМАЊЕ ПРИВИЛЕГИЈЕ

Принцип најмање привилегије (PoLP – Principle of Least Privilege) подразумева да корисници, апликације и системски процеси добијају искључиво оне привилегије које су неопходне за извршавање конкретних задатака. Овај приступ подразумева додељивање приступа ресурсима и овлашћењима на најнижем могућем нивоу, што значајно смањује површину напада и умањује потенцијалну штету у случају злоупотребе или компромитације.

Предности примене принципа најмање привилегије

1. **Смањење ризика од инсајдерских претњи**
   - Корисници и процеси имају строго дефинисане, ограничене привилегије. Чак и у случају компромитовања налога, могућности злоупотребе су знатно смањене.
   - **Пример:** Уколико службеник у банци има приступ само једном сегменту клијентских података, чак и у случају крађе његових акредитива, нападач неће моћи да приступи целокупној бази података.
2. **Ограничавање штете у случају компромитације**
   - Ако злонамерни актер добије приступ систему, ограничења привилегија онемогућавају критичне радње као што су инсталација malware-а или измена системских датотека.
   - **Пример:** Хакер који експлоатише рањивост у серверској апликацији која ради са ограниченим овлашћењима неће моћи да преузме контролу над системом.

3. **Повећана стабилност и предвидивост система**
    - Ограничавање приступа системским компонентама смањује вероватноћу ненамерних грешака или злонамерних измена у конфигурацији.
    - **Пример:** Корисник са стандардним привилегијама не може да модификује системске библиотеке, чиме се избегавају озбиљни кварови система.
4. **Усклађеност са Zero Trust стратегијом**
    - Принцип најмање привилегије је саставни део Zero Trust модела, који се заснива на динамичком додељивању приступа на основу контекста и стварних потреба.
    - **Пример:** У Zero Trust окружењу, администратори немају сталне привилегије, већ морају поново да се аутентификују за извођење критичних радњи.
5. **Комплајенс са регулативама и стандардима**
    - Бројне регулативе и стандарди информационе безбедности (нпр. **PCI DSS**, **HIPAA**, **GDPR**) захтевају примену принципа најмање привилегије ради заштите осетљивих података.
    - **Пример:** У здравственом систему, лекари имају приступ само медицинским картонима својих пацијената, а не комплетној бази података.

Примери примене у различитим окружењима

1. **Linux – sudo механизам**
    - Корисници функционишу са основним привилегијама, а администраторске команде се извршавају преко sudo уз додатну аутентификацију.
    - **Предност:** Онемогућава стално коришћење root налога, чиме се смањује ризик од критичних грешака и злоупотреба.
2. **Windows – User Account Control (UAC)**
    - Корисници раде под стандардним налозима, док се за административне радње захтева експлицитна дозвола (нпр. унос лозинке).
    - **Предност:** Спречава се несметана инсталација злонамерних програма који захтевају административни ниво приступа.
3. **Cloud окружења – AWS IAM, Azure RBAC**
    - Корисницима и сервисима се додељују минималне дозволе на основу њихове улоге.

- **Примери:**
  - Развојни тим има приступ само специфичним S3 bucket-има, не целој инфраструктури.
  - DevOps инжењери могу покретати виртуелне машине, али не и брисати продукционе базе података.

4. **Контејнеризација – Docker, Kubernetes**
   - Подразумева се извршавање контејнера као non-root корисника, са ограниченим приступом систему.
   - **Пример:** Docker контејнер који покреће веб апликацију не може да приступи или модификује системске датотеке host машине.

Како имплементирати принцип најмање привилегије

- ✓ **Сегментација улога:** Прецизно дефинисање улога као што су "аналитичар", "аудитор", "систем администратор", при чему свака улога има ограничен и јасно дефинисан опсег дозвола.
- ✓ **Редовне ревизије привилегија:** Периодично проверавање и аутоматско уклањање привилегија које нису коришћене током одређеног периода (нпр. 90 дана).
- ✓ **Привремене привилегије:** Примена *Just-In-Time* (JIT) приступа, где се административне привилегије додељују само у одређеном временском оквиру – нпр. коришћењем **Azure Privileged Identity Management (PIM)**.
- ✓ **Аутоматизована провера и мониторинг:** Алати као што су **AWS IAM Access Analyzer**, **Microsoft Entra Permissions Management** и слични, омогућавају откривање прекомерних овлашћења и препоручују оптимизацију приступа.
- ✓ **Едукација запослених:** Континуирана обука запослених о значају ограничавања привилегија и препознавању техника социјалног инжењеринга (нпр. фишинг).

Принцип најмање привилегије представља један од темељних стубова информационе безбедности у савременим ИТ окружењима. Његова исправна и доследна примена:

- Смањује ризик од инсајдерских и екстерних напада,
- Олакшава усклађеност са регулаторним оквирима,
- Повећава стабилност, предвидивост и отпорност система.

Иако примена овог принципа захтева пажљиво планирање и одговарајућу инфраструктуру (посебно у великим и комплексним системима), дугорочне користи у погледу сигурности, поузданости и регулаторне усклађености далеко превазилазе иницијалне напоре. Комбиновање са стратегијама као што су **Zero Trust** и **Need to Know** резултира слојевитом и ефикасном заштитом критичних ресурса и тајних података.

DATA ENCRYPTION – ШИФРОВАЊЕ ПОДАТАКА

Шифровање података представља процес заштите информација применом криптографских метода који омогућавају да подаци остану нечитљиви без одговарајућег кључа. Овај процес је кључан за обезбеђивање безбедности и приватности података — било да су у мировању, у преносу или у употреби. Уз примену снажних алгоритама и криптографских стандарда, шифровање спречава неовлашћени приступ, чиме се значајно смањује ризик од крађе података, манипулације или злоупотребе.

Типови шифровања:

- **Шифровање у мировању**

Шифровање у мировању односи се на заштиту података похрањених на дисковима, у базама података или другим складиштима. Ова врста шифровања осигурава да подаци остану недоступни неовлашћеним странама, чак и ако дође до физичког приступа уређају.

Најчешће коришћени алгоритам за шифровање података у мировању је **AES (Advanced Encryption Standard) са 256-битним кључем (AES-256)**. Овај алгоритам обезбеђује високу безбедност и користи се у различитим областима, укључујући банкарство, здравство и владине системе.

Поред AES-а, организације могу користити **BitLocker (на Windows системима)** или **FileVault (на macOS)** како би шифровале целе дискове, штитећи осетљиве податке од неовлашћеног приступа.

- **Шифровање у преносу**

Податке који се шаљу преко мрежа штите криптографски протоколи као што су **Transport Layer Security (TLS) 1.3** и **VPN решења**.

- **TLS 1.3** је најновија верзија сигурносног протокола за шифровану комуникацију преко интернета. Користи се за заштиту података у веб комуникацији, укључујући **HTTPS** веб странице, шифроване е-поруке и безбедне трансакције.
- **VPN (Virtual Private Network)** технологија обезбеђује шифроване тунеле за комуникацију, штитећи податке од пресретања и омогућавајући корисницима да безбедно приступају мрежама, чак и када користе јавне Wi-Fi мреже.

Поред тога, модерни мрежни комуникациони протоколи, као што су **SSH (Secure Shell) и SFTP (Secure File Transfer Protocol)**, користе криптографију за обезбеђивање безбедног преноса података између сервера и клијената.

- **End-to-End енкрипција (E2EE)**

Овај метод осигурава да подаци остану шифровани од тренутка слања до тренутка пријема, без могућности да их било ко прочита или дешифрује осим предвиђеног примаоца.

- **Апликација Signal** користи **end-to-end енкрипцију** за све облике комуникације, укључујући текстуалне поруке, аудио и видео позиве.

- **WhatsApp и Telegram (у тајном чету)** такође примењују E2EE за сигурну комуникацију, осигуравајући да чак ни сервери апликације немају приступ садржају порука.
- **ProtonMail**, популарни сервис за шифровану е-пошту, користи E2EE за обезбеђивање приватности корисника, чиме спречава неовлашћен приступ чак и од стране провајдера услуге.

Захваљујући **E2EE**, приватност корисника је максимално заштићена, што значи да нико – укључујући интернет провајдере, хакере или администраторе сервиса – не може приступити садржају комуникације без овлашћења.

SECURE COMMUNICATION – БЕЗБЕДНА КОМУНИКАЦИЈА: СТАНДАРДИ, ПРИМЕРИ И ПРЕПОРУКЕ

У ери све већих претњи по информациону безбедност, очување поверљивости комуникације представља кључни изазов за институције, компаније и појединце. Овај преглед обухвата проверене технологије и протоколе за заштиту преноса података, конкретне примере из праксе, важеће стандарде и препоруке за имплементацију. Посебан акценат стављен је на модерне облике енкрипције, заштиту метаподатака, као и спремност на квантне претње.

1. Безбедни канали преноса

Пренос тајних или осетљивих података мора се обављати искључиво преко безбедних комуникационих канала како би се спречио приступ неовлашћеним странама. Најчешће коришћене технологије и протоколи укључују:

- **VPN (Virtual Private Network)** – Криптира цео саобраћај између уређаја и мреже.
  - *Пример из праксе:* Коришћење IPSec VPN за удаљени приступ корпоративној мрежи (нпр. OpenVPN, Cisco AnyConnect).
  - *Стандард:* NIST SP 800-77 (IPSec VPNs), RFC 4301 (IPSec архитектура).
  - *Препорука:* Користите VPN са мултифакторском аутентификацијом (MFA) за додатни ниво заштите.
- **TLS (Transport Layer Security)** – Обезбеђује енкриптовану комуникацију преко интернета (нпр. HTTPS, SFTP).
  - *Пример из праксе:* Веб-сајтови који користе TLS 1.2 или 1.3 (нпр. банке, здравствене платформе).
  - *Стандард:* NIST SP 800-52, PCI DSS.
  - *Препорука:* Онемогућити застареле верзије (SSL 3.0, TLS 1.0, TLS 1.1) и користити јаке шифре (AES-256, ChaCha20).
- **Специјализоване платформе** – Решења као што су Signal (end-to-end енкрипција), ProtonMail (безбедни мејл), или SFTP/SCP за пренос фајлова.

- *Пример из праксе:* Коришћење Signal-а за поверљиве разговоре у владиним или корпоративним окружењима.
- *Стандард:* ISO/IEC 27001.
- *Препорука:* Проверити да ли платформа користи end-to-end
- енкрипцију и да ли је аудитирана (нпр. Signal је отвореног кода и независно проверен).

- **Комуникација отпорна на квантне претње**
  - *Нова пракса:* Имплементација post-quantum криптографских алгоритама у критичним системима.
  - *Пример:* Протоколи засновани на *CRYSTALS-Kyber* и *Dilithium* (NIST PQC стандардизација).
  - *Препорука:* Пратити развој NIST PQC финалиста и започети планирање миграције са класичних алгоритама (RSA, ECC).
- **Мобилна комуникација и VoLTE безбедност**
  - Пример: Заменити стандардне SMS и позиве употребом апликација са end-to-end енкрипцијом.
  - *Препорука:* Користити приватне APN мреже и управљане MDM системе за службене мобилне уређаје.

2. Додатне безбедносне мере

- **Енкрипција у мировању (Encryption at Rest)**
  - *Пример:* BitLocker (Windows), LUKS (Linux), или AWS KMS.
  - *Стандард:* NIST SP 800-111.
- **Строга контрола приступа**
  - *Пример:* Google Workspace користи OAuth 2.0 и RBAC.
  - *Препорука:* Примена Zero Trust модела за интерне мреже.
- **Редовни аудит и мониторинг**
  - *Пример:* SIEM алати као што су Splunk, Wazuh.
  - *Стандард:* ISO/IEC 27002.
- **Заштита метаподатака у комуникацији**
  - *Пример:* Коришћење Tor или VPN да би се сакрио IP и време комуникације.
  - *Препорука:* Редовно брисање логова и шифровање заглавља где је могуће.

3. Препоруке за имплементацију

- ✓ Изаберите проверене протоколе (TLS 1.3, WireGuard за VPN)
- ✓ Онемогућите застареле алгоритме (MD5, SHA-1, DES)
- ✓ Користите MFA за све приступе осетљивим подацима
- ✓ Обучите запослене о фишинг нападима и социјалном инжењерингу
- ✓ Правите резервне копије са енкрипцијом и чувајте их на безбедним локацијама
- ✓ Укључите квантно-отпорне алгоритме у дугорочне планове
- ✓ Примените Data Loss Prevention (DLP) механизме унутар система
- ✓ Безбедна комуникација је кључна за заштиту осетљивих података.
- ✓ Комбинација савремених VPN и TLS протокола, енкрипције у мировању, Zero Trust приступа и праћења метаподатака значајно смањује ризик од неовлашћеног приступа и цурења података.
- ✓ Придржавање актуелних стандарда као што су NIST, ISO/IEC и PCI DSS, као и благовремено усвајање квантно-отпорних решења, обезбеђује дугорочну отпорност комуникационих система на савремене и будуће претње.

AUDIT & LOGGING – НАДЗОР И ЕВИДЕНЦИЈА ПРИСТУПА ТАЈНИМ ПОДАЦИМА

Све активности које укључују приступ, измену или пренос тајних и осетљивих података морају бити евидентиране у циљу форензичке анализе, откривања злоупотреба и унапређења безбедносних политика. Ефикасан систем логовања и ревизије (аудита) омогућава рано откривање аномалија, непоштовања процедура и потенцијалних безбедносних инцидената.

Кључне компоненте:

- **Централизовано логовање**
  - *Пример из праксе:* Сви системски логови из различитих сервера, апликација и мрежне инфраструктуре прикупљају се у централни SIEM систем (нпр. *Splunk, Graylog, ELK Stack*).
  - *Препорука:* Користити *syslog, journald* или агенте (нпр. *Filebeat)* за слање логова у реалном времену.
  - *Стандард:* ISO/IEC 27002 (раздела 12.4 – *Logging and monitoring*), NIST SP 800-92 (*Guide to Computer Security Log Management*).

- **Заштита и интегритет логова**
    - *Пример:* Коришћење дигиталног потписа или WORM (*Write Once Read Many*) медија да се спречи накнадна измена логова.
    - *Препорука:* Ограничи приступ лог фајловима само овлашћеним лицима; имплементирати контролу интегритета (хеширање, checksum).
    - *Стандард:* NIST SP 800-137 (Information Security Continuous Monitoring), ISO/IEC 27001 – Контрола приступа логовима.
- **Аутоматизовано упозоравање и анализа**
    - *Пример:* Ако администратор приступи поверљивим подацима у необично време или из непознате локације, SIEM шаље аларм.
    - *Препорука:* Подесити алате за откривање одступања (anomaly detection) и коришћење шаблона понашања (UEBA – User and Entity Behavior Analytics).
- **Форензички значај и правна ваљаност логова**
    - *Пример:* У судским поступцима логови морају бити временски потписани (timestamped), непромењени и прослеђени преко безбедног ланца чувања.
    - *Препорука:* Користити NTP за синхронизацију времена и применити процедуре дигиталне форензике.

Додатне препоруке:

- ✓ Чувати логове минимум 1–3 године у зависности од регулативе и степена тајности
- ✓ Редовно тестирати алате за детекцију инцидената и евиденцију
- ✓ Применити принцип најмањег привилегију и логовати покушаје неовлашћеног приступа
- ✓ Анонимизовати податке где је могуће без умањења надзорне функције
- ✓ Укључити логове у систем за управљање инцидентима (ISMS, CSIRT)

Систематичан и заштићен процес логовања и ревизије представља један од стубова безбедности података. Уколико се правилно имплементира, омогућава не само откривање, већ и превенцију злоупотреба, као и доказивање у случају спора. Праћење глобалних стандарда и осавремењивање система у складу са развојем претњи остаје континуиран задатак сваке организације која рукује осетљивим или тајним информацијама.

ACCESS CONTROLS – НАПРЕДНЕ КОНТРОЛЕ ПРИСТУПА И АУТЕНТИФИКАЦИЈЕ

Контроле приступа представљају прву линију одбране од неовлашћеног приступа тајним и осетљивим информацијама. Модерни системи приступа комбинују традиционалне методе идентификације са напредним механизмима као што су двофакторска аутентификација (2FA), биометрија, и динамичке политике приступа засноване на ризику.

Кључне компоненте:

- **Двофакторска и вишефакторска аутентификација (2FA/MFA)**
  - *Пример из праксе:* Пријава на корпоративни портал захтева лозинку + једнократни код са мобилне апликације (нпр. Microsoft Authenticator, Google Authenticator, YubiKey).
  - *Препорука:* Обавезно применити MFA за све администраторске налоге и приступ осетљивим подацима.
  - *Стандард:* NIST SP 800-63B (Digital Identity Guidelines).
- **Биометријска идентификација**
  - *Пример:* Приступ безбедносно осетљивим зонама уз проверу отиска прста, мреже крвних судова или препознавање лица.
  - *Препорука:* Комбиновати биометрију са другим факторима (n+1 модел).
  - *Напомена:* Биометријски подаци се морају третирати као посебна категорија личних података у складу са GDPR/ЗЗЛПД.
- **Контрола приступа на основу улога (RBAC – Role-Based Access Control)**
  - *Пример:* Систем администратор има шири ниво приступа него редовни корисник; контролисано кроз *LDAP/Active Directory*.
  - *Препорука:* Спроводити политику најмањих привилегија – сваки корисник има само она овлашћења која су му неопходна.
  - *Алтернатива:* ABAC (*Attribute-Based Access Control*) – флексибилније приступање засновано на више критеријума.
- **Контроле приступа у реалном времену**
  - *Пример:* Ако систем детектује пријаву из атипичне геолокације, захтева додатну аутентификацију или блокира приступ.
  - *Технологије:* CASB (Cloud Access Security Broker), Conditional Access Policies (нпр. Azure AD).
- **Временски и контекстуални приступ**
  - *Пример:* Привремени приступ за уговорне сараднике који се аутоматски поништава након одређеног датума.
  - *Препорука:* Користити *just-in-time* приступ (JIT), токене са временским ограничењем и ревизију свих привилегованих налога.

Додатне препоруке:

- ✓ Увести MFA као стандардну безбедносну меру у свим системима
- ✓ Аутоматизовати процес доделе и опозива приступа (IAM/IDM алати)
- ✓ Редовно ревидирати приступне листе и бришите неактивне налоге
- ✓ Водити евиденцију сваког приступа и покушаја приступа осетљивим подацима
- ✓ Комбиновати RBAC са контекстуалним факторима за финију контролу

Напредне контроле приступа не само да спречавају неовлашћен приступ, већ и смањују могућност интерних злоупотреба. Примена вишефакторске аутентификације, динамичких правила и принципа најмањих привилегија осигуравају да само овлашћени корисници, у одговарајућим условима, имају приступ тајним подацима. Редовно ажурирање приступних политика и коришћење међународних стандарда гарантује дугорочну безбедност.

DATA INTEGRITY – ОЧУВАЊЕ ТАЧНОСТИ И КОНЗИСТЕНТНОСТИ ПОДАТАКА

Интегритет података подразумева да информације остану непромењене, тачне и потпуне током уноса, обраде, преноса и складиштења. Нарочито у контексту тајних или осетљивих података, очување интегритета је критично за доношење исправних одлука, правну валидност и заштиту од злонамерних измена или корупције података.

Кључне компоненте:

- **Хеш функције и дигитални потписи**
  - *Пример из праксе:* Када се документ дигитално потпише (нпр. електронским сертификатом), хеш функција (SHA-256) се користи да би се проверила његова неизмењеност.
  - *Препорука:* Користити јаке криптографске хеш функције (нпр. SHA-256, SHA-3), избегавати застареле (нпр. MD5, SHA-1).
  - *Стандард:* NIST FIPS 180-4 (SHA), eIDAS (за дигиталне потписе у ЕУ), ISO/IEC 10118.
- **Целокупна провера интегритета у систему**
  - *Пример:* Контролне суме и верификација датотека након преноса преко мреже (нпр. *checksum, HMAC*).
  - *Препорука:* Имплементирати механизме за аутоматску проверу интегритета при свакој читању или преносу података.
- **Контрола верзија и ревизија измена**
  - *Пример:* Користе се системи као што су *Git* или базе са *audit trail*-ом да би се пратили сви изменски кораци и аутори измена.

- *Препорука:* Свака измена осетљивог податка мора бити евидентирана и одобрена кроз процедуру.

- **База података са заштитом интегритета**
  - *Пример:* SQL базе користе *constraint-е* (нпр. *CHECK, FOREIGN KEY*) и механизме за ACID трансакције.
  - *Препорука:* Омогућити логовање измена и редовно извршавати тестове конзистентности.
  - *Стандард:* ISO/IEC 25012 (*Data Quality Model*), NIST SP 800-53 (SI-7 – *Software, Firmware, and Information Integrity*).

- **Заштита од неовлашћених измена**
  - *Пример:* Фајл системи са неизмењивим секцијама (*WORM)*, контролисан приступ системским фајловима.
  - *Препорука:* Комбиновати контроле приступа (*ACL*) са системима за надгледање измена (*File Integrity Monitoring – FIM*).

Додатне препоруке:

- ✓ Користити криптографске методе за верификацију интегритета при сваком улазу/излазу
- ✓ Применити version control систем за све критичне конфигурације и документе
- ✓ Обезбедити отпорност на отказе кроз репликацију и периодичну валидацију података
- ✓ Регуларно тестирати политике интегритета у оквиру безбедносних провера
- ✓ Аутоматски алармирати на сваки покушај неауторизоване измене података

Интегритет података је темељ поверења у дигиталне системе. Без њега, ниједна безбедносна мера није довољна. Комбинацијом хеширања, дигиталног потписивања, контроле верзија и мониторинга интегритета, организације могу обезбедити да њихови подаци остану тачни, потпуни и поуздани у сваком тренутку.

SEGMENTATION – СМАЊЕЊЕ ПОВРШИНЕ НАПАДА КРОЗ ИЗОЛАЦИЈУ СИСТЕМА

Сегментација представља технику логичког или физичког дељења мрежних ресурса на мање, изоловане целине. Циљ је да се ограничи кретање потенцијалног нападача унутар система, успорава или онемогућава *lateral movement* и минимизује могућност компромитовања критичних ресурса.

Кључне компоненте:

- **Виртуелне LAN (VLAN) и подмреже (subnets)**

- *Пример из праксе:* Радне станице запослених у посебној VLAN мрежи, одвојено од серверског сегмента и мрежа за управљање.
- *Препорука:* Употребити различите VLAN-ове за кориснике, сервере, IoT уређаје и администраторске сервисе.
- *Стандард:* ISO/IEC 27033-1 (Network security overview and concepts).

- **Firewall правила и контролисана комуникација између сегмената**
  - *Пример:* Правила firewall-а омогућавају само строго дефинисане протоколе и портове између сегмената (нпр. SQL сервер прихвата упите само са одређене апликације).
  - *Препорука:* Применити принцип „дозвољено је само оно што је изричито дефинисано“ (***default deny***).
  - *Технологије:* Next-Generation Firewalls (NGFW), ACL (*Access Control Lists*).
- **Микросегментација**
  - *Пример:* Унутар истог дата центра или cloud окружења, свака апликација или сервис се налази у сопственој зони са посебним правилима.
  - *Технологије:* VMware NSX, Cisco ACI, Zero Trust архитектура.
  - *Препорука:* Увести микросегментацију у *cloud* окружењима ради боље контроле комуникације између виртуелних машина и контејнера.
- **Изолована окружења (sandboxing, DMZ)**
  - *Пример:* Web server у демилитаризованој зони (*DMZ*) изолован од унутрашње мреже – чак и у случају компромитације, нападач нема директан приступ базама података.
  - *Препорука:* Критичне услуге изместити у сегменте са контролисаним приступом кроз *proxy* или *reverse proxy* слојеве.

Додатне препоруке:

- ✓ Урадити мапирање постојећих ресурса и дефинисати зонирање по нивоу осетљивости
- ✓ Омогућити инспекцију саобраћаја између сегмената (Deep Packet Inspection)
- ✓ Минимизовати број отворених путева комуникације између зона
- ✓ Тестирати пропусност правила firewall-а и симулирати lateral movement Комбиновати сегментацију са Zero Trust приступом

Сегментација није само техничка мера, већ кључна стратегија у спречавању ескалације напада. Поделом система по критеријумима функције, осетљивости и нивоа ризика, смањује се могућност ширења малвера, експлоатације пропуста и компромитације целе мреже. Сегментација, у комбинацији са прецизним правилима приступа и мониторингом, представља темељ савремене одбране.

CONTINUOUS MONITORING – НЕПРЕКИДНО ПРАЋЕЊЕ РАДИ БЛАГОВРЕМЕНОГ ОТКРИВАЊА И РЕАГОВАЊА НА ПРЕТЊЕ

Continuous Monitoring представља процес сталног надгледања безбедносних догађаја, системских активности и конфигурација у реалном времену, са циљем раног откривања инцидената, одступања и потенцијалних злоупотреба. То је кључна компонента проактивне информационе безбедности и темељ за доношење одлука заснованих на подацима.

Кључне компоненте:

- **SIEM (*Security Information and Event Management*) системи**
  - *Пример из праксе:* Употреба алата као што су *Splunk, Wazuh,* или *IBM QRadar* за анализу логова, корелацију догађаја и аутоматско алармирање.
  - *Препорука:* Подесити корелационе правиле за специфичне безбедносне инциденте, као што су неуспеле пријаве, промена права приступа или exfiltration података.
  - *Стандард:* NIST SP 800-137 (*Information Security Continuous Monitoring – ISCM*), ISO/IEC 27001: A.12.4 (*Logging and monitoring*).
- **Endpoint Detection & Response (EDR)**
  - *Пример:* Алат као што је CrowdStrike или Microsoft Defender for Endpoint који омогућава увид у активности на крајњим уређајима, изоловање компромитованих система и форензичку анализу.
  - *Препорука:* Интегрисати EDR са SIEM системом за централизовани преглед.
- **Network Monitoring и IDS/IPS (Intrusion Detection/Prevention Systems)**
  - *Пример:* Коришћење *Zeek, Snort* или *Suricata* за праћење мрежног саобраћаја и откривање аномалија или познатих потписа напада.
  - *Препорука:* Комбиновати IDS са *threat intelligence* фидовима ради благовременог откривања нових врста претњи.
- **Анализа понашања (UEBA – User and Entity Behavior Analytics)**
  - *Пример:* Откривање девијантног понашања запосленог (нпр. масовно копирање фајлова у касним вечерњим сатима) као потенцијалног индикатора компромитације.
  - *Препорука:* Интегрисати UEBA са политиком инцидент реаговања (*Incident Response Playbook*).

Додатне препоруке:

- ✓ Успоставити базну линију (*baseline*) за нормално понашање система и корисника

- ✓ Конфигурисати аларме за критичне догађаје (нпр. приступ тајним подацима ван радног времена)
- ✓ Обезбедити централизовано логовање са временском синхронизацијом (*NTP*)
- ✓ Редовно вршити анализу логова и ревизију политике алармирања
- ✓ Успоставити SOC (*Security Operations Center*) или ангажовати MSSP (*Managed Security Service Provider*)

Континуирано праћење је незаобилазан део сваког зрелог безбедносног система. Омогућава правовремену реакцију на инциденте, откривање непознатих претњи и побољшање укупне резилијенције система. Увођењем SIEM, EDR и IDS решења, у комбинацији са процедуром за одговор на инциденте, организација гради основу за ефективну и одрживу сајбер одбрану.

ЗАКЉУЧЦИ И ПРЕПОРУКЕ

Заштита тајних и осетљивих података захтева системски, свеобухватан и континуиран приступ. Примена принципа као што су *Zero Trust, Defense in Depth, Security by Design* и *Least Privilege* није ствар избора, већ нужност у условима све сложенијих и упорнијих сајбер претњи. Анализом елемената као што су безбедни комуникациони канали, контроле приступа, интегритет и сегментација, уочава се да ефикасност безбедности произилази из координације техничких мера и организационих политика.

Модерне претње не погађају само технологију – оне циљају и људске пропусте, нефункционалне процедуре и недостатак обуке. Зато је потребно не само увести техничке мере заштите, већ и редовно едуковати кориснике, спроводити тестирања, као и унапређивати постојеће политике на основу актуелних стандарда и реалних инцидената.

Кључне препоруке:

- ✓ Интегрисати безбедност у све фазе система – од пројектовања до свакодневног коришћења.
- ✓ Применити вишеслојну заштиту (Defense in Depth) и сегментацију мрежних зона.
- ✓ Успоставити Zero Trust модел – сваки приступ се верификује, без аутоматског поверења.
- ✓ Обавезно користити шифровање података у мировању и при преносу.
- ✓ Омогућити напредну контролу приступа, укључујући двофакторску аутентификацију (MFA) и биометрију.
- ✓ Увести редовно праћење и анализу логова, као и праћење интегритета података.
- ✓ Континуирано едуковати запослене, са фокусом на препознавање и превенцију социјалног инжењеринга и других безбедносних инцидената.
- ✓ Редовно вршити тестирања (аудите, пенетрационе тестове) и ажурирања мера заштите у складу са стандардима (NIST, ISO/IEC, ENISA).

- ✓ Обавезна акредитација ИКТ система од посебног значаја пре пуштања у рад када се у њима обрађују тајни подаци, како би се потврдила усаглашеност са прописаним безбедносним захтевима и стандардима.

Успешна имплементација безбедносних мера омогућава организацијама да проактивно одговоре на изазове, минимизују ризик од компромитовања тајних података и очувају поверење корисника и институција. Информациона безбедност није једнократна иницијатива – то је динамичан, континуирани процес који захтева пажњу, ресурсе и ангажовање свих учесника у систему. Иако су напредни технички механизми и строго дефинисани процеси неопходни за заштиту тајних података, човек остаје најслабија карика у безбедносном ланцу.

Недостатак свести, недостатак едукације или немар могу довести до највећих пропуста и угрожавања националне безбедности, организационе безбедности или концепата поверљивости, интегритета и доступности информација. Због тога је стална едукација, подизање безбедносне културе и одговорно понашање свих који рукују тајним подацима основа ефективне информационе безбедности.

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 тајних 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.

- 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_tajnih_podataka-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)

О АУТОРУ

Проф. др Горан Д. Матић

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

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

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

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

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

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

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

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

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

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

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

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

Адреса електронске поште за заказивање онлине консултација:
online.konsultacije@nsa.gov.rs

Адреса електронске поште за заказивање актуелних обука: obuke@nsa.gov.rs

Адреса електронске поште за заказивање брифинга: termini.sertifikati@nsa.gov.rs

Web:

www.nsa.gov.rs