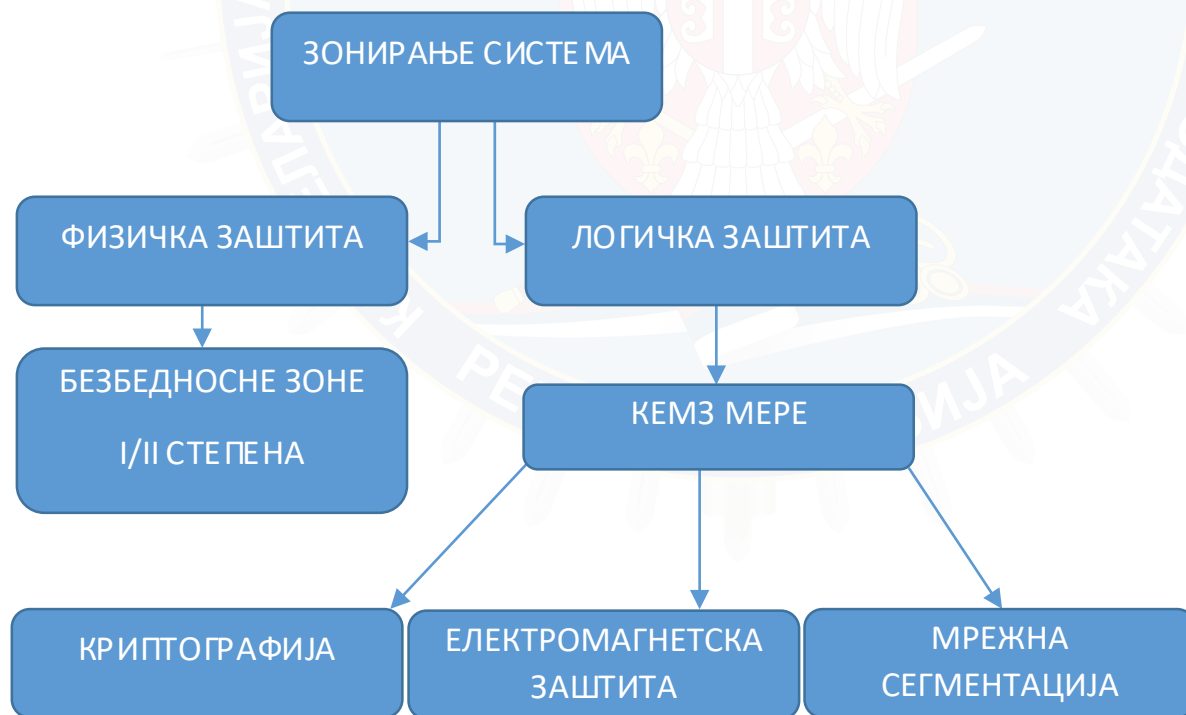




ЗОНИРАЊЕ ПРОСТОРА И СИСТЕМА – БЕЗБЕДНОСНЕ И АДМИНИСТРАТИВНЕ ЗОНЕ У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА И СИСТЕМИМА ЗА ОБРАДУ ТАЈНИХ ПОДАТАКА

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.





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

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.



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

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."



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

1. Правни основ

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.



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

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.



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

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.



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

5. TEMPEST мере - статус у Србији

Ставка	Стање
Лабораторија	Не постоји званична TEMPEST лабораторија.
Сертификација опреме	Није успостављен национални списак сертифициране 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 КСНБиЗТП)

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

Закључак

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.

Кључни савети:

1. **Крените од процене ризика** – Не морате спровести све одједном.
2. **Фокусирајте се на КЕМЗ** – Криптографија и мрежна сегрегација дају највећи ефекат.
3. **Документујте све** – Чак и одлуку да не примењујете TEMPEST (са образложењем).

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