ВОДИЧ КРОЗ ПРИМЕРЕ ЛОШЕ ПРАКСЕ У СИСТЕМУ РАДА СА ТАЈНИМ ПОДАЦИМА

веб: www.nsa.gov.rs

Проф.др Горан Д. Матић

Београд, 2025. година

Садржај

Увод

„Паметан учи на туђим грешкама, будала на својим — а неки ни тада ништа не науче.“

Руковање тајним подацима представља један од најосетљивијих аспеката функционисања државних институција, јавних органа и појединих правних лица. Одговорност коју носи рад са овом врстом информација захтева највиши степен професионализма, дисциплине и свести о потенцијалним ризицима који проистичу из било каквог одступања од прописаних процедура.

Тајни подаци обухватају информације чије би неовлашћено откривање, злоупотреба или губитак могли озбиљно да угрозе безбедност, интересе и међународне обавезе Републике Србије. У ту категорију спадају и подаци који су страни тајни или су третирани као тајни у складу са међународним споразумима и билатералним договорима.

Да би се обезбедило очување интегритета, поверљивости и доступности ових података, неопходно је успоставити свеобухватан систем заштите. Тај систем мора да укључује:

- јасно дефинисане безбедносне политике и процедуре,
- континуирану едукацију запослених,
- строг надзор приступа подацима и
- механизме реаговања у случају инцидента.

Инцидентом се сматра сваки догађај који је довео или би могао довести до компромитације тајних података — без обзира на то да ли је узрокован нехатом, техничким пропустом или злонамерним деловањем. Управо неадекватно поступање у оваквим ситуацијама представља основ за анализу лоших пракси.

Циљ овог водича је да кроз реалне примере укаже на критичне слабости у систему руковања тајним подацима, како би се подигла свест, ојачале процедуре и спречило понављање сличних пропуста у будућности.

Поступање у случају губитка, крађе, оштећења, уништења или неовлашћеног откривања тајних и страних тајних података

Уколико дође до сазнања о догађају који представља безбедносни инцидент у вези са тајним подацима, старешина органа јавне власти или овлашћено лице је дужно да без одлагања предузме низ мера у складу са законом. Ове мере имају за циљ утврђивање чињеничног стања, спречавање даљих штетних последица и документовање инцидента ради предузимања одговарајуће одговорности и заштите система. Основни кораци у поступању су:

1. **Утврђивање околности инцидента**
    - Идентификација узрока: да ли је у питању људска грешка, технички пропуст, злоупотреба, сајбер напад или други фактори.
    - Утврђивање обима и природе компромитованих података: који ниво тајности је у питању, која лица су имала приступ, који системи или физички простори су погођени.
2. **Процена настале штете**
    - Процена последица инцидента по националну безбедност, институционални интегритет, интересе органа или међународне обавезе.
    - Правна квалификација инцидента: да ли представља дисциплински, прекршајни или кривични догађај.
3. **Предузимање мера санације и спречавање поновног инцидента**
    - Техничке и организационе мере: привремена обустава приступа, изолација погођених система, ресетовање приступних права.
    - Интерна ревизија процедура, појачан надзор, додатне обуке запослених, провера безбедносних сертификата.
    - Јачање контролних механизама и преглед политика приступа и руковања.
4. **Израда извештаја о инциденту**
    - Извештај треба да садржи детаљан опис догађаја, анализу узрока, процену ризика, као и све мере које су предузете ради санације и спречавања сличних догађаја у будућности.
    - Извештај се доставља надлежним државним органима, као и другим субјектима у систему заштите тајних података, у складу са прописима.

Дефинисање безбедносног инцидента

Безбедносни инцидент представља сваки догађај, радњу или пропуст који је довео или може довести до неовлашћеног приступа, откривања, измене, уништења или губитка тајних података. Ово обухвата и стране тајне податке који

се налазе под заштитом на основу билатералних или мултилатералних уговора. Као инцидент се третира и свако одступање од прописаних мера заштите утврђених законом, подзаконским актима, безбедносним политикама или интерним процедурама институције. Инциденти могу бити:

- **Губитак** – физичко одсуство документа, уређаја или другог носача података, при чему није могуће утврдити где се подаци налазе.
- **Крађа** – неовлашћено преузимање тајних података од стране трећих лица.
- **Оштећење** – физичко или логичко оштећење носача података, услед чега је садржај угрожен.
- **Уништење** – трајно уклањање података без спровођења прописане процедуре за безбедно уништавање.
- **Неовлашћено откривање** – увид или приступ тајним подацима од стране лица која немају одговарајуће овлашћење или безбедносни сертификат.

Обавезе лица у систему заштите података

У складу са члановима 35. и 36. Закона о тајности података, свака особа која дође до сазнања да је дошло до безбедносног инцидента у вези са тајним подацима, дужна је да без одлагања обавести:

- старешину органа јавне власти,
- руковаоца тајних података у органу,
- овлашћено лице за заштиту тајних података.

Неиспуњавање ове обавезе сматра се пропустом који може имати озбиљне дисциплинске, прекршајне или кривичне последице, у зависности од конкретних околности и настале штете. Ова обавеза није ствар личне процене или дискреције — она произилази директно из закона и представља основу одговорног поступања у систему заштите поверљивих информација. Непоступање по наведеним обавезама третира се као пропуст који може водити ка озбиљним последицама, укључујући дисциплинску, прекршајну или кривичну одговорност, у зависности од тежине инцидента, степена настале штете и евентуалне намере или немара у поступању.

Правовремено и потпуно обавештавање представља не само законску обавезу, већ и кључни елемент очувања институционалне и националне безбедности. Оно мора бити део стандардне културе поступања сваке организације која ради са тајним подацима.

Карактеристике и правне последице инцидената

Сваки безбедносни инцидент има следеће заједничке карактеристике:

- Може бити резултат **намерне радње** (злоупотреба, саботажа, шпијунажа) или **ненамерне грешке** (нехат, непажња, недовољна обученост).
- Увек представља **одступање од прописаних мера заштите**, без обзира на последице.
- У зависности од тежине инцидента и његовог утицаја на безбедност, могуће су **различите правне последице**, укључујући дисциплинску одговорност, прекршајну казну или кривични прогон.

Сајбер безбедност и лоше праксе у руковању тајним подацима: Ризици и решења

Иако Република Србија још увек није успоставила потпуно формалан и свеобухватан нормативни оквир у области сајбер безбедности, постоје основе које омогућавају озбиљну анализу и деловање у овој области. Националне стратегије усмерене ка развоју информационог друштва, Закон о информационој безбедности, као и повезани регулативни документи, представљају платформу за сагледавање ризика и дефинисање мера заштите у сајбер простору. Србија не функционише као изоловано острво, већ као део глобалне мреже — у интеракцији са информационим екосистемима држава различитог степена технолошке развијености и различитих модела сајбер безбедности. Управо та повезаност, али и изложеност, захтева да се тема сајбер безбедности у раду са тајним подацима третира као приоритет у јавној управи и безбедносном сектору.

1. *Кључни проблеми сајбер безбедности* - Недовољна техничка заштита представља један од најозбиљнијих ризика по интегритет и поверљивост тајних информација. Уколико системи комуникације, уређаји и протоколи приступа нису усклађени са савременим безбедносним стандардима, ствара се простор за компромитацију података, неовлашћено коришћење и угрожавање институционалне или чак националне безбедности. Један од најчешћих пропуста односи се на комуникацију која не испуњава све безбедносне услове. Иако неке платформе као што је Viber користе енкрипцију, проблем може настати када се документи ознаке "строго поверљиво" размењују преко алата који нису намењени за професионалну размену тајних података. Није довољно да апликација има основну енкрипцију — потребно је да постоји вишеслојна заштита, управљање приступом и правна контрола над подацима. Gmail или WhatsApp, иако технички обезбеђују неки облик шифровања, често не задовољавају стандарде прописане за тајну преписку. Уз то, запослени понекад користе приватне адресе електронске поште за службене потребе, чиме се

директно крше прописане мере заштите и повећавају ризици од пресретања или злоупотребе садржаја.

Други проблем односи се на заштиту уређаја. Рад на персоналним рачунарима или мобилним телефонима без активиране енкрипције или антималвер заштите доводи до повећаних шанси за хаковање, злонамерни приступ и неовлашћено копирање или пренос података. У појединим случајевима, подаци остају доступни и након завршетка обраде, без одговарајућег брисања или архивирања.

Трећи аспект техничке неадекватности тиче се приступних механизама. Употреба једноставних лозинки које се лако погађају или деле усмено међу колегама представља озбиљну рањивост. Одсуство двослојне аутентификације при приступу системима значи да се целокупан безбедносни механизам ослања на један, често слаб, ниво заштите. У недостатку додатне верификације идентитета, све врсте злоупотребе остају реална претња.

Важно је разумети да технички пропусти нису искључиво ствар индивидуалне неодговорности, већ симптом ширег организационог оквира који није довољно развијен, едукован или контролисан. Сајбер безбедност се мора третирати као системско питање: са јасно дефинисаним процедурама, технолошком подршком и континуираном обуком свих запослених који имају приступ тајним подацима. Без таквог приступа, сви остали безбедносни механизми губе на ефективности.

2. *Лоше административне праксе* - Поред техничких недостатака, значајан ризик по безбедност тајних података и информација представљају и организационе слабости. Оне најчешће произилазе из недовољно уређених процедура, неодговорног приступа означавању степена тајности података, као и непостојања свеобухватне стратегије заштите. Такви пропусти утичу не само на смањење ефикасности постојећих механизама, већ стварају простор за злоупотребу, ненамерне грешке и компромитацију поверљивих информација.

У пракси, чест проблем представља непоштовање процедура означавања тајности. Документи се често одређују и означавају без озбиљне процене потенцијалне штете, што доводи до прекомерне или недовољне заштите појединих података и информација. Истовремено, евиденције и регистри тајних података у многим установама су неажурни или непотпуни, што узрокује губитак контроле над обимом, локацијом и категоријом тајних података.

Неовлашћени приступ подацима такође представља озбиљан организациони пропуст. У појединим случајевима, приступ тајним подацима добијају лица која нису прошла прописане безбедносне провере и не поседују одговарајући сертификат или чак страни држављани који не поседују одговарајућу дозволу за приступ тајним подацима. Физичке мере заштите често нису адекватно

спроведене — сервери остају откључани, документација се чува у неосигураним ормарима, а просторије са тајним подацима не контролишу се евиденцијом уласка и изласка.

Проблем додатно усложњава непостојање формално усвојених и примењених планова заштите тајних података. Органи јавне власти не располажу јасно дефинисаним стандардима који обухватају физичку и информациону безбедност. У пракси то значи да изостају елементарне мере као што су видео-надзор, контролисан приступ радним просторијама, антивирусна заштита и употреба firewall система који би надгледали мрежне активности и откривали сумњиво понашање.

Овакви недостаци не могу се решити појединачним напорима запослених. Они указују на системске празнине које захтевају институционални одговор. Успостављање јасних процедура, доследна примена контролних механизама и активно ангажовање руководства у креирању и спровођењу стратегија заштите представљају нужан предуслов за подизање безбедносних стандарда и очување поверљивости у раду са тајним подацима.

3. *Последице лоших пракси* - Пропусти у заштити тајних података, било да су техничке, организационе или повезане са понашањем појединаца, не остају без значајних последица. Уколико безбедносне мере нису примењиване доследно и ефикасно, последице могу бити озбиљне како по конкретну институцију, тако и по шири државни систем. Оне се јављају на различитим нивоима — од безбедносних ризика, преко правне одговорности, до дугорочног губитка поверења. Једна од најтежих последица јесте компромитовање националне безбедности. Цурење тајних података може угрозити фундаменталне интересе Републике Србије, укључујући одбрамбене структуре, спољнополитичке позиције и економску стабилност. Такве информације могу бити злоупотребљене од стране страних обавештајних служби, организованог криминала или појединаца са „лошим“ намерама, што Републику Србију излаже додатном спољном и унутрашњем притиску.

Уз безбедносне ризике, институције се могу суочити са правним санкцијама. Запослени и руководиоци сносе дисциплинску, прекршајну или кривичну одговорност, у складу са важећим законским актима, укључујући Закон о тајности података. Сама институција може постати предмет интерних ревизија, дисциплинских поступака или новчаних казни, што додатно урушава њену репутацију и оперативну стабилност.

Губитак поверења представља дугорочну последицу коју је тешко поправити. Нарушен углед установе у очима домаће и међународне јавности доводи у питање њену професионалност, поузданост и способност за одговорно

управљање повереним информацијама. Поновљени пропусти стварају трајан утисак системске неодговорности и институционалне слабости, што отежава сарадњу са партнерима и смањује кредибилитет у међусобним односима. Ове последице морају бити схваћене као озбиљно упозорење. Безбедност тајних података није питање формалне одлуке, већ захтева континуирану посвећеност, јасно дефинисане одговорности и висок степен свести међу свим актерима — од запослених на оперативном нивоу до доносилаца одлука у руководству.

4. *Препоруке за побољшање* - Ефикасна заштита тајних података не може се заснивати само на формалним процедурама или изолованим техничким решењима. Она захтева интегрисан приступ који обухвата техничке, административне и културолошке компоненте, прилагођене специфичностима установе и врсти података којима се управља. Само свеобухватним деловањем може се изградити отпоран систем који одговара на актуелне претње и системске слабости.

Најпре, неопходна је строга и доследна примена прописа. План заштите тајних података мора бити не само усвојен, већ и оперативно примењиван, са детаљно разрађеним процедурама које обухватају све фазе руковања тајним подацима — од одређивања и означавања до приступа, дистрибуције, као и архивирања и уништавања. Осим тога, обуке за запослене морају бити редовне, прилагођене ризицима у окружењу, и обавезно укључивати теме из области сајбер безбедности, уз конкретне примере, симулације и сценарије угрожавања.

Поред регулативе, кључну улогу имају технолошка решења. Примена савремених метода шифровања комуникације и података — укључујући VPN тунеле и TLS протоколе — представља минимум за сигуран рад са поверљивим информацијама. Установе би требало да имплементирају и системе за детекцију упада (IDS), који омогућавају благовремено откривање сумњивих активности и заштиту мрежне инфраструктуре пре него што дође до компромитације.

На крају, од пресудног значаја је културна промена у оквиру организације. Запослени морају бити охрабрени да пријављују безбедносне инциденте без страха од одмазде, кроз механизме који гарантују анонимност, заштиту и позитивно вредновање одговорног понашања. Руководство има обавезу да континуирано комуницира ризике, подржи превентивне мере, и својим примером покаже да се безбедносне процедуре не доживљавају као формалност, већ као основ професионалног и национално одговорног деловања.

Заштита тајних података више не може почивати искључиво на техничким решењима и регулативама — она захтева дубоку интеграцију свих аспеката безбедносне праксе. У контексту брзог технолошког развоја, транснационалног

протока информација и сложених безбедносних изазова, потребно је усвојити приступ који комбинује различите типове мера.

Најпре, неопходна је **континуирана едукација** запослених. Теоријско познавање прописа није довољно ако није праћено конкретним искуством — зато су симулације реалних инцидената и сценарија угрожавања кључне за изградњу оперативне способности у препознавању ризика и адекватном реаговању.

Поред тога, **инвестиције у технологију** представљају предуслов за поуздану заштиту. Примена енкрипције, аутентификационих механизама, системске детекције упада и надзора комуникације мора бити усклађена са највишим стандардима и стално прилагођавана новим облицима претњи.

На крају, посебну пажњу треба посветити **транспарентности и култури пријављивања пропуста**. Организације морају изградити механизме који омогућавају сигурно, анонимно и непристрасно пријављивање кршења, уз јасан институционални став да је сваки сигнал важан и да свако ко укаже на ризик доприноси заштити целог система.

Само кроз уравнотежену комбинацију ових елемената могуће је изградити отпоран, флексибилан и одговоран систем заштите који не само да одговара на претње, већ их проактивно спречава. Тајни подаци не смеју бити схваћени као формалност — већ као стратегијски ресурс, чија заштита представља стуб сигурности, кредибилитета и суверенитета државе.

Зашто запослени крше процедуре у раду са тајним подацима?

Психолошки аспекти проблема - Упркос строгим прописима и формалним процедурама, у пракси се запажа велики број одступања у раду са тајним подацима. Узроци ових пропуста често не леже у намери да се правила крше, већ у различитим психолошким и организационим механизмима који утичу на понашање запослених и постепено урушавају безбедносну културу. Кључни фактори који доприносе оваквим одступањима укључују:

- **Навику и аутоматизам** – Дугогодишње понављање истих задатака води ка рутинском приступу, где се прописане процедуре игноришу као „непотребне“ или „техничке сметње“.
- **Претерано самопоуздање** – Верујући да „грешка не може да се деси баш њима“, запослени неретко преузимају ризике без стварне процене могућих последица.
- **Страх од конфронтације** – У окружењима са израженом хијерархијом, запослени избегавају да пријаве неправилности из страха од негативних последица.

- **Временски притисак и стрес** – У условима интензивног рада, рокова и притиска, безбедносне процедуре често падају у други план у корист „брзог завршетка посла“.
- **Недовољно разумевање последица** – Ако запослени нису стално подсећани на важност и потенцијалну штету од несавесног поступања, развијају се ставови који омаловажавају ризике.

Ови фактори указују на потребу да се питање безбедности не сведе само на формално поштовање прописа, већ да постане тема системског деловања, континуиране едукације и културне трансформације унутар институција.

Сагледавајући свакодневну праксу у органима јавне власти и правним лицима који рукују са тајним подацима, издвајају се бројни фактори који суштински доприносе нарушавању безбедносних процедура:

1. *Илузија безопасности („ово неће ником нашкодити“)* - Један од најчешћих психолошких механизама који доводи до кршења процедура у раду са тајним подацима јесте утицај осећаја тривијалности. Запослени понекад развијају унутрашње уверење да „овај документ није толико битан“, што их наводи да занемаре прописане мере заштите. Такав став ствара простор за импровизацију и отвара врата неовлашћеном руковању подацима.

Овај начин размишљања често се подупире искуством из прошлости – ако ниједан претходни пропуст није био санкционисан или ако никада „ништа лоше није проистекло“ из неформалног поступања, запослени постепено стичу лажни осећај сигурности. Тај осећај води ка нормализацији ризичног понашања и слабљењу свести о потенцијалним последицама. Конкретне последице оваквог става укључују:

- непажљиво руковање поверљивим документима (остављање на непокривеним местима, неконтролисано умножавање, непрописно уништавање),
- разговарање о осетљивим информацијама ван простора предвиђених за безбедну комуникацију (у ходницима, кафетеријама или чак ван радне установе).

Управо оваква тривијализација безбедносних процедура представља тиха али озбиљна претња интегритету система заштите тајних података. Препознавање и деконструкција оваквих ставова морају бити кључни део сваке едукације и развоја безбедносне културе.

2. *Преоптерећеност и временски притисак* - Један од значајних узрока заобилажења процедура у раду са тајним подацима је притисак времена, односно

став да је ефикасност важнија од сигурности. Запослени често своју потребу да „заврше посао на време“ стављају испред захтева за поштовањем формалних безбедносних корака. Изјава попут „немам времена за све ове формалности“ указује на унутрашњи конфликт између оперативних обавеза и прописаних мера заштите. Осим тога, страх од санкција због кашњења — било да је реч о прекору, финансијским последицама или губитку поверења од стране надређених — често превагне над свешћу о последицама кршења безбедносних протокола. У таквом контексту, запослени могу проценити да је „боље ризиковати“ него „каснити“, не сагледавајући да тај ризик може имати далеко озбиљније последице.

Типичне последице оваквог приступа укључују:

- слање тајних података и других поверљивих информација путем несигурних комуникационих канала (нпр. стандардна е-пошта или апликације за дописивање без одговарајућих мера шифровања),
- употребу личних, непријављених уређаја за приступ или пренос тајних података, чиме се отвара простор за компромитацију система безбедности.

Овај облик лоше праксе није само индивидуални пропуст, већ сигнал да организациона динамика и управљање задацима нису усклађени са захтевима заштите података. Превентивно деловање мора обухватити не само додатне техничке мере, већ и промену перцепције времена као оправдања за заобилажење процедура.

3. *Социјални притисак и конформизам* - Још један значајан фактор који подстиче лошу праксу у раду са тајним подацима јесте социјални притисак, односно тенденција запослених да своје поступке прилагоде понашању већине или очекивањима хијерархије. Изрази попут „сви то раде“ указују на постојање нормализоване културе непоштовања процедура, у којој је кршење правила толико распрострањено да појединац осећа морално и професионално оправдање да следи такву праксу. Слично томе, подређеност хијерархијској структури може довести до пасивног прихватања небезбедног понашања – када запослени усвоје став „шеф је рекао да је у реду“, чак и ако то значи заобилажење званичних правила. Овакав облик конформизма, мотивисан жељом да се избегне конфронтација или казна, у суштини подрива систем одговорности. Последице оваквих механизама укључују:

- колективну толеранцију на кршење процедура, где ниједан члан тима не доводи у питање небезбедно понашање,
- игнорисање унутрашњих сигнала и упозорења, укључујући налазе контролних механизама или смернице безбедносних служби.

Социјална динамика унутар организације игра кључну улогу у формирању (или деформацији) безбедносне културе. Управо зато интервенције не смеју бити усмерене само на појединце, већ на читаве радне колективе, уз ангажовање руководилаца као носилаца позитивних вредности.

4. *Недовољна свест о последицама* - Недовољна свест о значају и вредности тајних података представља озбиљан психолошки и културолошки изазов у организацијама које се баве тајним подацима. Када запослени потцењују потенцијалну заинтересованост трећих страна, неретко се јавља став „ко би ово да украде?“, као да су тајни подаци релевантни само у неким „високобезбедносним“ сценаријима. Такав начин размишљања игнорише чињеницу да осетљиве информације могу бити мета не само страних служби већ и домаћих актера, криминалних група или чак конкуренције. Поред тога, одустајање од личне одговорности кроз мисао „није моја одговорност“ често води ка пасивном односу према безбедносним процедурама. Запослени у том случају почињу да виде заштиту података као задатак који припада неком другом — служби безбедности, надређеном или систему у целини. Такав став умањује лични ангажман и повећава ризик од пропуста који се могу спречити једноставном пажњом и здравим разумом. Последице овакве перцепције су директне и опасне:

- тајни подаци и документи се остављају на видљивим, неконтролисаним местима,
- лозинке или тајни подаци се усмено деле са колегама без верификације идентитета или потребе.

Укорењена индолентност према безбедности не сме бити прихваћена као културна норма. Повратак личне одговорности и изградња свести о стварним претњама представљају неопходан корак ка унапређењу праксе и јачању одбрамбеног капацитета организације.

5. *Осећај безнађа и апатије* - Један од најподмуклијих узрока лоше праксе у руковању тајним подацима јесте системска немотивисаност која произлази из дужег излагања нефункционалном систему. Када запослени почну да верују да њихови напори „ништа не мењају“ и да је „свеједно шта раде“, настаје атмосфера апатије и резигнације. Тај став се често изражава кроз реченице попут: „Шта више могу да урадим?“ — што је показатељ дубоког психолошког дистанцирања од одговорности. Недостатак поверења у механизме заштите додатно појачава проблем. Уколико се мере безбедности доживљавају као пука формалност, односно нешто што „постоји само на папиру“, запослени више не доживљавају прописе као релевантне или обавезујуће. То често настаје када систем не реагује адекватно на инциденте — било прикривањем случајева, избегавањем одговорности или недостатком казни. Последице овакве демотивације и губитка вере у систем могу бити озбиљне:

- намерно игнорисање правила, чак и у ситуацијама у којима је ризик очигледан,
- непоштовање физичке контроле, укључујући уношење личних уређаја у строго контролисана подручја, без одобрења или евиденције.

Овај облик одступања није питање индивидуалне одлуке, већ симптом дубљих организационих проблема. Да би се овакве појаве спречиле, неопходно је обновити поверење запослених у систем: кроз транспарентно деловање, доследну примену мера, и ангажовање запослених у креирању решења која имају смисла у реалном радном контексту.

Како побољшати ситуацију? - Да би се кроз системско деловање смањио број пропуста у заштити тајних података и подигла свест запослених, потребно је спровести низ мера које обухватају не само техничке аспекте, већ и дубоку промену у начину размишљања и функционисања организације.

1. Обуке са симулацијом реалних инцидената - Теоријско знање није довољно ако није поткрепљено практичним искуством. Зато се препоручује:

- омогућити да запослени доживе сценарије цурења података кроз симулиране ситуације,
- имплементирати реалистичне вежбе са моделима безбедносног угрожавања, које утичу на изградњу навика и убрзавају препознавање ризика у реалном окружењу.

2. Примена јасних санкција и позитивних подстицаја - Потребно је успоставити равнотежу између контроле и мотивације:

- доследно санкционисати прекршиоце у складу са важећим актима, без изузетака,
- награђивати запослене који покажу одговорност, самостално идентификују ризике и допринесу побољшању безбедносних стандарда.

3. Промена организационе културе - Безбедност тајних података мора постати саставни део радне етике:

- охрабрити свакодневне разговоре о безбедности, без формализма и страха,
- укључити безбедносне теме у редовне радне састанке и консултације како би се развила атмосфера поверења и заједничке одговорности.

4. Омогућавање анонимног пријављивања - Страх од одмазде често спречава запослене да реагују на уочене пропусте. Због тога је неопходно:

- успоставити механизме за сигурно и анонимно пријављивање инцидената,
- развијати поверење кроз доследну системску заштиту пријављивача, уз јасну поруку да организација подржава интегритет и храброст.

Кршење безбедносних процедура у раду са тајним подацима најчешће не представља изоловани чин неодговорности, већ је производ ширих околности: психолошких слабости, организационих недостатака и мањкавости у комуникацији. Тајни подаци, као осетљива категорија информација, захтевају системску одговорност и свеобухватан приступ који иде даље од формалних прописа. Да би се систем заштите подигао на виши ниво, неопходно је:

- унапредити радну организацију тако да безбедносне процедуре буду интегрисане у свакодневне токове рада, без додатног оптерећења;
- спроводити обуке које нису засноване искључиво на теорији, већ симулирају реалне ситуације и ојачавају индивидуалну и тимску реакцију на ризик;
- обезбедити јасан и доследан став руководства који показује да је безбедност – нарочито национална – ствар приоритета, а не административна формалност.

Иако је сваки запослени појединачно одговоран за поступање са тајним подацима, стварне и одрживе промене могу настати само ако целокупни систем пружа стабилну подршку, јасна правила и искрену мотивацију за њихово поштовање.

Примери из лоше праксе рада са тајним подацима

Наводимо неколико типичних и поучних примера из праксе који се могу користити у сврху едукације запослених у систему заштите тајних података. Ови примери имају за циљ да илуструју сложеност ситуација у којима може доћи до безбедносног инцидента и неопходност доследне примене безбедносних процедура. Примери су прилагођени за симулације, обуке и унутрашње провере спремности организације на поступање у критичним ситуацијама. Ови примери из праксе илуструју како се, чак и у условима примене важећих прописа, могу појавити ситуације у којима је одлучујућу улогу имала обученост, пажња и свест запослених о значају заштите података. У циљу превенције инцидената, овакви сценарији се препоручују као саставни део обуке, редовног вежбања и унутрашњих провера. Институционални одговор на овакве ситуације не сме бити

репресиван, већ усмерен на јачање система, унапређење културе безбедности и развој одговорности.

Системски пропусти - Неуспостављање система заштите тајних података у пракси органа јавне власти и правних лица на основу уговорног односа

У пракси се уочавају ситуације у којима субјекти који по својим надлежностима или на основу уговора рукују тајним подацима, не спроводе мере прописане Законом о тајности података, што доводи до системских безбедносних пропуста. У наставку се издвајају два репрезентативна примера:

а) Орган јавне власти без успостављеног система заштите: Један орган јавне власти континуирано обрађује тајне податке у оквиру општег канцеларијског пословања користећи информациони систем *е-Писарница*, али није донео план заштите тајних података, нити је одредио лице задужено за руковање тајним подацима. Иако у органу постоје безбедносно проверена лица, систематска примена закона изостаје, што доводи до тога да се тајни подаци циркулишу без прописане физичке и техничке заштите, без евиденције о приступу и ван одговарајуће евиденције руковања.

б) Рад са тајним подацима ван акредитованог простора: У другом случају, једно правно лице закључује уговор са органом јавне власти о обради тајних података. Иако је уговорена обрада у просторијама органа јавне власти, у пракси се послови обављају у седишту правног лица. Тај простор, међутим, није претходно акредитован од стране Канцеларије Савета за националну безбедност и заштиту тајних података, нити су утврђене и примењене процедуре руковања и чувања тајних података у складу са прописаним стандардима. Радници правног лица нису прошли безбедносну проверу у обиму који одговара нивоу тајности података са којима долазе у контакт, што представља вишеструко кршење закона и уговора.

Оцена: У оба случаја долази до компромитовања основних елемената система заштите тајних података – недефинисаност надлежности, одсуство контроле услова за обраду и чување, као и непоштовање принципа „потребно да зна“. Ови примери указују на неопходност да се, већ у фази планирања, разјасни где, ко и под којим условима може радити са тајним подацима, уз обавезну координацију са Канцеларијом Савета за националну безбедност и заштиту тајних података и укључивање безбедносно-техничких процедура у уговорне аранжмане.

Несистематизована радна места за рад са тајним подацима

Према Закону о тајности података, сваки орган јавне власти који поступа са тајним подацима мора у оквиру интерног нормативног уређења да изради Правилник о унутрашњем уређењу и систематизацији радних места, којим се јасно дефинишу послови, надлежности и услови за рад са тајним подацима, односно на сваком систематизованом радном месту предвиђа степен тајности којима лице запослено на том радном месту приступа у оквиру својих послова. Ова обавеза се посебно односи на рад са документима као што је План одбране, који по својој природи садржи податке највишег степена тајности. У пракси, међутим, јављају се случајеви где органи јавне власти:

- немају систематизована радна места за рад са тајним подацима;
- не дефинишу посебне позиције за рад на изради, чувању и обради докумената као што је План одбране;
- не повезују систематизацију са Листом овлашћених лица по принципу „потребно да зна“, што доводи до нејасноћа у надлежностима и одговорностима.

Овакви пропусти представљају кршење нормативне обавезе и доводе до:

- правне несигурности у поступању са тајним подацима;
- онемогућене примене мера персоналне и административне безбедности;
- повећаног ризика од неовлашћеног приступа и компромитовања поверљивих информација;
- угрожавања националне безбедности, нарочито у ванредним и кризним ситуацијама.

Пример из праксе: У једном министарству током контроле заштите тајних података утврђено је да нису успостављена посебна радна места за управљање Планом одбране, нити је систематизација усаглашена са Листом овлашћених лица. Запослени који су приступали овим документима радили су на другим радним позицијама без јасно дефинисаних надлежности и без додатне обуке за руковање са тајним подацима. Ова ситуација довела је до неодговорног руковања са материјалима са ознаком тајности и интерног безбедносног инцидента у виду неовлашћеног приступа тајним подацима.

Оцена: Несистематизовани радни односи у органима јавне власти директно угрожавају интегритет система заштите тајних података. Без јасне систематизације и дефинисаних надлежности, немогуће је применити адекватне мере контроле и одговорности, што повећава ризик од злоупотреба и компромитације података од значаја за националну безбедност. Стога је

неопходно што пре прилагодити систематизацију радних места нормативним захтевима и осигурати континуирану обуку и надзор.

Рад са тајним подацима без безбедносног сертификата

У складу са Законом о тајности података („Сл. гласник РС“, бр. 104/2009 и 36/2011), приступ подацима означеним као тајни може се одобрити искључиво лицима која су прошла прописану безбедносну проверу и којима је издат безбедносни сертификат одговарајућег степена. Ова процедура је предуслов за учешће у активностима које подразумевају руковање поверљивим информацијама, као што су израда и реализација одбрамбених планова, учешће у поступцима поверљивих јавних набавки или приступ документацији класификованој као „поверљиво“ или „строго поверљиво“.

У пракси, међутим, долази до одступања од овог правила, нарочито у ситуацијама када се орган јавне власти позива на хитност поступања. Један од забележених случајева односи се на запосленог у једном министарству, који је ангажован на изради техничке документације у оквиру израде плана одбране Републике Србије. Иако није поседовао безбедносни сертификат, лице је добило приступ материјалу који садржи податке означене као „поверљиво“, уз образложење да је реч о хитној фази израде и да је у питању „унутрашњи тим“. Нити је обезбеђена привремена мера приступа, нити је покренута процедура безбедносне провере.

Слична пракса забележена је и у поступку поверљиве јавне набавке за набавку комуникационе опреме за један орган у саставу. Члан радне групе задужен за техничке спецификације, иако није поседовао безбедносни сертификат, учествовао је у припреми конкурсне документације која садржи детаље о шифрованим каналима и мрежној архитектури, означеним као „поверљиво“.

Оцена: Овакви случајеви представљају озбиљно кршење закона и подривају институционални систем заштите тајних података. Позивање на „хитност“ не може бити легално оправдање за заобилажење безбедносне провере, јер закон не познаје изузетак од примене ових мера. Учешће лица без безбедносног сертификата у процесима који подразумевају рад са поверљивим информацијама доводи до ризика од неовлашћеног откривања података, правне неодрживости аката и губитка поверења међу органима државе. У свим наведеним случајевима постоји потенцијал за покретање дисциплинских поступака, а уколико дође до компромитације података, и за кривичну одговорност у складу са чл. 98. Закона о тајности података.

Приступ тајним подацима без претходне безбедносне провере и одобрења

Према Закону о тајности података („Сл. гласник РС“, бр. 104/2009 и 36/2011), приступ информацијама означеним као тајна дозвољен је само лицима која су успешно прошла безбедносну проверу, поседују важећи безбедносни сертификат одговарајућег степена и имају одобрење надлежног органа на основу принципа „потребно да зна“ (need-to-know). И План заштите тајних података, као интерни документ органа, предвиђа низ мера којима се обезбеђује да се приступ ограничи само на она лица којима су подаци заиста неопходни за извршавање службених дужности.

У пракси, међутим, долази до озбиљних одступања од овог законског оквира. У једном органу државне управе, приликом припреме стратешког документа уступљеног од стране другог органа јавне власти, који садржи податке означене као „строго поверљиво“, административном службенику, који није поседовао безбедносни сертификат нити је био пријављен као лице које има потребу да зна, омогућен је непосредан приступ том материјалу ради „помоћи у техничкој припреми документа“. Приступ је омогућен усменом наредбом руководиоца, без икаквог евидентирања у књизи корисника, супротно одредбама чл. 45. и 46. Закона о тајности података.

У другом случају, током ревизије планских докумената у једном министарству, интерна радна група је делила докумената означена као „поверљиво“ преко интерне електронске поште, без провере да ли су сва лица у „мејлинг листи“ уопште сертификована и пријављена за приступ. Испоставило се да је у преписци учествовало и лице запослено у подршци ИТ сектора које нема службену потребу да приступа тим подацима.

Оцена: Овакви пропусти представљају озбиљно кршење основних начела безбедносне културе и режима заштите тајних података. Омогућавање приступа лицима без безбедносне провере, без сертификата и без одобрења по принципу „потребно да зна“, резултира директном компромитацијом података и прави простор за интерне и екстерне злоупотребе. Последице могу бити вишеструке: од повреде законских процедура и дисциплинске одговорности, до угрожавања оперативне безбедности, правне неодрживости донетих одлука и — у крајњем исходу — повреде интереса националне безбедности. Систем интерне контроле, евиденције и управљања приступом мора се унапредити, уз обавезну одговорност руководилаца за евентуално допуштање неовлашћеног приступа.

Третирање тајних података као да нису под заштитом

Један од најтежих пропуста у примени мера заштите тајних података у органима јавне власти огледа се у поступању са подацима означеним као „поверљиво“ или „строго поверљиво“ као да се ради о обичним, неограниченим информацијама. Иако Закон о тајности података, као и подзаконски акти и интерни планови заштите, строго прописују услове под којима се овакви подаци смеју чувати, обрађивати и преносити, у пракси се бележе бројни случајеви потпуног игнорисања ових обавеза.

У једном органу извршне власти, службеник је приликом састављања дописа који садржи елементе из документације означене као „строго поверљиво“ послао радну верзију текста на приватну Gmail адресу свог колеге ради „брже координације“. Документ није био шифрован, није обележен ознаком тајности у фајл систему, нити је поступак пријављен службенику задуженом за заштиту података. Рад са тајним подацима регулисан је Законом о тајности података („Службени гласник РС“, бр. 104/2009), који у члановима 35, 36, 38 и 48 прецизира начин чувања, преношења, поступања у случају инцидената, као и услове за издавање безбедносних сертификата. Ови прописи су правна основа за све безбедносне мере и процедуре које морају да се спроводе у органима јавне власти и другим субјектима који раде са тајним подацима, који се детаљине уређују интерним актима односно планом заштите тајних података у органу јавне власти.

Други чест пример представља непоштовање физичке заштите докумената. Током једне интерне контроле у министарству, утврђено је да су материјали означени као „поверљиво“ држани на радним столовима, у незакључаним фиокама или чак у отвореним полицама канцеларија до којих приступ има велики број запослених и лица без безбедносне провере. У неким ситуацијама, такви документи су били изложени током састанака са спољним сарадницима, без икакве евиденције о приступу или претходне сагласности.

Оцена: Третирање тајних података као да нису под заштитом представља системску слабост која открива недостатак елементарне безбедносне културе унутар органа јавне власти. Такво поступање доводи у питање не само интегритет података, већ и кредибилитет институције. Неовлашћени пренос преко несигурних канала, попут јавних електронских платформи (Gmail, Yahoo, Dropbox), отвара могућност пресретања од стране страних служби, индустријске шпијунаже, као и ненамерног „цурења“ информација. Непоштовање физичке заштите омогућава увид или фотографисање података од стране посетилаца, особља за одржавање, или било ког другог неовлашћеног лица.

Такви пропусти нису само индивидуални – они су показатељ да орган није адекватно спровео обуку, надзор и контролу примене мера из Плана заштите тајних података. Потребно је систематски увести:

– **редовне обуке запослених**,
– **проверу коришћења електронских система**,
– **енфорсмент политике чувања докумената** (нпр. аутоматско закључавање фиока, ограничен приступ просторијама),
како би се ови ризици свели на минимум.

Самовољно одређивање тајности од стране неовлашћених лица

Према члану 9. Закона о тајности података, тајност податка може да одреди искључиво овлашћено лице, у складу са законом. Овлашћена лица су, између осталих, председник Народне скупштине, председник Републике, председник Владе, руководилац органа јавне власти, као и друга лица која су за то писмено овлашћена од стране руководиоца органа јавне власти. Значајно је да се овлашћења за одређивање тајности не могу преносити на друга лица (члан 9. став 2. тачке 5 и 6).

Поступак одређивања тајности податка регулисан је чланом 10. истог закона, према коме овлашћено лице мора да одреди тајност податка приликом његовог настанка, односно када орган јавне власти започне обављање посла чији је резултат настанак тајног податка. Изузетно, тајност може бити одређена накнадно, ако се испуне законом прописани критеријуми. При томе, овлашћено лице процењује могућу штету по интерес Републике Србије која би могла настати откривањем тог податка. Такође, свако лице запослено у органу јавне власти дужно је да обавести овлашћено лице о подацима који би могли бити одређени као тајни, у оквиру својих радних задатака (члан 10).

У пракси се, међутим, јављају случајеви када неовлашћени службеници — често административни сарадници или други запослени без пуног овлашћења — самовољно означавају документа као „Поверљиво“ или „Строго поверљиво“, без спровођења прописане процедуре и ван институционалног оквира. Овакво поступање представља кршење законских одредби и злоупотребу система заштите тајних података. Такве радње могу довести до правне несигурности, ометања нормалног рада органа јавне власти и смањења транспарентности у управљању тајним подацима.

Оцена: Ова појава је озбиљан безбедносни ризик, јер се тиме угрожава системска контрола и поузданост ознаке степена тајности података. Самовољно означавање података без овлашћења и без примене законске процедуре доводи до неоснованог ограничења приступа, потенцијално ремети ток послова и може

резултовати правним и дисциплинским последицама по одговорна лица. Стога је неопходно јасно инсистирати на поштовању надлежности прописаних Законом о тајности података и осигурати сталну контролу и обуку запослених у органима јавне власти о законским процедурама у вези са одређивањем тајности.

Непоштовање процедура заштите тајних података

У складу са Планом заштите тајних података, сваки орган јавне власти дужан је да успостави, одржава и доследно примењује прописане интерне процедуре које се односе на чување, пренос, обраду и уништавање тајних докумената. Ове интерне процедуре морају бити усклађене са прописаним мерама физичке, информационе и административне безбедности, како би се обезбедила непрекидност и интегритет система заштите поверљивих података.

Међутим, у пракси се срећу бројни примери где државне агенције нису успоставиле формализоване и применљиве интерне процедуре за рад са тајним подацима. У таквим случајевима, документи са ознаком „Поверљиво“ или „Строго поверљиво“ често се чувају у неосигураним ормарима или на радним површинама без одговарајуће физичке заштите. Такође, неретко се дешава да се поверљива документа бацају у обичне корпе за отпад, без примене прописаних и стандардизованих метода уништавања као што су физичко или хемијско уништавање, које гарантују немогућност поновног коришћења или откривања садржаја.

Један од честих пропуста је и чињеница да се тајни документи израђују на рачунарима који су повезани на интернет, без адекватних мера заштите, што отвара могућност неовлашћеног приступа или компромитовања података. Ипак, након штампања, ти документи се заведу и третирају као тајни, али такав поступак не неутралишу ризик који је већ настао током њихове израде на рачунарима повезаним на отворену мрежу.

Овакав поступак представља директно кршење одредби Закона о тајности података, нарочито чланова који прописују обавезе у вези са физичком и информационом безбедношћу тајних података. Последице оваквог занемаривања су вишеструке: компромитовање поверљивих информација, појава ризика од неовлашћеног откривања и злоупотребе, као и потенцијални губитак података који могу имати озбиљан утицај на националну безбедност. Такође, нарушава се и поверење у институционални систем заштите тајних података, што може додатно ослабити интегритет и кредибилитет органа јавне власти.

Оцена: Непоштовање утврђених интерних процедура заштите тајних података указује на недостатак свести о значају безбедности поверљивих информација и показује слабости у организационој култури и управљању безбедношћу.

Препоручује се хитно унапређење обука, јачање контролних механизама и редовна контрола примена интерних процедура у свим институцијама које рукују тајним подацима. Само доследна примена прописаних интерних процедура може гарантовати поуздану заштиту и смањити ризик од инцидената који могу имати озбиљне последице по државну безбедност.

Рад са тајним подацима на незаштићеним ИКТ системима

Према Закону о тајности података, Закону о информационој безбедности и смерницама из Плана заштите тајних података, рад са тајним подацима мора се обављати искључиво у оквиру безбедносно акредитованих информационо-комуникационих (ИКТ) система. Ови системи морају испуњавати прописане стандарде информационе безбедности, укључујући криптографску заштиту, контролу приступа, физичку безбедност и примену најбољих пракси у складу са међународним стандардом SRPS ISO/IEC 27001.

Ипак, у пракси се, нажалост, често јављају случајеви где службеници користе личне уређаје, без икаквих техничких заштита, за приступ тајним подацима, повезујући се на јавне или незаштићене Wi-Fi мреже у кафићима, хотелима и другим непровереним окружењима. Ова пракса представља грубо кршење како Закона о тајности података, тако и Закона о информационој безбедности, као и интерних процедура из Плана заштите тајних података. Неадекватна заштита у оваквим случајевима доводи до ризика од сајбер напада, неовлашћеног прислушкивања и компромитовања тајних података. Осим што угрожавају националну безбедност и интегритет система заштите тајних података, овакве праксе нарушавају и поверење у рад државних органа.

Стога, у складу са принципима SRPS ISO/IEC 27001, неопходно је обезбедити и континуирано унапређивати безбедносне контроле, спроводити редовне процене ризика, као и пружати адекватне обуке запосленима за рад са тајним подацима и другим штићеним пдоацима у безбедном окружењу.

Оцена: Рад са тајним подацима на незаштићеним ИКТ системима указује на значајне пропусте у примени важећих закона и стандарда. Неопходно је увести стриктније контроле приступа, техничке мере безбедности и сталне едукације запослених. Интеграција Закона о тајности података, Закона о информационој безбедности и стандарда SRPS ISO/IEC 27001 представља основ за одрживу и ефикасну заштиту тајних података а тиме и националне безбедности.

Непостојање безбедносних зона у објектима где се рукује тајним подацима

У складу са члановима 9–15 Уредбе о посебним мерама физичко-техничке заштите тајних података („Сл. гласник РС”, бр. 97/2011), сваки орган јавне власти је дужан да на основу процене могућег нарушавања безбедности тајних података дефинише административну и безбедносне зоне (I или II степена). Безбедносне зоне су намењене за рад са подацима класификованим као „ПОВЕРЉИВО”, „СТРОГО ПОВЕРЉИВО” и „ДРЖАВНА ТАЈНА” и морају бити физички и технички обезбеђене у складу са прописаним стандардима (SRPS EN). Мере укључују: надзор, контролу приступа, забрану уношења неовлашћене опреме, физичко и електронско обезбеђење, као и редовне противприслушне прегледе.

У пракси, међутим, бројни органи јавне власти не успостављају безбедносне зоне, па се тајни документи чувају у просторијама без видео надзора, без контроле улаза и излаза, без физичког или електронског обезбеђења, па чак и без закључавања. Осим тога, често се не воде евиденције о приступу, нити се издају безбедносне пропуснице, иако је то обавеза из члана 14. Уредбе. Ово све се правда недостатком одговарајућег простора, финансијских средстава, кадровским проблемима и осталим пригодним разлозима за непоступање са тајним подацима.

Такав начин руковања представља директно кршење како Закона о тајности података, тако и подзаконских аката који га разрађују, а посебно Уредбе о мерама физичко-техничке заштите. Уз то, непоштовање ових обавеза угрожава интегритет система заштите, јер омогућава неовлашћен приступ, прислушкивање или несанкционисано изношење података.

Оцена: Непостојање безбедносних зона и непоштовање физичко-техничких мера заштите прописаних Уредбом, озбиљно компромитује безбедност тајних података. Одсуство минималних безбедносних стандарда представља системски пропуст који директно угрожава националну безбедност и тражи хитно поступање надлежних органа ради успостављања законске и техничке дисциплине у руковању тајним подацима.

Неуспостављање привремене безбедносне зоне током имплементације Закона у органу јавне власти

У поступку увођења система заштите тајних података у органима јавне власти, посебно током прелазних фаза имплементације Закона о тајности података („Службени гласник РС“, бр. 104/2009), може бити неопходно привремено установити безбедносне зоне ван акредитованих просторија. Успостављање таквих зона дозвољено је у складу са проценом ризика, оперативним потребама

и расположивим техничко-организационим капацитетима органа, на основу Уредбе о посебним мерама физичко-техничке заштите тајних података („Службени гласник РС“, бр. 97/2011), којом је предвиђено да се мере физичке заштите примењују сразмерно степену тајности и процењеним претњама.

Примери ситуација у којима се успостављају привремене зоне:

- почетак имплементације закона;
- реконструкција или адаптација сталних просторија;
- теренско руковање поверљивим подацима;
- увођење или ревизија система заштите;
- ванредне, кризне или привремене активности обраде тајних података изван редовних капацитета.

Привремене безбедносне зоне морају бити јасно дефинисане у интерним актима, физички обезбеђене (контрола приступа, надзор, забрана уношења неовлашћене опреме), уз вођење евиденције свих лица која улазе и бораве у простору. Сви поступци у тим зонама морају бити усклађени са интерним процедурама садржаним у Плану заштите тајних података, као и са захтевима стандарда SRPS ISO/IEC 27001 и Закона о информационој безбедности („Службени гласник РС“, бр. 6/2016, 94/2017 и 77/2019).

Употреба рачунара повезаних на интернет у привременим зонама представља посебан ризик. У складу са важећим прописима, тајни подаци не смеју се чувати или обрађивати на уређајима који имају приступ јавним мрежама. Уколико се из оперативних разлога привремено користи такав уређај, он мора бити технички изолован од мреже (off-line режим), а документ се након штампања заводи и даље третира у складу са нивоом тајности. Оваква привремена решења могу се применити само изузетно и никако не смеју постати системска пракса нити оправдати одсуство успостављања стално акредитованих зона.

Неуспостављање привремене безбедносне зоне у прелазним фазама имплементације представља кршење одредаба Уредбе и интерних аката (План заштите), чиме се отвара простор за циркулацију тајних података у неадекватно заштићеним просторима. Такав приступ ствара формални привид примене закона, док суштински доводи до озбиљне рањивости система, ризика од неовлашћеног приступа, цурења података и компромитовања поверљивих информација.

Оцена ризика и препорука - Привремене зоне морају испуњавати највише стандарде заштите, у мери у којој је то технички и оперативно могуће. Изостанак успостављања адекватног привременог режима, нарочито у осетљивој фази увођења система заштите, угрожава кредибилитет органа јавне власти и

интегритет целокупног система. Тај пропуст је нарочито ризичан јер се јавља у тренутку највеће институционалне рањивости — у прелазу са неуређеног на уређени режим заштите.

Поверљиве набавке без спроведених безбедносних процедура

Поверљиве јавне набавке, посебно у секторима одбране, безбедности и критичне инфраструктуре, морају се спроводити у складу са Законом о тајности података („Сл. гласник РС“, бр. 104/2009), као и Законом о јавним набавкама („Сл. гласник РС“, бр. 91/2019). Основни предуслов за учешће у оваквим поступцима јесте да добављачи поседују одговарајућу безбедносну акредитацију, тј. сертификат о способности да поступају са тајним подацима у складу са прописаним стандардима физичке, техничке и организационе заштите.

Поред тога, Уредба о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа („Сл. гласник РС“, бр. 63/2013) прописује обавезне мере које се морају спровести када се поверљиви послови поверавају трећим лицима. Ова уредба прецизира да је потребно утврдити да ли уговорни партнер има одговарајуће техничке, просторне и кадровске услове, као и дефинисане процедуре за руковање тајним подацима у складу са степеном тајности.

У пракси, међутим, забележени су случајеви у којима органи јавне власти који и сами нису имплементирали Закон о тајности података, реализују набавке осетљиве опреме (нпр. система за мониторинг комуникација, намена криптографских средстава или контролних уређаја) од правних лица — привредних субјеката који:

- немају безбедносни сертификат,
- немају акредитован простор и техничке капацитете за рад са тајним подацима,
- нису спровели безбедносне провере запослених који рукују поверљивом документацијом.

У многим ситуацијама, техничка документација која садржи елементе са ознаком тајности (нпр. упутства за конфигурацију, параметре интеграције у постојеће системе) доставља се у незаштићеном облику, ван безбедносне зоне, без протоколисања, евиденције или надзора од стране овлашћеног лица за заштиту тајних података. На тај начин, поступање органа директно нарушава чланове 30–33. Закона о тајности података који прописују обавезу заштите тајних података у свим фазама обраде.

Нарочито је ризично када се, позивајући се на „хитност поступка“, изоставе безбедносне провере и акредитације, без да је донета званична одлука о хитности у складу са чланом 36. Закона о јавним набавкама, нити је сачињена процена ризика у складу са Законом о информационој безбедности („Сл. гласник РС“, бр. 6/2016, 94/2017, 77/2019).

Током спровођења поверљиве набавке техничке опреме за потребе једног органа јавне власти, утврђено је да изабрани добављач није имао важећу безбедносну акредитацију, нити је располагао прописаним условима за рад са тајним подацима, као што су акредитовани простори и обука запослених. У складу са тим, приликом предаје техничке документације нису примењене прописане безбедносне мере — документација је била достављена ван безбедносне зоне и без пратеће евиденције.

Ова ситуација указала је на неопходност пооштравања контроле и праћења безбедносних процедура приликом поверљивих набавки, као и на важност доследне примене Уредбе о о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа („Службени гласник РС“, бр. 63/2013). На основу извршене анализе, препоручено је увођење обавезне провере безбедносне акредитације добављача пре закључења уговора, као и обавезног праћења примопредаје тајних података уз евиденцију и надзор овлашћеног лица.

Оцена: Поверљиве набавке захтевају висок степен одговорности и формалне безбедносне процедуре које морају бити унапред дефинисане, а не ретроактивно оправдаване. Изостанак безбедносне акредитације правних лица и формалне процене ризика доводи у питање легалитет поступка, угрожава тајност података и подрива поверење у капацитете државних органа да адекватно штите информације од значаја за националну безбедност.

Објављивање тајних података у медијима без претходне процедуре скидања тајности

Према Закону о тајности података, подаци који су одређени као „СТРОГО ПОВЕРЉИВО“ подлежу строгом режиму заштите, а њихово откривање неовлашћеним лицима може нанети неотклоњиву штету интересима Републике Србије. У пракси, јављају се случајеви у поверљивим јавним набавкама где су технички параметри и конфигурације опреме која садржи поверљиве податке достављени медијима или јавности без спровођења прописаних процедура скидања тајности. На пример, током једне набавке безбедносне опреме за потребе једно органа јвне власти, поједини делови техничке документације означени као „СТРОГО ПОВЕРЉИВО“ били су објављени у јавности без претходне формалне процедуре укидања тајности. То се догодило услед непажње и недовољне

контроле приликом предаје докумената трећој страни која није имала сертификат за приступ поверљивим подацима. Овакав пропуст је резултирао потребом за хитним интерним поступком процене штете и ревизијом мера заштите у оквиру институције. Овакво поступање може довести до:

- компромитовања безбедносних система и пословних тајни;
- угрожавања интегритета и поверења у државне органе;
- губитка конкурентске предности добављача и могућих правних последица;
- повећања ризика од индустријске шпијунаже и злоупотребе информација.

У оваквим случајевима, надлежни орган је дужан да:

- хитно процени штету и покрене поступак заштите;
- утврди узроке пропуста и одговорност;
- предузме мере за спречавање даљег ширења информација;
- спроведе обуку и подигне свест запослених о значају контроле приступа поверљивим подацима.

Оцена: Објављивање поверљивих података без претходне процедуре скидања тајности представља озбиљан безбедносни пропуст који подрива систем заштите информација од значаја за националну безбедност. Посебно у области поверљивих набавки, где су подаци често од стратешког значаја, неопходно је строго придржавање прописа и увођење јасних контролних механизама. Примери из праксе показују да се овакви инциденти могу избегнути доследним применом закона, интерних процедура и континуираном едукацијом свих учесника у процесу.

Нефункционална унутрашња контрола рада са тајним подацима

У складу са Законом о тајности података, сваки орган јавне власти који поступа са тајним подацима мора успоставити два одвојена механизма:

- **Руковалац тајних података** — лице или организациона јединица задужена за примену мера заштите, руковање документацијом, означавање степена тајности, вођење евиденција и техничко поступање са подацима;
- **Унутрашња контрола** — независна функција коју успоставља руководилац органа, задужена за надзор над применом закона, процену ризика, проверу евиденција, откривање неправилности и извештавање о стању система заштите.

У пракси се, међутим, често уочавају озбиљни пропусти у раду ових функција. Дешава се да у неким органима јавне власти руковалац тајних података уопште није именован или је формално постављен али није обучен и не обавља прописане послове. Слично, унутрашња контрола може бити само формална категорија без стварне активности и надзора. Често је проблем и недостатак адекватних обука, као и прецизних процедура за вођење евиденције о раду са тајним подацима и контрола свих евиденције. Без ових елемената, постоји потпуна непрегледност у томе ко, када и како ради са тајним подацима, што отвара простор за злоупотребе и компромитацију безбедности података.

Пример из праксе: У једном органу јавне управе, током ванредне провере надлежних органа, утврђено је да није именовано лице које би имало улогу руковаоца тајних података. Поред тога, унутрашња контрола није ни постојала, а приступ тајним подацима није евидентиран. Запослени нису били упознати са процедурама заштите и нису прошли обуке. Као резултат, тајни подаци су неколико пута били изношени из просторија без икакве контроле, што је представљало озбиљан безбедносни ризик. Овај пропуст је идентификован тек након више месеци, када је један од запослених пријавио сумњиву активност. Након тога уследиле су кадровске и организационе измене, као и обуке запослених и успостављање нових процедура.

Овакви пропусти представљају кршење нормативне обавезе из Закона о тајности података, онемогућавају унутрашњу контролу и откривање злоупотреба, а директно угрожавају националну безбедност.

Оцена: Нефункционална контрола приступа тајним подацима озбиљно угрожава интегритет система заштите поверљивих информација. Јасно је да су механизми руковођења и унутрашње контроле кључни за спречавање злоупотреба и заштиту од неовлашћеног приступа. Практични примери из органа јавне власти указују на потребу за јачим фокусом на успостављање и одржавање ефикасних контролних механизама, укључујући континуиране обуке запослених и редовне унутрашње контроле.

Непрописно означавање степена тајности података

Означавање тајних података мора се вршити искључиво у складу са прописаним критеријумима, процедурама и правним основом, како би се обезбедила адекватна заштита информација од значаја за Републику Србију. Према Закону о тајности података, степен тајности се одређује на основу процене потенцијалне штете која би могла настати у случају неовлашћеног откривања, а овлашћено лице је дужно да примени најнижи степен тајности који спречава штету. У пракси, међутим, јављају се случајеви произвољног означавања — као што је пример где руководилац службе ставља ознаку „Строго поверљиво“ на све

документе, укључујући и интерне записе о организацији ручка у канцеларији, без спроведене процене, без формалне одлуке и без правног основа.

Овакво поступање представља прекршај из члана 99. тачка 3. Закона о тајности података, којим је предвиђена одговорност за неодговарајуће означавање тајних података у документу, што доводи до неоснованог ограничења приступа, правне несигурности и могућег излагања органа јавне власти непотребним ризицима. Поред тога, прекомерно означавање тајности података без стварне потребе:

- нарушава принцип транспарентности у раду органа јавне власти;
- оптерећује систем заштите непотребним процедурама;
- смањује кредибилитет ознака тајности и доводи до њихове девалвације;
- потенцијално прикрива нерелевантне или чак незаконите активности под плаштом тајности.

Такође, према Уредби о начину и поступку означавања тајности података („Службени гласник РС“, бр. 8/2011), означавање мора бити јасно, видљиво, и пропраћено свим неопходним елементима, као што су печат, евиденција, као и пропратни акт. Непоштовање ових процедура додатно отежава контролу и ревизију безбедносних мера.

Пример из праксе: У једном органу јавне власти у Србији, током редовне унутрашње контроле установљено је да је велики број докумената означен степеном „Строго поверљиво“, без икаквог оправдања или формалне одлуке. Међу тим документима били су и акти који се односе на унутрашњу организацију и једноставне административне процесе који нису имали елементе који захтевају тајност. Ова пракса је изазвала проблеме приликом контроле приступа, јер су запослени морали да захтевају безбедносне дозволе за приступ непотребно великом броју докумената, што је створило препреке у свакодневном раду. Након интервенције надлежних служби, унапређен је систем означавања и спроведена обука одговорних лица о правилној примени процедура, што је довело до редукције злоупотреба и повећане ефикасности заштите података.

Оцена: Непрописно означавање степена тајности података је озбиљан безбедносни пропуст који нарушава правну сигурност и функционалност система заштите података у органима јавне власти. Оваква пракса подрива кредибилитет система заштите, отежава контролу приступа и повећава ризик од злоупотреба. За унапређење је неопходно континуирано едуковати одговорна лица, строго пратити примену уредби и закона, као и редовно спроводити интерне контроле како би се осигурала адекватна и пропорционална заштита тајних података.

Неспровођење обука о заштити тајних података

Континуирана едукација запослених који поступају са тајним подацима представља обавезну меру у складу са Законом о тајности података и Планом заштите тајних података. Обука је кључна за изградњу безбедносне културе, разумевање правних обавеза, примену процедура и спречавање пропуста у руковању поверљивим информацијама. Према званичним смерницама, сваки орган јавне власти и организација која поступа са тајним подацима мора да обезбеди редовне теоријске и практичне обуке, као и систем евалуације и сертификације запослених.

У пракси, међутим, јављају се случајеви као што је пример једне државне институције у којој запослени годинама нису прошли обуке о заштити тајних података, иако су редовно поступали са документацијом означеном као „Строго поверљиво“ и „Поверљиво“. Овакво поступање представља кршење обавезе континуиране едукације, доводи до смањене безбедносне свести, повећава ризик од инцидента, и може резултирати компромитовањем поверљивих података, што директно угрожава националну безбедност и економску стабилност.

Пример из праксе: У једној државној институцији која управља поверљивим подацима о стратешким партнерствима, утврђено је да више запослених није прошло обавезне обуке из заштите тајних података у последњих пет година. Као последица недостатка знања и свести, дошло је до пропуста приликом руковања тајним подацима — документ са ознаком „Строго поверљиво“ је био привремено остављен у отвореној канцеларији, што је омогућило приступ неовлашћеним лицима. Након овог инцидента, уведене су обавезне редовне обуке, као и систем праћења присуства и евалуације знања, чиме је значајно побољшана безбедносна култура унутар институције.

Оцена: Неспровођење редовних обука о заштити тајних података представља значајан безбедносни ризик и кршење законских обавеза које може довести до озбиљних последица по поверење и сигурност информација од значаја за Републику Србију. Увођење систематске и континуиране едукације запослених, уз проверу ефективности и примене знања, неопходно је за смањење ризика и јачање свести о важности заштите тајних података у свим органима и организацијама.

Неправилан пренос тајних података

Пренос тајних података мора се вршити искључиво путем безбедносно акредитованих канала комуникације, који обезбеђују криптографску заштиту, контролу приступа, евиденцију преноса и физичку сигурност. Овакав приступ је у складу са мерама из Плана заштите тајних података, као и члановима 35–40

Закона о тајности података, који забрањују коришћење незаштићених средстава комуникације (нпр. Gmail, Yahoo, Viber, WhatsApp) за пренос докумената који садрже поверљиве информације, без обзира на степен тајности. У пракси, међутим, долази до озбиљних пропуста.

Пример из праксе: У једном случају, шеф кабинета у једном министарству проследио је документ са ознаком „Строго поверљиво“ отвореним Gmail налогом, уз додатно обавештење адресату путем апликације Viber. Као разлог навео је „хитност поступања и немогућност да се користи службени канал у том тренутку“. Документ је садржао анализу мера из домена националне безбедности и био намењен ограниченом броју лица са безбедносним сертификатом. Иако до цурења података није дошло, овај инцидент је покренуо унутрашњи надзор.

Последице:

- Повећан ризик од сајбер напада и неовлашћеног прислушкивања;
- Могућност компромитације тајних података и откривања истих;
- Повреда процедура и губитак поверења у институције;
- Потенцијална кривична и дисциплинска одговорност лица које је извршило пренос.

Оцена: Непоштовање правила о безбедном преносу тајних података је једна од најозбиљнијих претњи за систем заштите података. У недостатку јасне техничке инфраструктуре и културе безбедносне одговорности, овакви инциденти не само да доводе у питање легитимитет рада органа, већ могу имати далекосежне последице по националну безбедност. Неопходно је спровести редовну обуку, увести аутоматизоване безбедносне алате и успоставити јасне санкционе механизме за овакве пропусте.

Разговори о тајним подацима у јавности

Поступање са тајним подацима подразумева не само техничке и административне мере заштите, већ и сталну личну одговорност овлашћених лица да поверљиве информације не откривају у окружењима која нису безбедносно контролисана. У складу са члановима 22. и 38. Закона о тајности података, подаци означени степеном тајности морају се обрађивати, чувати и преносити искључиво унутар безбедносно акредитованих простора (тзв. безбедносне зоне), уз примену мера физичке и персоналне безбедности.

Пример из праксе: У једном случају, два запослена из органа јавне власти разговарали су у кафићу у близини своје институције о тајним подацима. Разговор се одвијао без икакве провере окружења, а присутна лица за суседним столовима могла су недвосмислено чути о чему је реч. Један од присутних,

новинар локалног портала, касније је у свом тексту наговестио одређене детаље који су одговарали садржају разговора. Накнадна унутрашња контрола утврдила је да је дошло до повреде правила поступања са тајним подацима.

Оцена: Овакво поступање представља озбиљно кршење принципа заштите тајних података јер:

- неовлашћена лица могу добити приступ тајним подацима;
- не постоји контрола окружења, нити техничка заштита од прислушкивања;
- разговори ван безбедносних зона нису евидентирани ни надгледани;
- постоји ризик од компромитовања оперативних активности и угрожавања безбедности лица, ресурса или државног интереса.

Поред дисциплинске одговорности на основу прописа о раду, овакви пропусти могу довести и до кривичне одговорности, у складу са члановима 98. и 99. Закона о тајности података. Уједно, овакви инциденти урушавају институционално поверење и представљају директну претњу националној безбедности.

Неовлашћени улазак странаца у безбедносне зоне

Безбедносне зоне представљају просторе у којима се обрађују, чувају или преносе тајни подаци, а приступ је дозвољен искључиво лицима која су прошла безбедносну проверу, поседују одговарајући степен овлашћења (дозволу за приступ тајним подацима за странце) и налазе се на Листи лица по принципу „потребно да зна“. Према члану 43. и члану 50. Закона о тајности података, улазак лица која нису прошла одговарајућу процедуру представља озбиљно кршење мера физичке и персоналне безбедности.

Пример из праксе: У једном јавном предузећу из енергетског сектора, страни консултанти који раде у оквиру међународног пројекта били су смештени у просторијама службе за планирање и анализу, где се налази документација и рачунарска опрема са приступом тајним подацима о безбедносно критичним инфраструктурама. Ниједан од тих консултаната није имао безбедносну проверу и дозволу за приступ тајним подацима, није био евидентиран као лице са приступом тајним подацима, нити је постојао надзор њиховог кретања унутар објекта. Чак је један од њих користио несигурну Wi-Fi мрежу за приступ радним документима на лаптопу који није био регистрован у систему техничке заштите.

Последице и оцена: Овакво поступање резултира следећим ризицима и одговорностима:

- **компромитовање тајних података**, укључујући могућност копирања, фотографисања или дигиталног извоза докумената;
- **угрожавање националне безбедности**, посебно ако је реч о информацијама везаним за енергетску стабилност, војну инфраструктуру или критичне системе;
- **ризик од индустријске шпијунаже**, нарочито у контексту конкуренције у области инвестиција;
- **могућност сајбер инцидената**, услед непроверених уређаја и приступа мрежама;
- **правна и дисциплинска одговорност** руководиоца објекта, руковаоца тајних података и надлежног лица за безбедност.

Према члану 98. и 99. Закона, овакви пропусти могу бити основ за покретање прекршајног или кривичног поступка. Орган који контролише простор обавезан је да хитно предузме мере:

- ревизију приступа безбедносној зони,
- процену ризика,
- пријаву инцидента надлежној служби унутрашње контроле,
- и обавештавање Канцеларије Савета за националну безбедности и за заштиту тајних података.

Напомена: Овај пример указује на потребу за бољом сарадњом између носилаца међународних пројеката и националних служби безбедности, као и на неопходност да инострани партнери буду упознати са домаћим прописима пре него што им се омогући физички или дигитални приступ тајним подацима Републике Србије.

Уступање тајних података непозваним лицима

Тајни подаци се могу уступити искључиво лицима која су овлашћена у складу са *принципом „потребно да зна“*, која поседују важећи **безбедносни сертификат**, и која су наведена у *Листи овлашћених лица* од стране надлежног органа. Уступање поверљивих информација лицима која нису део институционалног оквира, без одобрења, без евиденције и ван прописане процедуре, представља **кривично дело** у складу са чланом 98. Закона о тајности података. У пракси, пример службеника који прослеђује тајне документе о националној одбрани пријатељу у приватној фирми, без икаквог овлашћења, представља:

- **неовлашћено откривање тајних података**;
- **угрожавање националне безбедности и одбрамбених капацитета државе**;

- **повреду службене дужности и злоупотребу положаја**;
- основу за покретање **кривичног поступка**, као и дисциплинске и прекршајне мере.

Овакво поступање може довести до:

- компромитовања оперативних планова и стратегија;
- угрожавања живота и безбедности лица наведених у документима;
- нарушавања међународне сарадње и поверења;
- правне одговорности службеника и институције.

У конкретном случају, након спроведене унутрашње контроле и обавештавања Канцеларије Савета за националну безбедност и заштиту тајних података, надлежни орган је покренуо поступак преиспитивања безбедносног сертификата службенику и забранио му приступ тајним подацима док траје кривични поступак, док је надлежно тужилаштво покренуло поступак због неовлашћеног одавања тајних података. Институција је, као последицу, морала да спроведе хитну ревизију свих комуникационих и безбедносних процедура, што је изазвало значајне трошкове, унутрашње реструктурирање и нарушавање јавне и међународне репутације органа.

Поука: Уступање тајних података, чак и ако је вођено добром намером, али изван прописаног оквира, може имати озбиљне безбедносне, правне и политичке последице. Информација која носи степен тајности мора бити заштићена не само техничким средствима, већ и кроз развијену и доследну културу безбедности код свих запослених.

Неовлашћено уношење електронских уређаја у безбедносне зоне

Безбедносне зоне су просторије у којима се чувају, обрађују или уништавају тајни подаци, и у које је дозвољен улазак искључиво овлашћеним лицима, уз претходну безбедносну проверу и у складу са прописаним процедурама. Према *Уредби о посебним мерама физичко-техничке заштите*, уношење **електронских уређаја** — као што су мобилни телефони, лаптопи, паметни сатови, USB меморије и друга опрема са могућношћу снимања, преноса или складиштења података — у безбедносне зоне је **строго забрањено**, осим ако је уређај акредитован и одобрен за рад са тајним подацима.

У пракси, међутим, јављају се случајеви као што је пример запосленог у министарству који носи мобилни телефон са камером у просторије где се чувају документи са ознаком „Државна тајна“. Овакво поступање представља:

- **кршење мера физичке и техничке безбедности**;
- **ризик од шпијунаже, компромитовања или неовлашћеног снимања тајних података**;
- основу за покретање **дисциплинског, прекршајног или кривичног поступка**, у складу са прописима о раду, односно чланом 98. и 99. Закона о тајности података;
- директно **угрожавање националне безбедности** и оперативне способности институције.

Орган је дужан да:

- спроведе противприслушни преглед просторија;
- обезбеди контролу уласка и изласка лица и опреме;
- води евиденцију о уређајима који се уносе у зону;
- обучи запослене о забранама и ризицима.

Сваки вид непоштовања безбедносних процедура унутар заштићених зона, па и уношење недозвољених електронских уређаја, мора се третирати као потенцијална безбедносна претња са озбиљним последицама — како по појединца, тако и по институцију у целини.

На крају уместо закључка

Примери наведени у овој анализи недвосмислено указују на то да непоштовање прописа у вези са поступањем са тајним подацима представља озбиљан и вишеслојан безбедносни ризик. Пропусти као што су неовлашћен приступ, игнорисање прописаних процедура, недовољна обученост кадрова, непостојање јасне систематизације радних места, као и занемаривање контролних и надзорних механизама, могу довести до:

• злоупотребе тајних података, докумената и информација;
• неовлашћеног откривања, губитка или компромитовања тајних података;
• угрожавања оперативних, институционалних и државних интереса;
• директног нарушавања интегритета и стабилности националне безбедности.

У циљу спречавања оваквих ризика и унапређења безбедносне културе у институцијама које поступају са тајним подацима, неопходно је:

• успоставити јасне, стандардизоване и доследно применљиве процедуре заштите тајних података, како за потребе поверљивих

набавки, тако и за потребе плана одбране али и дугих послова у којима се ради са тајним подацима у органу јавне власти;
• обезбедити редовне и обавезујуће обуке, едукације и тестирање запослених који раде са тајним подацима;
• развити и примењивати ефикасне контролне механизме — како интерне (унутрашња контрола и самопроцена – процена безбедности тајних података), тако и спољне (стручни надзор, инспекцијски надзор, безбедносне провере физичких и правних лица);
• систематски јачати и неговати културу безбедности, односно свест о важности заштите тајних података на свим нивоима институционалне хијерархије.

Само свеобухватним, одговорним и континуираним приступом може се обезбедити висок ниво поузданости у руковању тајним подацима и тиме допринети очувању безбедносног, институционалног и државног интереса Републике Србије.

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.