



АКРЕДИТАЦИЈА ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Акредитација ИКТ система за рад са тајним подацима у Републици Србији, иако постоје одређене нејасноће у прописима, обавља се у складу са Законом о тајности података и Законом о информационој безбедности, као и подзаконским актима донетим на основу ова два закона. Процес акредитације обухвата две врсте:

1. **Безбедносна акредитација** - Ово обухвата физичку и административну заштиту података, као што су контрола приступа, обука запослених и примена мера заштите. Спроводи је Канцеларија Савета за националну безбедност и заштиту тајних података и друге институције, у зависности од врсте система.
2. **Технолошка акредитација** - Фокусира се на техничке аспекте као што су заштита од компромитације електромагнетним зрачењем (КЕМЗ) и примена специфичних безбедносних мера, на основу прописа о одбрани, укључујући ЕУ и НАТО стандарде.

У Републици Србији, постоје ИКТ системи који се регулишу посебним прописима у областима безбедности и одбране, унутрашњих и спољних послова.

Кључни кораци у процесу акредитације:

- Процена ризика: идентификација претњи и слабости система.
- Пројектовање и имплементација безбедносних мера: успостављање мера заштите као што су криптографија и контрола приступа.
- Документација и подношење захтева: подношење документације надлежним институцијама.
- Инспекција и верификација: провера усклађености са прописаним стандардима.
- Издавање акредитације: уколико је систем усклађен са технолошким и безбедносним захтевима, који се спроводи кроз стручни надзор Канцеларије Савета за националну безбедност и заштиту тајних података.
- Надзор и ревизија: регуларне провере безбедности и могућност опозива акредитације.

Недостатак прописаних услова, процедура и акредитационих тела

Услови за степене тајности

- Услови за степене тајности „ДРЖАВНА ТАЈНА“, „СТРОГО ПОВЕРЉИВО“ и „ПОВЕРЉИВО“ нису детаљно регулисани важећим прописима.
- Стандард SRPS ISO 27001 је довољан само за најнижи степен тајности „ИНТЕРНО“. Виши нивои тајности захтевају додатну регулативу и усклађеност са специфичним безбедносним захтевима и стандардима.



АКРЕДИТАЦИЈА ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Недостатак процедура за акредитацију

- У важећим прописима не постоји детаљно уређена процедура акредитације ИКТ система за рад са тајним подацима.
- Прописи пружају само општа начела која укључују процену ризика, примену безбедносних мера и основне кораке у акредитацији.

Недостатак акредитационих тела

- У Републици Србији не постоје одговарајућа акредитациона тела која би се бавила сертификацијом опреме и система за рад са тајним подацима.
- Република Србија је у великој мери ослоњена на увоз и усклађивање са стандардизацијом према страним телима, попут NATO SDIP и ЕУ листе.

КЕМЗ и TEMPEST: Шта је КЕМЗ у односу на TEMPEST?

- КЕМЗ (Компромитација електромагнетним зрачењем) представља шири концепт који обухвата техничке и организационе мере за спречавање цурења података путем електромагнетних емисија.
- TEMPEST је стандардизовани скуп техника и тестова за спречавање компромитације. Док КЕМЗ означава све мере заштите, TEMPEST је конкретно оријентисан ка сертификацији и тестирању уређаја (нпр. NATO SDIP-27).

Зонирање

Зонирање представља систематску поделу просторија у зоне различитих нивоа безбедности у складу са Законом о тајности података, Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима и Уредбом о посебним мерама физичко-техничке заштите тајних података:

- **Зоне високе безбедности** – садрже TEMPEST мере, криптографску опрему и физичке баријере (безбедносне зоне 1. и 2. степена).
- **Контролисане зоне** – просторије са ограниченим приступом и додатним мерама заштите (административне зоне).
- **Опште зоне** – просторије са основним мерама безбедности.



АКРЕДИТАЦИЈА ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Закључак

Процес акредитације у Републици Србији, иако још увек није уређен у потпуности, је важан за безбедност и усаглашавање са међународним стандардима. Иако се ослањамо на спољне стандарде, развој домаћих капацитета за акредитацију и сертификацију је кључан за будућност и већу безбедност и сигурност тајних података.

У складу са тренутним прописима, процес акредитације укључује како безбедносне аспекте у складу са прописима о тајности података, тако и технолошке аспекте у складу са прописима о информационој безбедности. Међутим, потребно је значајно унапређење у делу прописивања детаљнијих процедура и дефинисања компетенција акредитационих тела која би била у стању да сертифицију опрему и системе за рад са тајним подацима. Развој домаћих капацитета за акредитацију и сертификацију ИКТ система кључан је за унапређење безбедности тајних података и смањење зависности од страних регулаторних тела и стандарда.

Процес акредитације, иако формално није предвиђен прописима о раду са тајним подацима и информационој безбедности, у Републици Србији спроводи се кроз стручни надзор Канцеларије Савета за националну безбедност и заштиту тајних података, кроз оцену испуњености услова за рад са тајним подацима.

**КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ
И ЗАШТИТУ ТАЈНИХ ПОДАТАКА**

e-mail: office@nsa.gov.rs, kontakt@nsa.gov.rs

web: www.nsa.gov.rs