ИНТЕГРИСАНИ МОДЕЛ УПРАВЉАЊА РИЗИЦИМА У СИСТЕМУ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Систем заштите тајних података представља сложен и међусобно повезан скуп организационих, техничких и нормативних мера, чија ефикасност зависи од уравнотежене примене свих његових компоненти. Полазећи од те чињенице, овај материјал обједињује преглед кључних елемената система, њихових основних циљева и ризика који настају у случају њихове непримене. На тој основи извршена је процена ризика применом матрице вероватноће и утицаја, чиме се омогућава јасно идентификовање критичних тачака и рангирање приоритета у заштити тајних података.

У другом кораку, резултати процене ризика преведени су у структуриран план мера, који обезбеђује постепено и логично унапређење система — од адресирања најкритичнијих рањивости до уређења нормативних и уговорних аспеката. Овако постављен приступ омогућава рационално усмеравање ресурса, јачање отпорности система на инсајдерске и спољне претње, као и успостављање континуираног и одрживог механизма контроле и унапређења заштите тајних података.

Компактна табела која пореди све компоненте система заштите тајних података, њихов основни циљ и ризике у случају непримене:

Компонента система	**Основни циљ**	**Ризик ако се не примењује**
Регистарски систем	Уређено и контролисано руковање тајним подацима кроз евиденцију и акредитацију	Хаотично управљање, губитак података или њихово неовлашћено откривање
Персонална безбедност	Процена поузданости лица која имају приступ тајним подацима	Инсајдерске претње и злоупотреба овлашћеног приступа
Административна безбедност	Правилна одређивање и ознечавање тајности, као и престанак тајности	Погрешно означавање података и неконтролисано ширење информација
Физичка безбедност	Контрола простора и примена физичких заштитних мера	Неовлашћен физички приступ, крађа или уништење података
Информациона безбедност	Заштита ИКТ система, као и интегритета, поверљивости и доступности података	Сајбер напади, губитак интегритета и доступности информација
Индустријска безбедност	Заштита тајних података код извођача и подизвођача	Цурење поверљивих информација кроз уговорне односе
Контрола и надзор	Континуирана провера примене мера и систем извештавања	Формална примена без суштинске контроле и постојање скривених пропуста

Овако уређена табела омогућава да се на први поглед сагледа допринос сваке Компоненте систему у целини, као и кључни ризици који настају у случају њиховог занемаривања.

ИНТЕГРИСАНИ МОДЕЛ УПРАВЉАЊА РИЗИЦИМА У СИСТЕМУ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Матрица ризика (вероватноћа × утицај) за компоненте система заштите тајних података

Вероватноћа настанка ризика процењује се на основу учесталости појављивања догађаја у релевантном организационом и безбедносном контексту:

- **Висока вероватноћа** – догађај се очекује више пута у току једне године.
- **Средња вероватноћа** – догађај се може појавити у интервалу од једне до три године.
- **Ниска вероватноћа** – догађај је могућ, али се очекује ретко (у интервалу дужем од пет година).

Овако дефинисани критеријуми омогућавају уједначено и објективније вредновање ризика унутар система.

Компонента система	Вероватноћа	Утицај	Ниво ризика	Приоритет деловања
Персонална безбедност	Висока	Висок	**Критичан**	Највиши
Информациона безбедност	Висока	Висок	**Критичан**	Највиши
Регистарски систем	Средња	Висок	**Висок**	Висок
Физичка безбедност	Средња	Висок	**Висок**	Висок
Контрола и надзор	Средња	Висок	**Висок**	Висок
Административна безбедност	Средња	Средњи	**Средњи**	Средњи
Индустријска безбедност	Ниска–средња	Средњи	**Средњи**	Средњи

Објашњење:

- **Критични ризици**: *персонална* и *информациона безбедност* — инсајдерске претње и сајбер напади имају истовремено високу вероватноћу настанка и изузетно висок утицај на систем, што их позиционира као приоритет број један.
- **Високи ризици**: *регистарски систем*, *физичка безбедност* и *контрола и надзор* — пропусти у овим компонентама могу произвести озбиљне последице по интегритет система, иако је њихова вероватноћа по правилу нижа него код критичних ризика.
- **Средњи ризици**: *административна* и *индустријска безбедност* — иако значајне, ове компоненте имају релативно ограниченији домет последица или се пропусти чешће откривају кроз друге контролне механизме.

Структурисана матрица омогућава јасно приоритизовање ресурса, усмеравање надзорних активности и рационално планирање мера унапређења система заштите тајних података.

Иако су ризици у матрици приказани појединачно, у пракси постоји изражена међузависност компоненти система. Пропуст у једној области може иницирати ланац последица у другим сегментима заштите.

На пример, недовољно развијен систем **контроле и надзора** може довести до тога да се небезбедно понашање запосленог не уочи благовремено (**персонална безбедност**), што даље може резултирати неовлашћеним приступом или цурењем података услед недовољно заштићених ИКТ система (**информациона безбедност**).

Ова повезаност потврђује да се мере морају спроводити интегрисано, а не изоловано.

План приоритета мера за унапређење система заштите тајних података *(заснован на матрици ризика: вероватноћа × утицај)*

План је структуриран по нивоима ризика, тако да се најпре адресирају критичне рањивости система, а затим се мере постепено проширују на високе и средње ризике.

Иако је у плану мера административна безбедност сврстана у средњи приоритет у погледу имплементације, она представља **системски предуслов за функционисање свих осталих компоненти**.

Без јасно дефинисаног система класификације и управљања подацима:

- није могуће адекватно одредити ниво приступа (персонална безбедност),
- није могуће применити одговарајуће техничке мере (информациона безбедност),
- нити дефинисати услове физичке и индустријске заштите.

Из тог разлога, административна безбедност мора се успостављати **паралелно са критичним приоритетима**, као основа за доследно функционисање система.

За ефикасно праћење примене мера, неопходно је увести мерљиве индикаторе учинка:

- **Персонална безбедност**
  - Индикатор: 100% лица са приступом тајним подацима поседује важећи безбедносни сертификат.
  - Индикатор: реализоване обуке и проверено знање (тестирање запослених).
- **Информациона безбедност**
  - Индикатор: сви ИКТ системи акредитовани и документовани.
  - Индикатор: време реаговања на инциденте у складу са дефинисаним стандардима.
- **Контрола и надзор**
  - Индикатор: број спроведених контрола и проценат уочених неправилности које су отклоњене у року.

Ови индикатори омогућавају објективну процену успешности примене мера и континуирано унапређење система.

Критични приоритети (спровести без одлагања)

Персонална безбедност

- Успоставити и доследно примењивати строге процедуре провере лица (*background check*, издавање безбедносних сертификата).
- Увести континуирано праћење понашања запослених, уз функционалан систем за пријаву сумњивих активности.
- Организовати редовне обуке о инсајдерским претњама и безбедносној култури.

Информациона безбедност

- Спровести акредитацију ИКТ система и криптографске опреме.
- Увести вишеслојну заштиту: двофакторску аутентификацију, криптовање података и мониторинг мрежног саобраћаја.
- Успоставити и тестирати План реаговања на сајбер инциденте (*Incident Response Plan*).

Високи приоритети (спровести у кратком року)

Регистарски систем

- Успоставити јединствену и централизовану евиденцију за руковање тајним подацима.
- Увести стандардизоване процедуре за пријем, евидентирање, коришћење и уништавање података.

Физичка безбедност

- Успоставити контролу приступа просторијама (идентификационе картице, биометријски системи).
- Обезбедити видео-надзор и јасно дефинисане сигурносне зоне са физичким баријерама.

Контрола и надзор

- Успоставити функционалну унутрашњу контролу у органима јавне власти.
- Обезбедити редовно извештавање и спољни инспекцијски надзор од стране надлежних институција.

Средњи приоритети (спровести у средњем року)

Административна безбедност

- Уредити јасан и доследан систем одређивања, означавања и начина престанка тајности података.
- Увести униформне ознаке и стандардизоване процедуре за управљање службеним документима.

ИНТЕГРИСАНИ МОДЕЛ УПРАВЉАЊА РИЗИЦИМА У СИСТЕМУ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Поред уговорних обавеза и надзора, индустријска безбедност мора обухватити и **претходну безбедносну проверу извођача и подизвођача (due diligence) и прибављање одговарајућих сертификата за приступ тајним подацима за физичка и правна лица**. То подразумева процену:

- техничких и организационих капацитета за заштиту тајних података,
- кадровске поузданости,
- постојећих безбедносних политика и сертификата.

Без овакве провере, уговорне клаузуле остају формалне и не обезбеђују стварну заштиту података у ланцу снабдевања.

Поред тога, потребно је:

- Обезбедити да сви уговори са извођачима садрже обавезујуће клаузуле о заштити тајних података.
- Успоставити систематичан надзор над подизвођачима и поступцима поверљивих набавки.

Овако дефинисан план јасно утврђује редослед деловања:

1. **Прво** се стабилизују најосетљивије тачке система — персонална и информациона безбедност.
2. **Затим** се јачају системски механизми контроле — регистарски систем, физичка заштита и надзор.
3. **На крају** се уређују нормативни и уговорни аспекти — административна и индустријска безбедност.

Такав приступ омогућава рационално усмеравање ресурса, максимизацију ефеката мера и постепено, али свеобухватно јачање система заштите тајних података.

Интегрисани модел управљања ризицима у систему заштите тајних података није само нормативни оквир, већ представља оперативни инструмент који омогућава континуирано унапређење и јачање отпорности целог система. Његова вредност лежи у томе што повезује све компоненте заштите у једну функционалну целину, обезбеђује мерљиве индикаторе учинка и омогућава благовремено откривање и отклањање слабости. На тај начин, систем заштите тајних података постаје динамичан и одржив механизам, способан да се прилагођава новим претњама и изазовима, истовремено штитећи националне интересе и институционални интегритет.