

Тестови за рад са тајним подацима у Републици Србији за органе јавне власти

Канцеларија Савета за националну безбедност и заштиту тајних података развила је сет тестова осмишљених за подизање нивоа безбедносне свести и културе у органима јавне власти у области рада са тајним подацима.

Ови тестови служе двострукој сврси: с једне стране, они доприносе јачању капацитета запослених у органима јавне власти у заштити тајних података, а с друге стране, пружају подршку старешинама органа јавне власти и руковооцима тајним подацима у ефективном управљању персоналом безбедношћу. Такође, омогућавају самосталну едукацију запослених, чиме подстичу континуирано унапређење стручности из ове области. Редовним тестирањем и едукацијом, запослени добијају практичну примену теоријских знања, што доводи до већег нивоа одговорности и свести о безбедности. Кроз овакве иницијативе, институције постају отпорније на претње и адекватно реагују на све безбедносне изазове.

Овај сегмент програма едукација представља не само алат за изградњу безбедносне свести и културе, већ и важан корак у имплементацији јавних политика у делу који се односи на заштиту тајних података. Редовна обука и самостална примена ових тестова унутар органа јавне власти доприносе унапређењу свеукупних безбедносних пракси, јачању система националне безбедности и обезбеђењу доследности у примени стандарда у овој области.

Практични аспекти спровођења обука и едукација кроз тестирање запослених у органима јавне власти укључују следеће активности:

1. **Идентификација потенцијалних претњи:** Тестови омогућавају запосленима да кроз симулиране ситуације увежбавају препознавање необичних захтева за приступ поверљивим документима. Такве вежбе подучавају запослене како да идентификују потенцијалне претње и правилно реагују, алармирајући надлежне особе.
2. **Безбедно управљање тајним подацима:** У оквиру обука, запослени, старешине и руковооци тајним подацима у органима јавне власти пролазе кроз сценарије који укључују процену ризика приликом обраде и заштите тајних података. Ове активности имају за циљ јачање способности за доношење одлука које унапређују организациону безбедност и заштиту тајних података.

Кроз практичне и интерактивне приступе, ове активности не само да осигуравају примену теоријских знања у реалним ситуацијама, већ и граде културу безбедности унутар органа јавне власти. Редовна примена оваквих програма значајно доприноси отпорности институција и њиховој способности да се адекватно суоче са савременим безбедносним изазовима.

Крајњи циљ ових тестова јесте побољшање безбедносних пракси у раду са тајним подацима у органима јавне власти, као и у другим институцијама, доприносећи јачању свеукупног система националне безбедности.

Напомена: Тестови садрже и решења и намењени су искључиво за унутрашњу употребу унутар органа јавне власти.

КОМБИНАЦИЈА 1.

1. Организациона култура и свест је:

- А) Скуп правила и прописа о раду у државним органима.
- Б) Ниво безбедносне културе запослених у систему заштите података.
- В) Начин на који организација управља информацијама и подацима.
- Г) Модел основних претпоставки, вредности и норми, које је дата група развила или открила учећи како да решава проблеме екстерне адаптације и интерне интеграције и који функционишу довољно добро да би били пренети новим члановима.

(тачан одговор: Г)

2. Приватне тајне су:

- А) Подаци којима је законом одређен степен тајности.
- Б) Сазнање о одређеним интимним и приватним подацима која се сазнају од других лица на основу родбинског, пријатељског или емотивног односа, као и међусобног поверења.
- В) Пословне информације предузећа које нису доступне јавности.
- Г) Поверљиви подаци које институције размењују у оквиру међународне сарадње.

(тачан одговор: Б)

3. Шта чини информациону сигурност (заокружи одговор који ту не припада)?

- А) Поверљивост, интегритет и доступност података.
- Б) Заштита од неовлашћеног приступа и злоупотребе информација.
- В) Мере заштите од сајбер напада и угрожавања података.
- Г) Заштита достојанства и интегритета сваког појединца.

(тачан одговор: Г)

4. Информатичка приватност обухвата:

- А) Скуп података (информација) о личности, насталих употребом дигиталне технологије.
- Б) Личне податке садржане само у папирним документима.
- В) Приватност података у пословном окружењу.
- Г) Право државних органа да надгледају интернет комуникацију.

(тачан одговор: А)

5. Пословна тајна је:

- А) Документ са означеним степеном тајности у државним институцијама.
- Б) Категорија интелектуалне својине.
- В) Податак о пословању доступан само јавним органима.
- Г) Финансијски извештај компаније доступан јавности.

(тачан одговор: Б)

6. Шта представља појам класификација података?

- А) Обележавање података као тајних или јавних.
- Б) Заштиту докумената од неовлашћеног приступа.
- В) Одвајање података у различите категорије података.
- Г) Начин складиштења података у архивама.

(тачан одговор: В)

7. Тајни податак је:

- А) Подаци од интереса за Републику Србију који су законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређени и означени одређеним степеном тајности.
- Б) Било који податак који није доступан јавности.
- В) Лични подаци грађана који се чувају у регистрима.
- Г) Документ којем се приступ може ограничити унутар једне организације.

(тачан одговор: А)

8. Којем појму није овде место када је у питању приватни живот?

- А) Поверљивост личних података.
- Б) Право на заштиту комуникација.
- В) Контрола над личним информацијама.
- Г) Јавна политика.

(тачан одговор: Г)

9. Право на проток личних података је:

- А) Право на неограничено дељење информација.
- Б) Ограничено право на размену података у оквиру правних прописа.
- В) Право на проток.
- Г) Немогућност размене личних података без дозволе државе.

(тачан одговор: В)

10. Рад са професионалном тајном уређен је:

- А) Законом о заштити података о личности.
- Б) Интерним процедурама компаније.
- В) Правилима безбедносне културе.
- Г) Кодексом етике.

(тачан одговор: Г)

11. Заштићени податак је општи термин за:

- А) Само податке означене као тајне.
- Б) Личне податке грађана.
- В) Само пословне тајне.
- Г) Податке који су заштићени на основу закона или уговора.

(тачан одговор: Г)

12. Подаци о личности су:

- А) Само име и презиме особе.
- Б) Податак који се односи на било које правно лице.
- В) Финансијски подаци предузећа.
- Г) Подаци који се односе на физичко лице.

(тачан одговор: Г)

13. Повреда података је:

- А) Коришћење података без дозволе власника.
- Б) Оштећење базе података услед кvara.
- В) Промене података без званичног одобрења.
- Г) Неовлашћено откривање штићених података.

(тачан одговор: Г)

14. Човек је увек:

- А) Потпуно поуздан у безбедносном систему.
- Б) Најјача карика у сваком систему.
- В) Најслабија карика сваког система.
- Г) Незамењив у безбедносним процесима.

(тачан одговор: В)

15. Како је уређена приватност у Републици Србији?

- А) Искључиво законом о заштити података о личности.
- Б) Потпуно неуређена.
- В) Делимично уређена Уставом и другим прописима.
- Г) Само кроз судску праксу.

(тачан одговор: В)

КОМБИНАЦИЈА 2.

1. **Који је основни циљ система заштите тајних података?**
 - А) Омогућавање слободног приступа информацијама
 - Б) Обезбеђивање усаглашености са законским и институционалним захтевима
 - В) Смањење броја запослених у организацији
 - Г) Повећање профита компаније

(тачан одговор: Б)
2. **Шта обухвата персонална безбедност у контексту заштите тајних података?**
 - А) Проверу физичке спремности запослених
 - Б) Процедуре за утврђивање подобности лица за приступ тајним подацима
 - В) Инсталацију сигурносних камера
 - Г) Обезбеђивање финансијске стабилности организације

(тачан одговор : Б)
3. **Који је основни документ који дефинише мере заштите тајних података у организацији?**
 - А) Пословник о раду
 - Б) Упутство о мерама заштите тајних података
 - В) Финансијски извештај
 - Г) Годишњи план рада

(тачан одговор: Б)
4. **Шта подразумева индустријска безбедност у контексту заштите тајних података?**
 - А) Заштиту индустријских машина од оштећења
 - Б) Обезбеђивање да правна лица испуњавају услове за рад са тајним подацима
 - В) Повећање производње у фабрикама
 - Г) Смањење трошкова производње

(тачан одговор : Б)
5. **Који орган је надлежан за спровођење унутрашње контроле над радом са тајним подацима?**
 - А) Министарство финансија
 - Б) Канцеларија Савета за националну безбедност и заштиту тајних података
 - В) Министарство културе
 - Г) Агенција за привредне регистре

(тачан одговор : Б)
6. **Који је основни циљ унутрашње контроле у систему заштите тајних података?**
 - А) Повећање профита организације
 - Б) Обезбеђивање усаглашености са законским и институционалним захтевима
 - В) Смањење броја запослених
 - Г) Промоција компаније у медијима

(тачан одговор : Б)
7. **Шта представља регистарски систем у контексту заштите тајних података?**
 - А) Систем за евиденцију запослених
 - Б) Систем за руковање тајним подацима у складу са прописима
 - В) Систем за управљање финансијама
 - Г) Систем за управљање пројектима

(тачан одговор : Б)
8. **Који је основни циљ физичке безбедности у систему заштите тајних података?**
 - А) Заштита физичког здравља запослених
 - Б) Заштита објеката и опреме у којима се чувају тајни подаци
 - В) Повећање продуктивности
 - Г) Смањење трошкова одржавања

(тачан одговор : Б)

- 9. Шта подразумева информациона безбедност у контексту заштите тајних података?**
А) Заштиту информационих система од неовлашћеног приступа
Б) Повећање брзине интернета
В) Инсталацију нових софтвера
Г) Обучавање запослених за коришћење рачунара
(тачан одговор : А)
- 10. Који је основни циљ административне безбедности у систему заштите тајних података?**
А) Обезбеђивање правилног управљања документацијом и приступом тајним подацима
Б) Повећање броја административних радника у институцији
В) Смањење количине папирне документације
Г) Увођење нових процедура за рад са подацима без обзира на безбедносне стандарде
(тачан одговор : А)
- 11. Која мера се примењује за заштиту тајних података у електронском облику?**
А) Складиштење података на јавно доступним серверима
Б) Користи се криптографска заштита и контролисан приступ
В) Пренос тајних података путем личних имејл адреса
Г) Забрана било какве електронске обраде података
(тачан одговор : Б)
- 12. Ко је одговоран за утврђивање нивоа тајности података?**
А) Свако лице које има приступ тајним подацима
Б) Лице овлашћено за одређивање нивоа тајности података
В) Радна група за правне послове
Г) Особа која физички рукује документима
(тачан одговор : Б)
- 13. Шта је примарни разлог за евидентирање приступа тајним подацима?**
А) Ради контроле и спречавања неовлашћеног приступа
Б) Да би се направила статистика коришћења докумената
В) Да би се смањио број запослених са приступом тајним подацима
Г) Да би се олакшао административни процес архивирања
(тачан одговор : А)
- 14. Која од наведених радњи представља кршење мера заштите тајних података?**
А) Чување тајних докумената у неовлашћеним просторијама
Б) Коришћење прописане процедуре за руковање тајним документима
В) Приступ тајним подацима искључиво у оквиру овлашћења
Г) Редовна обука запослених о мерама безбедности
(тачан одговор : А)
- 15. Како се поступа са тајним подацима након истека рока тајности?**
А) Они се уништавају у складу са прописаним процедурама
Б) Аутоматски постају доступни јавности
В) Чувају се у архиви без икаквог додатног поступка
Г) Преносе се у надлежност Министарства културе
(тачан одговор : В)

КОМБИНАЦИЈА 3.

1. **Који је примарни циљ система заштите тајних података?**
 - А) Ограничити приступ информацијама без обзира на потребе државних органа
 - Б) Осигурати да тајни подаци буду доступни само овлашћеним лицима
 - В) Повећати број особа које имају увид у поверљиве податке
 - Г) Омогућити слободан проток информација ради транспарентности

(тачан одговор : Б)
2. **Које од следећих информација НЕ спадају у категорију тајних података?**
 - А) Стратешки документи у области одбране
 - Б) Планови за евакуацију у случају ванредних ситуација
 - В) Лични подаци грађана садржани у здравственим картонима
 - Г) Оперативни подаци безбедносних служби

(тачан одговор : В)
3. **Који закон у Србији регулише заштиту података о личности?**
 - А) Закон о тајним подацима
 - Б) Закон о заштити података о личности
 - В) Закон о јавном информисању и медијима
 - Г) Закон о одбрани

(тачан одговор : Б)
4. **Ко има право приступа поверљивим подацима у здравственим установама?**
 - А) Само пацијент на кога се подаци односе
 - Б) Овлашћена лица у оквиру здравствене институције и други субјекти у складу са законом
 - В) Свако лице које ради у здравственој установи
 - Г) Сви запослени у државним органима

(тачан одговор : Б)
5. **Како се у Србији означавају нивои тајности података?**
 - А) 'Службена тајна', 'Вољна тајна', 'Ограничено', 'Јавно'
 - Б) 'Поверљиво', 'Строго поверљиво', 'Државна тајна', 'Интерно'
 - В) 'Високо поверљиво', 'Ограничено', 'Јавно', 'Тајна документа'
 - Г) 'Доступно јавности', 'Неовлашћено', 'Ограничена тајност', 'Највиша тајност'

(тачан одговор: Б)
6. **Који је исправан начин преноса докумената који садрже поверљиве податке?**
 - А) Путем личне е-поште ако је порука заштићена лозинком
 - Б) Физички транспорт у запечаћеном омоту уз службену потврду
 - В) Путем било ког доступног комуникационог канала
 - Г) Објављивањем у интерном билтену организације

(тачан одговор : Б)
7. **Шта представља безбедносна провера лица?**
 - А) Процедуру којом се проверава безбедносна култура лица
 - Б) Процес утврђивања да ли особа испуњава услове за приступ тајним подацима
 - В) Контролу радног учинка у институцијама
 - Г) Проверу радне етике код запослених

(тачан одговор : Б)
8. **Који од ових података НЕ спада у категорију службене тајне?**
 - А) Интерни извештаји о раду државних институција
 - Б) Планови заштите критичне инфраструктуре
 - В) Јавно доступни подаци о буџету државе
 - Г) Детаљи о оперативним мерама безбедносних служби

(тачан одговор : В)

- 9. Које мере се предузимају ради физичке заштите тајних података?**
А) Употреба криптографских алгоритама
Б) Контролисан приступ објектима и употреба сигурносних ормара
В) Оглашавање процедуре за заштиту података у медијима
Г) Слободан приступ службеним просторијама без ограничења
(тачан одговор : Б)
- 10. Које институције су у Србији надлежне за спровођење мера заштите тајних података?**
А) Министарство правде и Повереник за заштиту равноправности
Б) Канцеларија Савета за националну безбедност и надлежни државни органи
В) Народна скупштина и невладине организације
Г) Локалне самоуправе и приватне компаније
(тачан одговор : Б)
- 11. Који је исправан начин уништавања тајних докумената након истека рока тајности?**
А) Спаљивање, дробљење или употреба специјализованих машина за уништавање
Б) Одлагање у контејнер за рециклажу
В) Предаја медијима ради информисања јавности
Г) Архивирање без додатне обраде
(тачан одговор : А)
- 12. Шта је 'Need-to-Know' принцип у безбедности података?**
А) Право свих запослених да знају све информације у оквиру организације
Б) Ограничење приступа тајним подацима само на оне који имају стварну потребу за тим подацима
В) Обавеза дељења свих информација међу колегама ради боље сарадње
Г) Аутоматско приступање тајним подацима свим руководиоцима
(тачан одговор : Б)
- 13. Која од наведених радњи представља кршење мера заштите података о личности?**
А) Достављање личних података грађана трећим лицима без правног основа
Б) Чување личних података у складу са законом
В) Коришћење података о запосленима у статистичке сврхе унутар компаније
Г) Приступ личним подацима само овлашћених лица
(тачан одговор : А)
- 14. Која врста података спада у категорију 'пословна тајна'?**
А) Информације о приватним животима запослених
Б) Стратешки планови компаније и финансијски подаци који нису доступни јавности
В) Лични документи запослених који су доступни у базама података
Г) Сви подаци о фирми без изузетка
(тачан одговор : Б)
- 15. Како се правилно врши обука запослених за заштиту података?**
А) Повремени тестови и едукације у складу са безбедносним стандардима
Б) Самостално читање прописа без контроле знања
В) Потпуна слобода у руковању подацима без формалне обуке
Г) Једнократна инструкција на почетку запослења
(тачан одговор : А)

КОМБИНАЦИЈА 4.

1. **Који је основни принцип заштите тајних података?**
 - А) Омогућавање слободног приступа свим запосленима
 - Б) Дефинисање овлашћења и контролисан приступ подацима
 - В) Аутоматско архивирање без контроле приступа
 - Г) Складиштење података без икаквих мера заштите

(тачан одговор : Б)
2. **Шта представља појам 'заштита пословне тајне'?**
 - А) Ограничење приступа подацима који су од кључног значаја за компанију
 - Б) Слободно дељење свих података међу запосленима
 - В) Обавеза архивирања свих докумената без додатних мера
 - Г) Јавно објављивање финансијских података предузећа

(тачан одговор : А)
3. **Који закон у Србији регулише заштиту података о личности?**
 - А) Закон о заштити података о личности
 - Б) Закон о слободном приступу информацијама од јавног значаја
 - В) Закон о тајним подацима
 - Г) Закон о раду

(тачан одговор : А)
4. **Који је исправан начин обраде података о личности у складу са законом?**
 - А) Обрада искључиво на основу правног основа и уз поштовање принципа заштите
 - Б) Обрада без ограничења ако је у интересу организације
 - В) Објављивање личних података ради транспарентности
 - Г) Чување личних података без икаквих мера заштите

(тачан одговор : А)
5. **Које информације спадају у категорију података који се штите у здравственим установама?**
 - А) Само дијагноза пацијента
 - Б) Лични, медицински и генетски подаци пацијента
 - В) Само финансијски извештаји о лечењу
 - Г) Сви подаци који нису повезани са здравственим стањем

(тачан одговор : Б)
6. **Како се класификују тајни подаци у Србији?**
 - А) 'Интерно', 'Поверљиво', 'Строго поверљиво', 'Државна тајна'
 - Б) 'Јавно', 'Тајно', 'Највиша тајност'
 - В) 'Пословна тајна', 'Информациона тајна', 'Службена тајна'
 - Г) 'Ограничено', 'Поверљиво', 'Висока тајност'

(тачан одговор : А)
7. **Шта је 'Need-to-Know' принцип у систему заштите података?**
 - А) Свако има право да зна све информације у оквиру организације
 - Б) Ограничење приступа тајним подацима само на оне који имају стварну потребу за тим подацима
 - В) Обавеза размене свих информација унутар државних институција
 - Г) Аутоматски приступ свим тајним подацима за руководиоце

(тачан одговор : Б)
8. **Који документи спадају у категорију критичне инфраструктуре?**
 - А) Планови заштите електроенергетског система
 - Б) Туристички водичи за градове
 - В) Листе јавних манифестација
 - Г) Комерцијални каталози предузећа

(тачан одговор : А)

- 9. Како се исправно преносе тајни подаци између институција?**
А) У запечаћеним омотима, уз службену потврду о пријему
Б) Путем обичних електронских порука
В) Објављивањем на интерној мрежи без шифровања
Г) Усмено, без пратеће документације
(тачан одговор : А)
- 10. Које су последице непоштовања мера заштите тајних података?**
А) Кршење закона и могућност покретања кривичног поступка
Б) Само интерна дисциплинска мера
В) Нема последица ако подаци нису злоупотребљени
Г) Само усмено упозорење без даљих мера
(тачан одговор : А)
- 11. Како се правилно уништавају тајни документи?**
А) Коришћењем машина за уништавање или спаљивањем
Б) Одлагањем у обичне канте за отпад
В) Архивирањем без додатних мера заштите
Г) Објављивањем на интернету након истека рока тајности
(тачан одговор : А)
- 12. Који подаци се штите у контексту финансијске безбедности?**
А) Подаци о банковним трансакцијама и платним картицама
Б) Само информације о каматним стопама
В) Само извештаји о јавним приходима
Г) Листе купаца у супермаркетима
(тачан одговор : А)
- 13. Шта представља поверљивост података у дигиталном окружењу?**
А) Обавеза да подаци буду доступни само овлашћеним лицима
Б) Слободан приступ свим дигиталним фајловима
В) Архивирање података без шифровања
Г) Делење поверљивих докумената путем друштвених мрежа
(тачан одговор : А)
- 14. Које мере се примењују за заштиту података у информационим системима?**
А) Енкрипција, двофакторска аутентификација и ограничен приступ
Б) Остављање свих фајлова без лозинке
В) Коришћење једне лозинке за све системе
Г) Ослонац искључиво на антивирус програме
(тачан одговор : А)
- 15. Како се правилно врши обука запослених за заштиту података?**
А) Редовне едукације и тестирања знања
Б) Једнократни курс приликом запошљавања
В) Ослонац на самостално информисање без провере знања
Г) Нема потребе за обуком ако су запослени потписали поверљивост
(тачан одговор : А)

КОМБИНАЦИЈА 5.

1. **Који закон у Републици Србији регулише заштиту тајних података?**
 - А) Закон о заштити података о личности
 - Б) Закон о слободном приступу информацијама од јавног значаја
 - В) Закон о тајности података
 - Г) Закон о информационој безбедности

(тачан одговор : В)
2. **Који је највиши степен тајности података у Републици Србији?**
 - А) Поверљиво
 - Б) Строго поверљиво
 - В) Државна тајна
 - Г) Интерно

(тачан одговор : В)
3. **Ко је одговоран за одређивање степена тајности података у органима јавне власти?**
 - А) Сваки запослени
 - Б) Руководилац органа јавне власти или овлашћено лице
 - В) Министарство унутрашњих послова
 - Г) Канцеларија Савета за националну безбедност

(тачан одговор : Б)
4. **Шта представља појам "тајни податак"?**
 - А) Подаци доступни јавности
 - Б) Подаци који су означени одређеним степеном тајности
 - В) Подаци без икаквог степена заштите
 - Г) Подаци који су изгубљени

(тачан одговор : Б)
5. **Која је сврха примене посебних мера заштите тајних података?**
 - А) Омогућавање слободног приступа информацијама
 - Б) Спречавање неовлашћеног приступа и откривања тајних података
 - В) Смањење броја запослених у органима јавне власти
 - Г) Повећање транспарентности рада органа

(тачан одговор : Б)
6. **Који орган је надлежан за надзор над применом мера заштите тајних података у Републици Србији?**
 - А) Министарство правде
 - Б) Канцеларија Савета за националну безбедност и заштиту тајних података
 - В) Народна скупштина
 - Г) Агенција за борбу против корупције

(тачан одговор : Б)
7. **Шта подразумева термин "информационо-телекомуникациона безбедност" у контексту заштите тајних података?**
 - А) Заштиту физичких просторија
 - Б) Заштиту информација у електронским системима
 - В) Обезбеђивање превоза тајних докумената
 - Г) Контролу приступа зградама

(тачан одговор : Б)

8. Која је улога безбедносне провере у систему заштите тајних података?
- А) Провера техничке исправности опреме
 - Б) Провера подобности лица за приступ тајним подацима
 - В) Провера квалитета тајних података
 - Г) Провера финансијског стања запослених
- (тачан одговор : Б)
9. Шта је "безбедносна зона" у контексту физичке заштите тајних података?
- А) Јавно доступна област
 - Б) Подручје са ограниченим приступом ради заштите тајних података
 - В) Област за складиштење јавних докумената
 - Г) Простор за обуку запослених
- (тачан одговор : Б)
10. Која мера се примењује за заштиту тајних података у електронској комуникацији?
- А) Коришћење јавних електронских поштанских услуга
 - Б) Енкрипција података
 - В) Слање података без икакве заштите
 - Г) Објављивање података на интернету
- (тачан одговор : Б)
11. Која је сврха категоризације тајних података?
- А) Омогућавање слободног приступа свим подацима
 - Б) Означавање степена тајности у складу са законом
 - В) Повећање броја докумената у архиви
 - Г) Смањење броја особа које могу руковати документима
- (тачан одговор : Б)
12. Шта представља термин „неовлашћено откривање тајних података“?
- А) Давање података овлашћеном лицу
 - Б) Губитак или доступност тајних података неовлашћеним лицима
 - В) Унутрашња контрола података
 - Г) Размена података између државних органа
- (тачан одговор : Б)
13. Како се поступа са документима који више нису тајни?
- А) Они остају под истим степеном тајности заувек
 - Б) Враћају се у архиву без промена
 - В) Применом процедура декласификације или уништења у складу са законом
 - Г) Пребацују се у јавно доступне базе података
- (тачан одговор : В)
14. Ко може приступити тајним подацима?
- А) Свако ко ради у државној управи
 - Б) Лица која су добила безбедносни сертификат и имају потребу за приступом
 - В) Свако ко има приступ интернету
 - Г) Само руководицац установе
- (тачан одговор : Б)
15. Шта је „принцип нужности знања“ у систему заштите тајних података?
- А) Лице сме да приступа само оним тајним подацима који су му неопходни за обављање посла
 - Б) Лице може приступити свим тајним подацима у институцији
 - В) Тајни подаци су доступни само министарствима
 - Г) Свако ко ради у безбедносном сектору може да их прегледа
- (тачан одговор : А)

КОМБИНАЦИЈА 6.

1. **Које лице може поднети захтев за издавање безбедносног сертификата?**
 - А) Свако пунолетно лице
 - Б) Само запослени у државним органима
 - В) Лице које има потребу за приступом тајним подацима и испуњава законом прописане услове
 - Г) Само руководиоци безбедносних служби

(тачан одговор : В)
2. **Које тело врши безбедносну проверу кандидата за издавање безбедносног сертификата?**
 - А) Повереник за информације од јавног значаја
 - Б) Канцеларија Савета за националну безбедност и заштиту тајних података
 - В) Народна скупштина
 - Г) Надлежни орган безбедносне службе

(тачан одговор : Г)
3. **Који степен тајности захтева највиши ниво безбедносне провере?**
 - А) Интерно
 - Б) Поверљиво
 - В) Строго поверљиво
 - Г) Државна тајна

(тачан одговор : Г)
4. **Колики је рок важења безбедносног сертификата?**
 - А) Једна година
 - Б) Три године
 - В) Пет година
 - Г) Неограничено

(тачан одговор : В)
5. **Шта се дешава у случају промене околности које утичу на безбедносни сертификат?**
 - А) Сертификат се аутоматски продужава
 - Б) Сертификат остаје важећи без обзира на промене
 - В) Потребно је извршити нову безбедносну проверу
 - Г) Сертификат се поништава без провере

(тачан одговор : В)
6. **Ко може отказати или суспендовати безбедносни сертификат?**
 - А) Лице коме је издат сертификат
 - Б) Надлежни безбедносни орган
 - В) Свако ко има увид у сертификат
 - Г) Канцеларија Повереника за информације

(тачан одговор : Б)
7. **Који подаци се проверавају приликом безбедносне провере кандидата?**
 - А) Само финансијско стање лица
 - Б) Само радни однос и стручна спрема
 - В) Лични, професионални и безбедносни аспекти кандидата
 - Г) Само подаци о здравственом стању

(тачан одговор : В)
8. **Шта значи принцип „непристрасне процене“ у безбедносној провери?**
 - А) Да безбедносни органи не могу доносити одлуке
 - Б) Да се сваки кандидат проверава према истим критеријумима
 - В) Да се одлука доноси искључиво на основу личних утисака
 - Г) Да се провера врши само формално, без детаљне анализе

(тачан одговор : Б)

- 9. Шта је основни услов за одузимање безбедносног сертификата?**
А) Када лице више нема потребу за приступом тајним подацима
Б) Када лице поднесе оставку на послу
В) Када лице промени адресу становања
Г) Када лице промени личне податке у документима
(тачан одговор : А)
- 10. Шта се дешава ако лице не прође безбедносну проверу?**
А) Сертификат му се издаје са ограничењем
Б) Лице добија условну дозволу за приступ тајним подацима
В) Захтев за издавање сертификата се одбија
Г) Лице може наставити да ради са тајним подацима
(тачан одговор : В)
- 11. Који од наведених разлога може бити основ за одбијање издавања безбедносног сертификата?**
А) Присуство дугова и финансијских проблема
Б) Чланство у спортским клубовима
В) Поседовање личне библиотеке са стручном литературом
Г) Учешће у хуманитарним организацијама
(тачан одговор : А)
- 12. Која институција чува евиденцију издатих безбедносних сертификата?**
А) Народна банка Србије
Б) Канцеларија Савета за националну безбедност и заштиту тајних података
В) Пореска управа
Г) Министарство културе
(тачан одговор : Б)
- 13. Шта лице коме је одбијен захтев за издавање безбедносног сертификата може учинити?**
А) Може уложити жалбу надлежном органу
Б) Мора чекати 10 година да поново поднесе захтев
В) Аутоматски добија сертификат нижег степена
Г) Може наставити да ради са тајним подацима без сертификата
(тачан одговор : А)
- 14. Колико времена је потребно за издавање безбедносног сертификата након завршене провере?**
А) До 30 дана
Б) До 60 дана
В) До 90 дана
Г) Нема дефинисаног рока
(тачан одговор : В)
- 15. Које лице може захтевати ревизију безбедносног сертификата?**
А) Лице коме је сертификат издат
Б) Орган који је издао сертификат
В) Само председник владе
Г) Само министар унутрашњих послова
(тачан одговор : Б)

КОМБИНАЦИЈА 7.

1. Који је документ обавезан за спровођење Закона о тајности података?
А) План заштите података
Б) Закон о заштити личних података
В) Водич за имплементацију ЗТП 2025
Г) Статут о јавним набавкама
(тачан одговор : В)
2. Који је највиши степен тајности података?
А) Строго поверљиво
Б) Тајно
В) Поверљиво
Г) Интерно
(тачан одговор : А)
3. Који документ не мора бити припремљен за имплементацију Закона о тајности података у органу јавне власти?
А) Одлука о одређивању степена тајности
Б) Листа „Потребно да зна“
В) Споразум о међународној сарадњи
Г) План заштите података за ванредне случајеве
(тачан одговор : В)
4. Која институција је одговорна за издавање сертификата за органе јавне власти?
А) Министарство правде
Б) Канцеларија Савета за националну безбедност
В) Министарство одбране
Г) Министарство за спољну трговину
(тачан одговор : Б)
5. Шта је основни циљ издавања сертификата за правна лица?
А) Да добију дозволу за рад са тајним подацима
Б) Да пријаве свој рад на безбедности
В) Да учествују у јавним набавкама
Г) Да добију статус повлашћених предузећа
(тачан одговор : А)
6. Која је разлика између „тајног“ и „строго поверљивог“ податка?
А) Строго поверљиви подаци захтевају посебан надзор
Б) Тајни подаци су увек доступни јавности
В) Поверљиви подаци захтевају највећу заштиту
Г) Строго поверљиви подаци се користе само за војне сврхе
(тачан одговор : А)
7. Која одлука није потребна за унутрашњу контролу у органу јавне власти?
А) Одлука о одређивању руководаца тајним подацима
Б) Одлука о одређивању степена тајности
В) Одлука о издавању сертификата
Г) Одлука о унутрашњој контроли
(тачан одговор : В)

8. Које документације су потребне за издавање сертификата за органе јавне власти?
- А) Споразум о међународној сарадњи
 - Б) Захтев за издавање сертификата
 - В) Листа „Потребно поделити са“
 - Г) Извештај о безбедности
- (тачан одговор : Б)
9. Шта подразумева појам "интерна контрола"?
- А) Контрола која се врши само од стране надлежних органа
 - Б) Контрола коју проводи стручни тим за тајне податке
 - В) Контрола која укључује стално праћење безбедности података
 - Г) Контрола која се односи само на финансијске трансакције
- (тачан одговор : В)
10. Која од ових институција није задужена за контролу тајних података?
- А) Канцеларија Савета за националну безбедност
 - Б) Министарство правде
 - В) Министарство заштите животне средине
 - Г) Влада Републике Србије
- (тачан одговор : В)
11. Који је основни циљ модела акта о информационој безбедности?
- А) Да се усмеравају напори ка заштити личних података
 - Б) Да се дефинишу правила заштите тајних података
 - В) Да се омогући слободан приступ подацима
 - Г) Да се праве јавне набавке за техничку опрему
- (тачан одговор : Б)
12. Који документ треба да садржи преглед података који се класификују?
- А) Одлука о заштити личних података
 - Б) Листа "Потребно поделити са"
 - В) План заштите података
 - Г) Одлука о степену тајности
- (тачан одговор : Г)
13. Шта је главни захтев за рад са тајним подацима?
- А) Регистровање свих корисника тајних података
 - Б) Држање свих тајних података у највећој тајности
 - В) Омогућавање јавности да прегледа податке
 - Г) Стално ажурирање закона о тајним подацима
- (тачан одгово : Б)
14. Који се документ користи за регулацију сарадње између различитих институција?
- А) План заштите података
 - Б) Споразум о међународној сарадњи
 - В) Модел Акта о информационој безбедности
 - Г) Листа „Потребно да зна“
- (тачан одговор : Б)
15. Шта подразумева појам „неопходно поделити са“?
- А) Подела података са свим јавним институцијама
 - Б) Подела података са правним лицима која раде са тајним подацима
 - В) Подела података само са државним органима
 - Г) Подела података са свим органима безбедности
- (тачан одговор : Б)

КОМБИНАЦИЈА 8.

1. **Која институција је задужена за контролу извршавања Закона о тајности података?**
 - А) Канцеларија Савета за националну безбедност
 - Б) Министарство правде
 - В) Министарство одбране
 - Г) Министарство спољних послова

(тачан одговор : А)
2. **Које од наведених података се класификују као "строго поверљиво"?**
 - А) Подаци који се односе на државну безбедност
 - Б) Подаци који се односе на здравствене информације
 - В) Подаци о платама запослених у јавним службама
 - Г) Подаци који се односе на јавне набавке

(тачан одговор : А)
3. **Који је основни циљ увођења система заштите тајних података у органима јавне власти?**
 - А) Повећати продуктивност запослених
 - Б) Обезбедити заштиту важних података од неовлашћеног приступа
 - В) Омогућити лакшу размену података
 - Г) Смањити трошкове управљања подацима

(тачан одговор : Б)
4. **Који документ не мора бити припремљен за примену Закона о тајности података у институцијама?**
 - А) План заштите података
 - Б) Листа тајних података
 - В) Стратегија за управљање ризицима
 - Г) Споразум о сарадњи

(тачан одговор : Г)
5. **Које од наведених радњи не припада унутрашњој контроли заштите тајних података?**
 - А) Праћење складиштења тајних података
 - Б) Одређивање степена тајности података
 - В) Провера приступа тајним подацима
 - Г) Одлука о наименовању руководиоца за тајне податке

(тачан одговор : Г)
6. **Који тип сертификата је потребан за рад са тајним подацима?**
 - А) Сертификат о безбедности
 - Б) Сертификат о заштити личних података
 - В) Сертификат о задовољавању стандарда заштите података
 - Г) Сертификат о безбедности и контролисаним приступима

(тачан одговор : А)
7. **Који је основни разлог за класификацију података као "поверљиво"?**
 - А) Подаци су осетљиви и могу наштетити ако се објаве
 - Б) Подаци су необавезујући за државне органе
 - В) Подаци су већ доступни јавности
 - Г) Подаци се користе искључиво у техничким анализама

(тачан одговор : А)

8. Који од наведених докумената се користи за постављање стандарда заштите података у организацији?
- А) Стратегија информационе безбедности
 - Б) Споразум о безбедносним мерама
 - В) Модел акта о тајности података
 - Г) Статут о безбедности
- (тачан одговор : В)
9. Шта се подразумева под изразом "потребно поделити са"?
- А) Подаци који су доступни за све грађане
 - Б) Подаци који се деле са људима из сличних индустрија
 - В) Подаци који се могу поделити само са лицима која имају овлашћења
 - Г) Подаци који су намењени само за војне сврхе
- (тачан одговор : В)
10. Који орган има овлашћење да одобри рад са тајним подацима у организацијама?
- А) Канцеларија Савета за националну безбедност
 - Б) Министарство правде
 - В) Министарство заштите животне средине
 - Г) Влада Републике Србије
- (тачан одговор : А)
11. Шта је потребно за издавање сертификата за правно лице?
- А) Извештај о унутрашњој контроли
 - Б) Податке о пословним партнерима
 - В) Уверење о безбедности
 - Г) Одлуку о одређивању степена тајности података
- (тачан одговор : В)
12. Које мере су неопходне за заштиту података из категорије "тајно"?
- А) Оповлачење приступа у случају неког инцидента
 - Б) Стално чување у архивама
 - В) Забрана делимичног приступа овим подацима
 - Г) Уклањање свих записа о приступу
- (тачан одговор : А)
13. Како се процењује безбедност података у институцијама?
- А) Кроз ревизију и тестирање система заштите
 - Б) Пошаљу се заштитни подаци међународним агенцијама
 - В) Размени се информације са јавним службама
 - Г) Не постоје посебни захтеви за процену безбедности
- (тачан одговор : А)
14. Који је најважнији документ који институције морају да усвоје како би спроводиле закон о тајности података?
- А) Одлука о ступању на снагу новог закона
 - Б) Писани документ о процени безбедности
 - В) План заштите тајних података
 - Г) Споразум о сигурности података
- (тачан одговор : В)
15. Шта подразумева "унутрашњу контролу" у систему заштите тајних података?
- А) Провера о свим процедурама унутар институције
 - Б) Стални надзор само над финансијским трансакцијама
 - В) Обавезно чување података по завршетку пројекта
 - Г) Стварање јавних извештаја
- (тачан одговор : А)

КОМБИНАЦИЈА 9.

1. **Који документ правно лице мора да поднесе како би добило сертификат за рад са тајним подацима?**
 - А) Потврда о безбедности издата од Министарства правде
 - Б) Листу запослених са приступом тајним подацима
 - В) План заштите тајних података
 - Г) Извештај о испуњавању безбедносних услова
(тачан одговор : В)
2. **Шта је основни циљ индустријске безбедности?**
 - А) Заштита производног процеса од економских и технолошких ризика
 - Б) Заштита права потрошача у индустрији
 - В) Смањење трошкова производње
 - Г) Подизање продуктивности радне снаге
(тачан одговор : А)
3. **Које активности представљају кључне заштитне мере у индустријској безбедности?**
 - А) Процена утицаја на животну средину
 - Б) Провера система заштите података и физичке безбедности
 - В) Подстицање сарадње са конкурентима
 - Г) Стално побољшање маркетинга
(тачан одговор : Б)
4. **Који је следећи корак након одобрења сертификата за правно лице?**
 - А) Израда планова за кризне ситуације
 - Б) Издавање дозвола за рад са тајним подацима
 - В) Оцена безбедносне инфраструктуре
 - Г) Примена мера за заштиту животне средине
(тачан одговор : Б)
5. **Шта је потребно за добијање сертификата за правно лице које се бави индустријском безбедношћу?**
 - А) Потврда о завршеном курсу за индустријску безбедност
 - Б) Писмени уговор са саветником за безбедност
 - В) Процена ризика у погону и инфраструктури
 - Г) Регистар свих запослених у компанији
(тачан одговор : В)
6. **Које мере су најважније за индустријску безбедност?**
 - А) Одржавање механизма за забрану приступа
 - Б) Спровођење обука за све запослене
 - В) Увођење технологија за аутоматизацију процеса
 - Г) Повећање запослености у компанији
(тачан одговор : А)
7. **Који је један од кључних захтева за добијање сертификата за правна лица?**
 - А) Редовне провере финансијских трансакција
 - Б) Испуњавање стандарда безбедности података
 - В) Плаћање накнаде за издавање сертификата
 - Г) Ажурирање свих записа о запосленима
(тачан одговор : Б)

8. **Како правна лица спроводе процену ризика у контексту индустријске безбедности?**
А) Применом стандардизованих обрасца процене
Б) Размени информација са конкуренцијом
В) Креирањем тајних планова за индустријски развој
Г) Признавањем безбедносних иновација
(тачан одговор : А)
9. **Шта је основна разлика између сертификата за индустријску безбедност и сертификата за безбедност података?**
А) Сертификат за индустријску безбедност не захтева специјалистичку обуку
Б) Сертификат за безбедност података се односи на дигиталне уређаје, а индустријски на физичке ризике
В) Индустријска безбедност не укључује управљање људским ресурсима
Г) Безбедност података подразумева само физичку заштиту сервера
(тачан одговор : Б)
10. **Шта треба да се укључи у документ за пријаву сертификата за правно лице?**
А) Документација која доказује финансијску стабилност компаније
Б) Подаци о свим запосленима у компанији
В) Процена ризика од могућих технолошких проблема
Г) Извештај о безбедносним мерама које компанија примењује
(тачан одговор : Г)
11. **Који је важан корак за осигурање индустријске безбедности у фабрикама?**
А) Чување података на једном месту
Б) Инсталирање модерних система за надзор
В) Одржавање континуираног процеса стручног усавршавања
Г) Повећање броја радника на производним тракама
(тачан одговор : Б)
12. **Које од наведених мера није део процеса за добијање сертификата за индустријску безбедност?**
А) Провера приступа тајним информацијама
Б) Спровођење обука за рад са опасним материјама
В) Инсталација видео надзора у свим просторијама
Г) Пријављивање свих нових инвестиција
(тачан одговор : Г)
13. **Шта је кључно за добијање сертификата за рад са тајним подацима у индустријским секторима?**
А) Потврда о безбедности од других компанија
Б) Процена ризика која укључује све могуће опасности
В) Спровођење обавезних медицинских прегледа за све раднике
Г) Активно учешће у националним и међународним форумима
(тачан одговор је под Б)
14. **Који подаци су неопходни за пријаву за сертификат у индустријској безбедности?**
А) Податке о инфраструктури компаније и уговорима
Б) Споразуме са конкурентима и добављачима
В) Листу производних машина и иновација
Г) Детаље о свим радницима који раде са опасним материјама
(тачан одговор : А)

15. Како се одређује да ли компанија испуњава безбедносне услове за добијање сертификата?

- А) Испитује се ефективност система заштите података
 - Б) Прави се обавезна анкета за све запослене
 - В) Ревидира се сва документација компаније
 - Г) Оцењује се колико компанија запошљава радника
- (тачан одговор : А)*

КОМБИНАЦИЈА 10.

1. Који је основни циљ сертификације правних лица за индустријску безбедност?

- А) Повечати производне капацитете
 - Б) Успоставити систем заштите тајних података
 - В) Побољшати маркетиншке стратегије
 - Г) Успоставити систем здравствене заштите
- (тачан одговор : Б)*

2. Шта представља индустријска безбедност у контексту сертификације?

- А) Заштита од природних катастрофа
 - Б) Превенција кибер напада на индустријске системе
 - В) Заштита од технолошких и физичких ризика
 - Г) Побољшање радних услова
- (тачан одговор : В)*

3. Шта правно лице мора да достави како би започело процес сертификације?

- А) Писмо намере од надлежног министарства
 - Б) Уговор са партнерима у иностранству
 - В) План безбедности са дефинисаним мерама
 - Г) Извештај о оперативној ефикасности
- (тачан одговор : В)*

4. Како се идентификују и процењују ризици у индустријској безбедности?

- А) Путем израде анкетних листова за раднике
 - Б) Путем процене могућих еколошких ризика
 - В) Путем процене технолошких и безбедносних слабости
 - Г) Путем мерења радне продуктивности
- (тачан одговор : В)*

5. Који је корак након успешне сертификације за индустријску безбедност?

- А) Обавезна контрола опреме
 - Б) Регуларна процена ефективности безбедносних мера
 - В) Издавање дозвола за увоз сировина
 - Г) Подизање финансијске границе за инвестиције
- (тачан одговор : Б)*

6. Који стандард је основа за сертификацију индустријске безбедности?

- А) Стандард за квалитет у производњи
 - Б) Стандард за безбедност радника
 - В) Стандард за заштиту тајних података
 - Г) Стандард за одрживи развој
- (тачан одговор : В)*

7. Које врсте докумената су потребне за пријаву сертификације индустријске безбедности?

- А) Преглед свих комерцијалних уговора
 - Б) Извештаји о безбедности од конкурентних компанија
 - В) Писани планови и процене безбедности
 - Г) Договори о сарадњи са локалним властима
- (тачан одговор : В)

8. Која је главна сврха процене ризика у индустријској безбедности?

- А) Процењивање ефикасности продаје
 - Б) Процењивање потенцијалних опасности и слабости система
 - В) Процењивање иновација у производњи
 - Г) Процењивање ефеката маркетиншке кампање
- (тачан одговор : Б)

9. Који је важан корак у процесу сертификације за правно лице?

- А) Програм обуке за раднике
 - Б) Потписивање меморандума о разумевању са конкурентима
 - В) Провера и усаглашавање са правним прописима
 - Г) Креирање планова за помоћ у ванредним ситуацијама
- (тачан одговор : В)

10. Који подаци су обавезни за достављање током процеса сертификације?

- А) Листа клијената и партнерских компанија
 - Б) Извештаји о свим технолошким иновацијама
 - В) Извештаји о мерама безбедности и инфраструктури
 - Г) Споразуми о сарадњи са локалним организацијама
- (тачан одговор : В)

11. Како се врши контролисање индустријске безбедности након добијања сертификата?

- А) Путем редовних безбедносних инспекција
 - Б) Путем радних састанака са менаџментом
 - В) Путем квалитетних ревизија производње
 - Г) Путем додатних обука за запослене
- (тачан одговор : А)

12. Који је први корак у процесу сертификације правног лица за индустријску безбедност?

- А) Спровођење обуке за сваког запосленог
 - Б) Достављање извештаја о оперативним активностима
 - В) Процена потенцијалних ризика у индустријским процесима
 - Г) Регистрација свих машина и технологија у компанији
- (тачан одговор : В)

13. Шта је највише захтевано у индустријској безбедности у контексту сертификације?

- А) Заштита интелектуалне својине
 - Б) Заштита од кибер напада и технолошких пропуста
 - В) Организација еколошких пројеката
 - Г) Повећање продаје производа на домаћем тржишту
- (тачан одговор : Б)

- 14. Који корак није део процеса сертификације индустријске безбедности?**
А) Преглед безбедносне инфраструктуре
Б) Оцена ефективности нових маркетиншких стратегија
В) Израда плана заштите од технолошких ризика
Г) Обављање редовних безбедносних провера
(тачан одговор : Б)
- 15. Шта се највише оценјује у процесу сертификације индустријске безбедности?**
А) Безбедност радних места
Б) Услови за живот радника
В) Технолошка стабилност и отпорност на нападе
Г) Капацитети за брзо проширење производње
(тачан одговор : В)

КОМБИНАЦИЈА 11.

- 1. Шта подразумева појам "тајни податак"?**
А) Сви подаци који се односе на јавне политике
Б) Сви подаци који су заштићени Законом о заштити података
В) Подаци од значаја за националну безбедност и одбрану
Г) Подаци који се односе на економску политику
(Тачан одговор : В)
- 2. Шта представља План заштите тајних података у органу јавне власти?**
А) Опис мера безбедности за заштиту свих података
Б) Кључни документ који дефинише мере за заштиту тајних података
В) План који се односи само на људске ресурсе
Г) Споразум између различитих јавних органа
(Тачан одговор : Б)
- 3. Шта је требало да уради сваки орган јавне власти у складу са Законом о тајности података?**
А) Обезбеди тајне податке са највишим степеном заштите
Б) Усмери све ресурсе ка вођењу истрага
В) Успостави систем заштите тајних података
Г) Направи архиву свих јавних података
(Тачан одговор : В)
- 4. Шта се дешава ако се не успостави систем заштите тајних података у органу јавне власти?**
А) Подаци се аутоматски класификују као поверљиви
Б) Ризикује се национална безбедност и кривично дело
В) Подаци се предају у јавну архиву
Г) Орган јавне власти добија нови рок за усаглашавање
(Тачан одговор : Б)
- 5. Шта представља обавезујући део заштите тајних података у органу јавне власти?**
А) План заштите тајних података
Б) Програми обуке запослених
В) Споразум о интерној сарадњи
Г) Контроле приступа личним подацима
(Тачан одговор : А)

6. Ко је одговоран за утврђивање степена тајности података?
А) Министар одбране
Б) Секретар у министарству
В) Руководилац органа јавне власти
Г) Одговорно лице унутрашње контроле
(Тачан одговор : В)
7. Шта је уобичајена мера заштите тајних података?
А) Класична архивирање података
Б) Строге безбедносне мере као што су шифровање и контрола приступа
В) Откривање података одобреним јавним органима
Г) Излагање података на јавним мрежама
(Тачан одговор : Б)
8. Шта се подразумева под “контролом приступа” за тајне податке?
А) Дозвола за коришћење свих врста података
Б) Ограничен приступ према степену тајности
В) Потпуна слобода приступа подацима
Г) Периодично ажурирање јавних података
(Тачан одговор : Б)
9. Које мере безбедности се примењују на осетљиве информације у електронском формату?
А) Постављање информација у јавни домен
Б) Шифровање и контролисан приступ
В) Пренос информација у папирном облику
Г) Потпуно уклањање података из система
(Тачан одговор : Б)
10. Шта се подразумева под терминима “штетност” и “опасност” у контексту тајних података?
А) То су нивои ризика који се односе на систем података
Б) Показатељ колико информације могу да буду корисне за јавност
В) Оцене које се користе за класификацију података
Г) Дефиниције које се користе за дефинисање врсте података
(Тачан одговор : А)
11. Ко је одговоран за спровођење мера заштите тајних података у предузећу?
А) Директор предузећа
Б) Врховни суд
В) Одговорна лица за тајност података
Г) Министар унутрашњих послова
(Тачан одговор : В)
12. Како се осигурава заштита тајних података у међународној сарадњи?
А) Постављање података у јавне базе
Б) Применом међународних безбедносних стандарда и протокола
В) Коришћењем података у свим јавним институцијама
Г) Отварањем свих података за међународне власти
(Тачан одговор : Б)
13. Ко има право да утврди степен тајности података?
А) Министарство здравља
Б) Влада Србије
В) Надлежно лице у органу јавне власти
Г) Лице одговорно за људске ресурсе
(Тачан одговор : В)

14. Шта значи да је неки податак “поверљив”?

- А) Да се мора чувати од свих јавних органа
- Б) Да има минимални степен заштите и не може се открити без одобрења
- В) Да се подаци могу делити са јавним органима
- Г) Да се одмах уништавају након употребе

(Тачан одговор : Б)

15. Како се утврђује да ли податак треба да буде класификован као тајан?

- А) На основу степена ризика по националну безбедност
- Б) Према одлуци председника Републике
- В) Према категорији података која је већ објављена
- Г) Према једноставним правилима о правима грађана

(Тачан одговор : А)