ISSN 1821-4088
COBISS.SR-ID 49270540

СЛУЖБЕНИ ВОЈНИ ЛИСТ

БРОЈ 3 **Београд, 21. јануар 2010.** **ГОДИНА CXXIX**

24.

На основу члана 106. став 3, а у вези са чланом 14. став 2. тачка 23. Закона о одбрани („Службени гласник РС“, бр. 116/07 и 88/09), министар одбране прописује

У П У Т С Т В О
О КОРИШЋЕЊУ РАЧУНАРСКЕ МРЕЖЕ КОМАНДОВАЊА У МИНИСТАРСТВУ ОДБРАНЕ И ВОЈСЦИ СРБИЈЕ

I. ОСНОВНЕ ОДРЕДБЕ

1. Овим упутством прописује се начин коришћења система РАчунарска Мрежа КОмандовања у Министарству одбране и Војсци Србије (у даљем тексту: РАМКО), планирање и организација рада у РАМКО и планирање и организација мера безбедности и заштите у раду у РАМКО.

2. Овим упутством дефинисани су елементи система РАМКО и прописана правила понашања запослених у Министарству одбране и припадника Војске Србије у раду у РАМКО.

3. По одредбама овог упутства поступају организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије.

1. Основни појмови

4. Просторну рачунарску мрежу (*Wide Area Network*) Министарства одбране и Војске Србије (у даљем тексту: *WAN*) чине центри и чворишта везе Министарства одбране и Војске Србије који су повезани спојним путевима и са елементима криптозаштите представљају организациону и техничко-технолошку целину намењену и оспособљену за пренос и заштиту података.

5. Локалну рачунарску мрежу (*Local Area Network*) у Министарству одбране и Војсци Србије (у даљем тексту: *LAN*) чине повезани рачунари и рачунарско-комуникациона опрема размештена на мањем простору (канцеларија, објекат или мања група објеката) намењена за размену информација унутар организационих јединица Министарства одбране, организационих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије.

6. Самостална радна станица је рачунар директно повезан на *WAN*, која је намењена за размену информација из организационих јединица Министарства одбране, организационих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије које немају локалну рачунарску мрежу.

7. Демаркациона тачка између *WAN* и *LAN* у организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије односно самостална радна станица представља позицију физичког прикључка реализованог у *Ethernet* технологији и размештеног у простор којим располаже организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије. За једну организациону јединицу Министарства одбране, организациону јединицу Генералштаба Војске Србије и команду, јединицу и установу Војске Србије може да постоји само једна демаркациона тачка.

8. Демилитаризована зона је логички одвојен део *LAN* у који се смештају серверски рачунари са примењеном контролом приступа из осталог дела *LAN* и из *WAN*.

9. Апликације представљају програмска решења која дају информатичку подршку одређеним сегментима пословања (кадровска евиденција, материјални ресурси, финансије и сл.), које су развијене за потребе тактичких носилаца ради повећања њихове функционалности и ефикасности.

10. Сервиси представљају програмске модуле који обезбеђују опште или специфичне услуге и подржавају функције у систему. Сервиси са хардверском инфраструктуром и системским софтвером пружају базну подршку апликацијама.

2. Дефинисање

11. РАМКО чине локалне рачунарске мреже у Министарству одбране и Војсци Србије и самосталне радне станице предвиђене за рад у РАМКО намењене за размену информација и података битних за подршку руковођењу и командовању и ефикасном функционисању организационих јединица Министарства одбране, организационих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије у рату и миру, које су међусобно повезане у једну функционалну целину преко *WAN*, као и софтверске компоненте РАМКО.

12. Главни РАМКО центар је *LAN* у којој се налазе главни сервери за све сервисе од суштинске важности за функционисање РАМКО, као и главни сервери за апликације, ако њихово постављање није предвиђено на другим локацијама у РАМКО.

13. Корисник РАМКО је организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије којој је одобрено прикључење у РАМКО.

14. Крајњи корисник РАМКО је припадник корисника РАМКО који има право коришћења ресурса РАМКО.

15. Главни администратор РАМКО је лице из Главног РАМКО центра одговорно за функционисање Главног РАМКО центра и надзор РАМКО у целини.

16. Главни администратор заштите РАМКО је лице које одређује Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије (у даљем тексту: Управа за телекомуникације и информатику) и одговорно је за предлагање, спровођење и контролу примене мера безбедности и заштите у РАМКО.

17. Администратор корисника РАМКО је лице из органа информатичког обезбеђења оспособљено за обављање послова администрирања РАМКО. Уколико корисник РАМКО нема орган информатичког обезбеђења, надлежно лице одредиће администратора корисника РАМКО из свог састава, уз сагласност Управе за телекомуникације и информатику.

18. Прикључак у РАМКО представља сваки физички прикључак на опреми за пренос података у РАМКО намењен за прикључење хардверских компонената РАМКО. Прикључци у РАМКО деле се на инфраструктурне прикључке, прикључке корисника РАМКО и прикључке крајњих корисника РАМКО.

19. Инфраструктурни прикључци су физички прикључци на опреми за пренос података намењени за повезивање са другом опремом за пренос података у *WAN*.

20. Прикључци корисника РАМКО су физички прикључци на опреми за пренос података у *WAN* намењени за повезивање са опремом за пренос података или самосталном радном станицом корисника РАМКО.

21. Прикључци крајњих корисника РАМКО су физички прикључци на опреми за пренос података у *LAN* корисника РАМКО.

3. Намена

22. РАМКО је намењен искључиво за потребе руковођења и командовања у Министарству одбране и Војсци Србије и омогућава пренос и дистрибуцију информација у реалном времену.

23. Основни циљ увођења РАМКО је да омогући ефикасно руковођење и командовање у реалном времену стварањем мрежне инфраструктуре за потребе развоја и имплементације информационих система у Министарству одбране и Војсци Србије (у даљем тексту: ИС) и командно-информационих система у Војсци Србије (у даљем тексту: КИС).

4. Хардверске и софтверске компоненте РАМКО

24. Хардверске компоненте РАМКО чине: рачунари, рачунарска опрема, опрема за пренос података и телекомуникациона опрема.

25. Софтверске компоненте РАМКО чине: системски софтвер, сервиси и апликативни софтвер.

26. Системски софтвер је скуп програма који служе за директно управљање хардвером.

27. Апликативни софтвер обухвата: општи апликативни софтвер (текст-процесори, табеларни алати, графички алати и сл.) и наменски апликативни софтвер (КИС, ИС кадровска евиденција, ИС за материјалне ресурсе, ИС финансија и сл.).

28. Компоненте које се користе за испуњење безбедносних сервиса у РАМКО (поверљивост, аутентичност, интегритет, непорецивост и расположивост) могу бити реализоване хардверски, софтверски и хардверско-софтверски.

29. Хардверске и софтверске компоненте РАМКО дефинисане су Захтевима за опрему која се користи у РАМКО који су дати у Прилогу 1 овог упутства и чини његов саставни део. Сходно променама у развоју информационо-комуникационих технологија, Управа за телекомуникације и информатику једном годишње или чешће предложиће измену Прилога 1 овог упутства.

5. Сервиси и апликације у РАМКО

30. Сервиси у РАМКО су: системски сервиси, сервиси командовања и сервиси подршке.

31. Системски сервиси су сервиси који обезбеђују основне функционалности РАМКО или рад сервиса командовања, сервиса подршке и наменског апликативног софтвера.

32. Сервиси командовања су сервиси који обезбеђују ефикасније руковођење и командовање у Министарству одбране и Војсци Србије.

33. Сервиси подршке су сервиси који су реализовани по захтеву тактичких носилаца ради ефикасније размене информација из њихове надлежности.

34. Управа за телекомуникације и информатику води евиденцију сервиса и апликација у РАМКО на обрасцу Сервиси и апликације који се користе у РАМКО који је дат у Прилогу 2 овог упутства и чини његов саставни део.

35. Апликације у РАМКО чине: апликације засноване на Интернет технологијама и апликације намењене за синхронизацију података (процедурални механизми, системски механизми – репликација података и *file transfer*).

36. Безбедоносни механизми за коришћење апликације уграђују се и примењују унутар апликације, што је обавеза носиоца развоја апликације.

37. Управа за телекомуникације и информатику је одговорна за увођење нових сервиса и апликација у РАМКО.

II. ЕЛЕМЕНТИ ОРГАНИЗАЦИЈЕ РАМКО

1. Дефинисање тактичких и техничких носилаца

38. Управа за телекомуникације и информатику је на основу својих надлежности тактички и технички носилац за РАМКО и одговорна је за планирање, развој, организацију, регулативу, опремање и безбедност и заштиту РАМКО.

39. Центар за командно-информационе системе и информатичку подршку (у даљем тексту: ЦКИСИП) је технички носилац за Главни РАМКО центар.

40. Бригада везе је технички носилац за *WAN*, осим у Ваздухопловству и противваздухопловној одбрани где је технички носилац јединица надлежна за телекомуникационо-информатичко обезбеђење Ваздухопловства и противваздухопловне одбране.

41. Центар за примењену математику и електронику (у даљем тексту: ЦПМЕ) је технички носилац за криптографску заштиту података у РАМКО.

42. Управа за телекомуникације и информатику је на основу својих надлежности одговорна за одређивање задатака и обавеза техничким носиоцима у систему РАМКО.

43. Системске основе организације рада РАМКО чине: пројекат рачунарске мреже РАМКО, наређење за телекомуникационо-информатичко обезбеђење, у делу који се односи на надлежности у функционисању телекомуникационо-информатичког система, ово упутство, као и остала акта којима се регулишу аспекти РАМКО.

44. Управа за телекомуникације и информатику као највиши стручни орган за РАМКО, у складу са својом функцијом и надлежностима, обавља следеће задатке:

1) доноси и усваја системске основе организације рада РАМКО;

2) израђује стручна упутства за рад у РАМКО и учествује у изради других прописа из ове области;

3) планира и организује обуку за администраторе РАМКО;

4) планира, организује и контролише безбедност и заштиту у РАМКО;

5) управља адресним простором у РАМКО;

6) дефинише форму и садржај захтева за прикључење корисника у РАМКО;

7) прима захтеве за увођење нових сервиса и апликација, организује и координира њихово тестирање за рад у РАМКО и одобрава њихово увођење на основу добијених резултата;

8) планира, организује и врши контролу рада у РАМКО;

9) предлаже измене прилога овог упутства у складу са насталим потребама;

10) предлаже уређивање осталих питања у вези са РАМКО која нису регулисана овим упутством.

45. ЦКИСИП формира Главни РАМКО центар и обавља следеће задатке:

1) инсталира и обезбеђује функционисање потребног хардвера и софтвера у Главном РАМКО центру;

2) испитује употребљивости нових хардверских и софтверских компонената РАМКО (рачунара, рачунарске опреме, опреме за пренос података и софтверских компонената РАМКО) ради унапређења функционалности РАМКО;

3) пројектује и учествује у увођењу и примени сервиса и апликација које су намењене за РАМКО.

46. Бригада везе односно јединица надлежна за телекомуникационо-информатичко обезбеђење Ваздухопловства и противваздухопловне одбране обезбеђује телекомуникационе ресурсе за функционисање РАМКО и обавља следеће задатке:

1) обезбеђује функционисање *WAN* на транспортном и приступном нивоу;

2) гради мрежу у делу спојних путева и система преноса;

3) обезбеђује непрекидно функционисање система преноса;

4) активира прикључке у РАМКО и прикључује кориснике РАМКО у демаркационој тачки;

5) врши надзор и управљање *WAN* и отклања уочене проблеме;

6) врши процену претњи и ризика по безбедност компонената РАМКО у својој надлежности и имплементира сигурносне механизме до демаркационе тачке са стране *WAN*;

7) обезбеђује криптозаштиту *WAN* линкова.

47. ЦПМЕ обавља послове развоја, увођења и верификације криптографских метода заштите података у РАМКО и пружа стручну помоћ носиоцима развоја апликација које ће се користити у РАМКО у имплементацији безбедносних механизама.

48. Главни администратор РАМКО обавља следеће задатке:

1) врши надзор и управљање над хардверским и софтверским компонентама РАМКО у Главном РАМКО центру;

2) прати рад софтверских компонената РАМКО ван локације Главног РАМКО центра и пружа помоћ надлежним органима у отклањању уочених проблема;

3) врши надзор *WAN* и пружа помоћ Бригади везе односно јединици надлежној за телекомуникационо-информатичко обезбеђење Ваздухопловства и противваздухопловне одбране у отклањању уочених проблема;

4) врши процену претњи и ризика по безбедност Главног РАМКО центра и имплементира сигурносне механизме;

5) предлаже мере безбедности и заштите у РАМКО.

49. Главни администратор заштите РАМКО обавља следеће задатке:

1) врши процену потенцијалних рањивости, претњи и напада у РАМКО;

2) предлаже мере безбедности и заштите у РАМКО;

3) пружа помоћ администраторима корисника РАМКО у дефинисању и примени мера безбедности и заштите у РАМКО;

4) контролише примену мера безбедности и заштите у РАМКО;

5) води евиденцију безбедносних инцидената у РАМКО за систем РАМКО у целини.

50. Администратор корисника РАМКО обавља следеће задатке:

1) инсталира и обезбеђује функционисање потребног хардвера и софтвера у *LAN* или самосталне радне станице за потребе корисника РАМКО;

2) доставља захтеве за приступ сервису или апликацији претпостављеној команди, на основу установљених потреба и прибављене сагласности тактичког носиоца сервиса или апликације; организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде оперативних састава Војске Србије захтеве за приступ сервису или апликацији и прибављену сагласност упућују Управи за телекомуникације и информатику;

3) доставља захтеве за активирање прикључака у РАМКО надлежном стационарном центру везе, на основу добијеног одобрења и створених минималних захтева које треба да задовољи опрема која се користи за РАМКО;

4) доставља захтеве за деактивирање прикључака у РАМКО надлежном стационарном центру везе на основу указане потребе;

5) прикључује рачунаре крајњих корисника РАМКО у *LAN* корисника РАМКО за коришћење одобрених сервиса и апликација;

6) врши процену претњи и ризика по безбедност компонената РАМКО у својој организационој целини, предлаже мере безбедности и заштите, имплементира сигурносне механизме и контролише спровођење мера;

7) организује и изводи обуку корисника за употребу сервиса и апликација у РАМКО;

8) води евиденцију безбедносних инцидената у РАМКО у саставу за који је одговоран.

2. Евиденција и извештавање у РАМКО

51. У РАМКО воде се следеће евиденције: евиденција свих сервиса и апликација, евиденција корисника одређеног сервиса или апликације (корисничких налога), евиденција прикључака у РАМКО, евиденција свих радних станица прикључених у РАМКО (самостална радна станица или станица у *LAN*), евиденција опреме за пренос података у РАМКО и евиденција безбедносних инцидената у РАМКО.

52. Управа за телекомуникације и информатику предлаже форму образаца свих евиденција и, по потреби, предлаже увођење нових евиденција.

53. ЦКИСИП води евиденцију свих сервиса и апликација у РАМКО на обрасцу Евиденција сервиса и апликација у РАМКО који је дат у Прилогу 3 овог упутства и чини његов саставни део.

54. Евиденцију свих корисника (корисничких налога) води тактички носилац за одређени сервис или апликацију, односно лице задужено за администрацију сервиса или апликације на обрасцу Евиденција корисника сервиса или апликације (корисничких налога) који је дат у Прилогу 4 овог упутства и чини његов саставни део.

55. Евиденцију прикључака у РАМКО и Евиденцију опреме за пренос података у РАМКО води Бригада везе (надлежни центар стационарних веза) односно јединица надлежна за телекомуникационо-информатичко обезбеђење Ваздухопловства и противваздухопловне одбране на обрасцима који су дати у прилозима 5 и 6 овог упутства и који чине његов саставни део.

Приступ подацима из става 1. ове тачке обезбеђен је електронским путем и Главном администратору РАМКО.

56. Администратор корисника РАМКО води Евиденцију опреме за пренос података у РАМКО на обрасцу који је дат у Прилогу 6 овог упутства и Евиденцију радних станица у РАМКО на обрасцу који је дат у Прилогу 7 овог упутства и чине његов саставни део.

III. НАЧИН ПРИКЉУЧЕЊА У РАМКО

1. Минимални и препоручени услови за прикључење корисника РАМКО

57. Минимални услови за прикључење корисника РАМКО су:

1) да се поседује један персонални рачунар намењен за формирање самосталне радне станице у РАМКО;

2) да постоји директна линија од локације корисника РАМКО до стационарног центра везе реализована по бакарној или оптичкој кабловској инфраструктури чија траса не излази ван круга објекта или локације Министарства одбране и Војске Србије;

3) да постоји лице одговорно за радну станицу у РАМКО;

4) да су корисници обучени за рад на радној станици РАМКО;

5) да су корисници упознати са правилима рада у РАМКО и прописаним мерама безбедности и заштите.

58. Препоручени услови за прикључење корисника РАМКО су:

1) да постоји организована *LAN* са јавним (*WAN*) и приватним делом мреже и демилитаризованом зоном која се преко рутера везује на прикључак РАМКО у демаркационој тачки;

2) да постоје бар два сервера у демилитаризованој зони *LAN;* улога сервера је да обезбеде функционисање системских сервиса и сервиса подршке у *LAN* корисника РАМКО;

3) да постоји могућност за једноставну интеграцију сервера у *LAN* са сервисима командовања РАМКО;

4) да је одређен администратор *LAN;*

5) да су крајњи корисници РАМКО упознати са правилима рада и мерама безбедности и заштите у РАМКО.

2. Типови прикључака корисника РАМКО

59. Прикључак корисника РАМКО служи да се корисници РАМКО повежу на *WAN*.

60. По времену трајања прикључци корисника РАМКО могу бити: стални (у функцији су непрекидно, а реализују се у складу са плановима развоја мреже и по захтеву организационих јединица Министарства одбране, организационих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије) и привремени (успостављају се по потреби и на одређено време, а реализују се по захтеву организационих јединица Министарства одбране, организационих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије).

61. По броју прикључених рачунара корисника РАМКО, прикључци могу бити: прикључак за самосталну радну станицу, прикључак за групу самосталних радних станица – *ad hoc* мрежа (до 10 рачунара без сервера) и прикључак за *LAN* мрежу.

3. Поступак за прикључење у РАМКО

62. Управи за телекомуникације и информатику захтев за прикључење у РАМКО упућују организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде оперативних састава Војске Србије за себе и своје организационе јединице, односно своје потчињене саставе.

Захтев за прикључење корисника РАМКО је дат у Прилогу 8 овог упутства и чини његов саставни део.

63. Управа за телекомуникације и информатику на основу сагледаних техничких могућности одобрава прикључење у РАМКО. Одобрење за прикључење корисника РАМКО је дато у Прилогу 9 овог упутства и чини његов саставни део.

64. На основу одобрења Управе за телекомуникације и информатику, администратор корисника РАМКО упућује Бригади везе захтев за активирање прикључка у РАМКО.

Захтев за активирање/деактивирање прикључка у РАМКО је дат у Прилогу 10 овог упутства и чини његов саставни део.

4. Поступак за увођење нових сервиса и апликација у РАМКО

65. Предлог за увођење новог сервиса или апликације у РАМКО могу поднети организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде оперативних састава Војске Србије преко надлежног тактичког носиоца за тај сервис или апликацију.

66. Тактички носилац доставља Управи за телекомуникације и информатику захтев за увођење новог сервиса или апликације у РАМКО из своје надлежности ради повећања функционалних и оперативних способности Министарства одбране и Војске Србије.

Захтев за увођење сервиса и апликације у РАМКО је дат у Прилогу 11 овог упутства и чини његов саставни део.

67. Управа за телекомуникације и информатику у сарадњи са тактичким носиоцем и предлагачем разматра захтев ради процене потребних хардверских, софтверских и комуникационих ресурса у РАМКО.

68. Управа за телекомуникације и информатику врши верификацију новог сервиса или апликације и одобрава њихово увођење у РАМКО.

Одобрење за увођење сервиса и апликације у РАМКО је дато у Прилогу 12 овог упутства и чини његов саставни део.

69. Одобрење за увођење новог сервиса или апликације у РАМКО садржи План увођења сервиса или апликације са следећим елементима: начин и динамика обезбеђења неопходног хардвера и софтвера, њихов распоред, дефинисан ниво приоритета саобраћаја новог сервиса у односу на постојећи саобраћај и ресурсе у РАМКО и одговорности током експлоатације сервиса.

5. Коришћење сервиса и апликација у РАМКО

70. Коришћење појединачног сервиса или апликације у РАМКО прописује се упутством којим се, између осталог, регулише начин одржавања сервиса или апликације и са којих рачунара и под којим условима ће бити омогућен приступ датом сервису или апликацији.

За израду и измену упутства о коришћењу сервиса или апликације у РАМКО одговоран је тактички носилац сервиса или апликације.

71. Приликом коришћења сервиса или апликације, корисници су дужни да се придржавају упутства о коришћењу сервиса или апликације и прописаних мера безбедности за рад у РАМКО.

IV. БЕЗБЕДНОСТ И ЗАШТИТА РАМКО

1. Опште одредбе

72. РАМКО је део интегралног система руковођења и командовања и спада у виталне објекте Министарства одбране и Војске Србије које треба заштитити. Примену РАМКО у систему руковођења и командовања треба да прате детаљно разрађене, добро организоване и непрекидно спровођене мере безбедности и заштите РАМКО.

73. Намена безбедности и заштите у РАМКО је да заштити ресурсе РАМКО користећи организационе, административне, персоналне, физичке и посебне мере безбедности и заштите (хардверско-софтверске и безбедносне процедуре) у интегралном, модуларном, слојевитом и скалабилном систему заштите од:

1) случајног или намерног оштећења, неовлашћеног приступа, промене, деструкције и откривања поверљивих података и информација;

2) нарушавања интегритета, поузданости и расположивости сервиса и апликација.

74. Ресурси РАМКО су: подаци и информације, хардверске и софтверске компоненте и кадрови.

75. Потенцијални напади на РАМКО су напади: на мрежну инфраструктуру, на сервисе и апликације, злонамерним програмима и социјалног инжињеринга (напад у којем нападач настоји да дође до осетљивих информација за приступ у РАМКО преваром, крађом и вршењем притиска на припаднике корисника РАМКО).

76. Напади имају за циљ да искористе безбедносне пропусте у компонентама и организацији РАМКО како би угрозили поверљивост, интегритет, аутентичност података и информација, непорецивост трансакција у РАМКО, ефикасност и функционалност РАМКО.

77. Потенцијалне претње за РАМКО су: елементарне непогоде (земљотрес, поплаве, атмосферска електрична пражњења и сл.), људски извори претњи и претње окружења система (дугорочни прекиди напајања електричном енергијом, загађење околине и сл.).

78. Потенцијални људски извори претњи могу бити унутрашњи и спољашњи.

Унутрашњи људски извори претњи су крајњи корисници РАМКО, администратори РАМКО и остала лица у Министарству одбране и Војсци Србије која не користе РАМКО.

Спољашњи људски извори претњи су лица или организације ван Министарства одбране и Војске Србије, а имају за циљ да угрозе безбедност РАМКО. Најчешћи спољашњи извори људских претњи су непријатељски настројена лица, криминалне организације, терористичке организације и стране обавештајне службе.

79. Методе напада на РАМКО су директни и индиректни напади.

Директни напади су напади који искоришћавају техничке карактеристике и особине РАМКО. Најчешћи технички напади су напади на аутентикационе механизме, напади злонамерним програмима и напади укидања сервиса.

Индиректни напади су напади социјалног инжињеринга.

80. Претње безбедности проузроковане случајним оштећењем обухватају: ненамерне грешке, неискуство, грешке у хардверско-софтверским компонентама, незгоде и увођење нових комплексних сервиса и апликација.

81. Рањивост је недостатак или пропуст у хардверско-софтверским компонентама РАМКО или организацији РАМКО, а нападач је може искористити за угрожавање безбедности.

82. Администратор корисника РАМКО врши процену рањивости и извора претњи, одређује ризике испољавања претњи и израђује план мера безбедности и заштите ради отклањања или ублажавања рањивости.

83. Администратор корисника РАМКО може одредити мере безбедности и заштите које нису обухваћене овим упутством, под условом да не угрожавају безбедност ресурса РАМКО.

84. О додатно одређеним мерама безбедности и заштите које нису обухваћене овим упутством, администратор корисника РАМКО извештава надлежно лице корисника РАМКО и Главног администратора заштите РАМКО. За додатно одређене мере безбедности и заштите сагласност даје Главни администратор заштите РАМКО, а одобрава их надлежно лице корисника РАМКО.

Мере безбедности и заштите РАМКО су дате у Прилогу 13 овог упутства који чини његов саставни део.

85. Безбедност и заштита РАМКО може се проширити додатним мерама безбедности и заштите према безбедносној процени корисника РАМКО, а све мере безбедности и заштите РАМКО појединачног корисника РАМКО дефинишу се на обрасцу који је дат у Прилогу 14 овог упутства и чини његов саставни део.

86. У случају нарушавања безбедности РАМКО, администратор корисника РАМКО одмах искључује из РАМКО локацију на којој се инцидент догодио и врши евидентирање инцидента, а безбедносни инцидент се пријављује линијом крајњи корисник РАМКО – администратор корисника РАМКО – надлежно лице корисника РАМКО, Главни администратор заштите РАМКО и Главни администратор РАМКО – надлежни орган Војнобезбедносне агенције Министарства одбране и Управа за телекомуникације и информатику.

87. Евиденција о безбедносним инцидентима у РАМКО води се на обрасцу који је дат у Прилогу 15 овог упутства и чини његов саставни део.

88. Системски приступ у решавању безбедности и заштите РАМКО и примене одговарајућих мера на потенцијалне претње обухвата следеће активности:

1) одређивање ресурса које треба заштитити;

2) вршење анализе могућих опасности и угрожености система и разрада мера безбедности и заштите које ће бити саставни део плана безбедности и заштите;

3) израда плана безбедности и заштите од могућих опасности;

4) непрекидно надгледање примене и ефикасности мера безбедности и заштите и њихово усавршавање у току експлоатације РАМКО;

5) извођење обуке крајњих корисника и администратора РАМКО у примени мера безбедности и заштите;

6) развој свести о значају безбедности и заштите.

89. Основна начела безбедности и заштите РАМКО су:

1) одговорност командне структуре, одговорних лица и корисника сервиса и апликација;

2) правовременост предузимања мера безбедности и заштите;

3) свеобухватност предузимања мера безбедности и заштите:

4) доследност у предузимању и придржавању мера безбедности и заштите;

5) једноставност функционисања свих елемената РАМКО.

90. Мере безбедности и заштите се спроводе у процесу планирања, развоја, организације, опремања, увођења и функционисања РАМКО системским приступом и придржавањем основних начела безбедности и заштите РАМКО.

2. Одговорност

91. Управа за телекомуникације и информатику је одговорна за дефинисање, ажурирање, успостављање, контролу мера безбедности и заштите РАМКО у организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије и набавку софтверско-хардверских решења за безбедност и заштиту у РАМКО.

92. Управа за телекомуникације и информатику одредиће Главног администратора заштите РАМКО који има улогу консултанта, надзорног и контролног органа у свим пословима који се односе на безбедност и заштиту ресурса РАМКО.

93. Надлежно лице корисника РАМКО одговорно је за: идентификацију и безбедност и заштиту ресурса РАМКО у својој надлежности и организацију, дефинисање мера безбедности и заштите, њихово спровођење и контролу у складу са прописима.

94. За планирање и спровођење мера безбедности и заштите у РАМКО одговорне су организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије које су корисници РАМКО.

95. Са планом мера безбедности и заштите корисника РАМКО мора бити сагласан орган Војнобезбедносне агенције Министарства одбране надлежан за корисника РАМКО.

96. Крајњи корисници и администратори РАМКО су одговорни за примену мера безбедности и заштите у складу са дефинисаним мерама безбедности и заштите у организационој јединици.

97. Војнобезбедносна агенција Министарства одбране учествује у планирању, организовању и контроли мера безбедности и заштите РАМКО и планира, организује и спроводи мере контраобавештајне заштите РАМКО у складу са прописима.

3. Избор особља за рад у РАМКО

98. За рад на елементима РАМКО одређују се лица која имају одговарајуће квалификације, завршене специјалистичке курсеве и сагласност Управе за телекомуникације и информатику.

99. За лица која су предвиђена за рад на елементима РАМКО мора се извршити безбедносна провера.

4. Усклађеност праксе и безбедности и заштите РАМКО

100. Уколико се утврди неусклађеност плана мера безбедности и заштите корисника РАМКО са безбедношћу и заштитом РАМКО према овом упутству или неодговарајућа примена прописаних мера безбедности и заштите, контролни орган известиће надлежне о природи и озбиљности повреде безбедности и заштите РАМКО и, по потреби, захтевати хитно спровођење мера за отклањање недостатака.

101. На основу процене угрожености безбедности и заштите ресурса РАМКО против прекршиоца предузеће се одговарајуће мере.

V. ЗАВРШНА ОДРЕДБА

102. Ово упутство ступа на снагу осмог дана од дана објављивања у „Службеном војном листу“.

Р.в.п. бр. 2
18. јануара 2010. године
Београд

Министар одбране
Драган Шутановац, с. р.

Прилог 1

Захтеви за опрему која се користи у РАМКО

ХАРДВЕР				СОФТВЕР		
Тип опреме	**Компонента**	**Минимална**	**Препоручена**	**Системски**	**Кориснички**	**Антивирусна заштита**
Радна станица	Процесор	*Pentium 3*	*Pentium 4*	*Windows XP Pro with SP2*	*Microsoft Office XP* *Internet Eksplorer v6* *Outlook Express v6*	*NOD32 v4 +*
	Радна меморија	*256 MB*	*512 MB +*			
	Харддиск	*20 GB*	*40 GB +*			
	Графичка картица	*Интегрисана са 8 MB дељене RAM меморије*	*PCI VGA Card sa 128 MB RAM +*			
	Монитор	*15" CRT*	*17" CRT +*			
	Оптички уређај	CD читач	*DVD* читач +			
	Тастатура	*Стандардна*	*Стандардна*			
	Миш	*Оптички*	*Оптички*			
	УПС уређај	–	*650 VA +*			
	Штампач	–	*Laserski c/b A4 +*			
	Скенер	–	*A4 +*			
Сервер	Процесор	*Pentium 4*	*Xeon +*	*Windows 2000 Server +*	*Према намени сервера*	*NOD32 v4 +*
	Радна меморија	*512 MB +*	*2 GB +*			
	Харддиск	*160 GB +*	*2 x 300 GB+*			
	Оптички уређај	*DVD писач*	*DVD писач*			
	УПС уређај	*1000 VA*	*3000 VA*			
Опрема за пренос података	Рутер *WAN*	*CISCO 3750 24x*	*CISCO 7606*	*CISCO IOS ...*	–	–
	Модем *WAN – LAN*	*G HDSL 2Mb/s*		*Firmware: Ver 2.1* *IOS ...*	–	–
	Рутер *LAN*	*CISCO 1741*	*CISCO 2811*	*CISCO IOS ...*	–	
	Switch LAN	*TP LINK 3428*	*CISCO 29xx*	*IOS ...са активираним Port Security механизмом заштите*	–	

Прилог 2

С П И С А К
сервиса и апликација који се користе у РАМКО

Редни број	Назив сервиса или апликације	Тактички носилац	Технички носилац	Врста	Кратак опис сервиса или апликације
1	2	3	4	5	6

Напомена:

1. У колону 1 уноси се редни број сервиса или апликације.
2. У колону 2 уноси се званичан назив апликације или сервиса.
3. У колону 3 уноси се назив тактичког носиоца за сервис или апликацију.
4. У колону 4 уноси се назив техничког носиоца за сервис или апликацију.
5. У колону 5 уноси се податак о врсти, а врста може бити сервис или апликација. Ако је сервис, он може бити: системски сервис, сервис командовања и сервис подршке.
6. У колону 6 уноси се кратак опис функционалности сервиса или апликације.

Прилог 3

Евиденција сервиса и апликација у РАМКО

Редни број	Назив сервиса или апликације	Опис сервиса или апликације	Врста	*IP* адреса сервера	Тактички носилац	Одговорно лице		
			Статус	Порт апликације	Технички носилац	Име и презиме	Организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије	Контакт телефон
1	2	3	4	5	6	7	8	9

Напомена:

1. У колону 1 уноси се редни број сервиса или апликације.
2. У колону 2 уноси се званичан назив апликације или сервиса.
3. У колону 3 уноси се кратак опис функционалности сервиса или апликације.
4. У колону 4 уносе се врста и статус сервиса или апликације. Статус сервиса или апликације може бити: А – активан (извршава се), Т – тестирање (у фази тестирања), М – модификација (у фази надоградње) и Н – неактиван (тренутно се не извршавају на РАМКО).
5. У колону 5 уноси се *IP* адреса сервера на којем се извршава сервис или апликација и порт путем којег се приступа сервису или апликацији.
6. У колону 6 уноси се назив тактичког и техничког носиоца за сервис или апликацију.
7. У колоне 7, 8 и 9 уносе се подаци о одговорном лицу.

Прилог 4

Евиденција корисника сервиса или апликације (корисничких налога)

_____
(назив сервиса или апликације)

Редни број	Назив корисничког налога	Врста налога	Статус	Основ отварања налога		Одговорно лице			
			Датум стављања у статус	Деловодни број	Организациона јединица која је издала наређење	Име и презиме	Формацијска дужност	Организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије	Контакт телефон
1	2	3	4	5	6	7	8	9	10

Напомена:

1. У колону 1 уноси се редни број корисника сервиса или апликације.
2. У колону 2 уноси се назив корисничког налога.
3. У колону 3 уноси се врста налога којој припада кориснички налог (администратор, корисник и сл.).
4. У колону 4 уносе се статус налога (А – активан, Н – неактиван, С – суспендован) и датум преласка у статус.
5. У колону 5 уноси се деловодни број наређења на основу којег је отворен кориснички налог.
6. У колону 6 уноси се назив организационе јединице која је издала наређење за отварање корисничког налога.
7. У колоне 7, 8, 9 и 10 уносе се подаци о лицу коме је додељен кориснички налог.

Прилог 5

Евиденција прикључака у РАМКО

_____
(организациона јединица)

Редни број	Корисник (организациона јединица)	Врста уређаја	Тип порта	Врста порта	*IP* адреса	Статус порта	Број захтева	Број одобрења	Сервис и апликација
			Капацитет	Број прикључка	*MAC* адреса				
1	2	3	4	5	6	7	8	9	10

Напомена:

1. У колону 1 уноси се редни број прикључка.
2. У колону 2 уносе се подаци о кориснику (функционална дужност) порта.
3. У колону 3 уноси се врста уређаја.
4. У колону 4 уносе се тип порта (серијски, *ethernet*, …) и капацитет порта (максималан капацитет).
5. У колону 5 уноси се врста порта – интерни (портови крајњих корисника РАМКО) и екстерни (портови према *WAN*).
6. У колону 6 уноси се *IP* адреса и *MAC* адреса корисничког уређаја или екстерног порта.
7. У колону 7 уноси се статус порта (А – активан и Н – неактиван).
8. У колону 8 уноси се број захтева за прикључак.
9. У колону 9 уноси се број одобрења.
10. У колону 10 уносе се подаци о сервисима и апликацијама које користи корисник на прикључку.

Прилог 6

Евиденција опреме за пренос података у РАМКО

_____
(стационарни центар веза, односно центар стационарних веза)

Редни број	Назив уређаја	Врста уређаја	Интерфејс			
			Тип	Статус	Датум стављања у статус	MAC адреса
1	2	3	4	5	6	7

Напомена:

1. У колону 1 уноси се редни број опреме за пренос података.
2. У колону 2 уноси се назив уређаја.
3. У колону 3 уноси се податак о врсти уређаја.
4. У колону 4 уноси се тип интерфејса (серијски, *ethernet* и сл.).
5. У колону 5 уноси се податак о статусу интерфејса (А – активан, Р – у резерви и С – суспендован).
6. У колону 6 уноси се датум стављања интерфејса у статус.
7. У колону 7 уноси се *MAC* адреса.

Прилог 7

Евиденција радних станица у РАМКО

_____
(организациона јединица)

Редни број	**Назив радне станице**	**Хардверске карактеристике**	**Системски и апликативни софтвер**	**Инсталирани сервиси и апликације**	***IP* адреса или опсег** ***MAC* адреса**	**Број прикључка на мрежном уређају**
1	2	3	4	5	6	7

Напомена:

1. У колону 1 уноси се редни број радне станице.
2. У колону 2 уноси се назив радне станице (нпр. Хост 01, ...).
3. У колону 3 уносе се хардверске карактеристике радне станице (*Klasa/CPU/RAM/Video/Monitor,* нпр. P4/1,6/1000/64/17).
4. У колону 4 уносе се подаци о системском и апликативном софтверу на радној станици (оперативни систем, пакет за канцеларијско пословање, антивирусни софтвер, претраживач и сл.).
5. У колону 5 уносе се подаци о сервисима и апликацијама које користи корисник на радној станици.
6. У колону 6 уноси се *IP* адреса и *MAC* адреса корисничког уређаја.
7. У колону 7 уноси се број прикључка на мрежном уређају.

Прилог 8

Захтев за прикључење корисника РАМКО

Назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије	
Тип прикључка у РАМКО	
Број рачунара на прикључку	
Локација (зграда и просторија у згради) на којој треба обезбедити прикључење у РАМКО	
Образложење захтева (навести сервисе и апликације који би се користили и локацију сервера на којима се извршавају)	
Администратор корисника РАМКО (чин, име, презиме, телефон, функционална дужност и информатички курсеви)	

Прилог 9

Одобрење за прикључење корисника РАМКО

Назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије	
Одобрена брзина комуникације у РАМКО	
Тип прикључка у РАМКО	
Опсег *IP* адреса за корисника РАМКО	
Локација (зграда и просторија у згради) на којој се обезбеђује прикључење на РАМКО	
Списак одобрених сервиса и апликација	
Неопходне информације за све одобрене сервисе и апликације (*IP* адреса, *TCP/UDP* порт)	
Број прикључка на РАМКО на којем се реализује прикључење	
Организационо-техничке информације значајне за повезивање	

Прилог 10

Захтев за активирање односно деактивирање прикључка у РАМКО

_____
(организациона јединица)

Редни број	Корисник сервиса или апликације	Врста уређаја	Тип порта	Врста порта	*IP* адреса	Статус порта	Сервис и апликација
			Капацитет	Број прикључка	*MAC* адреса		
1	2	3	4	5	6	7	8

Напомена:

1. У колону 1 уноси се редни број прикључка.
2. У колону 2 уноси се податак о кориснику сервиса или апликације (функционална дужност или организациона јединица).
3. У колону 3 уноси се податак о врсти уређаја.
4. У колону 4 уносе се подаци о типу порта (серијски, *ethernet*, …) и капацитету порта (максималан капацитет).
5. У колону 5 уносе се подаци о врсти порта: интерни (портови крајњих корисника РАМКО) и екстерни (портови према *WAN*) и броју прикључка.
6. У колону 6 уноси се *IP* адреса и *MAC* адреса корисничког уређаја или екстерног порта.
7. У колону 7 уноси се податак о статусу порта (А – активан или Н – неактиван).
8. У колону 8 уносе се подаци о сервисима и апликацијама које захтева корисник на прикључку, а које је одобрила Управа за телекомуникације и информатику.

Прилог 11

Захтев за увођење сервиса или апликације у РАМКО

1	Назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије		
2	Назив сервиса или апликације		
3	Сврха коришћења сервиса или апликације		
4	Образложење захтева		
5	Тактички носилац		
6	Технички носилац		
7	Захтеви за функционисање сервиса или апликације	Хардверско-софтверски	
		Систем за управљање базом података	
		Клијентски део сервиса или апликације	
		ODBC, OLE DB, …	
		IP адреса и порт	
		Остало	
8	Одговорно лице	Чин, име и презиме	
		Организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије	
		Контакт телефон	
9	Врста сервиса или апликације		

Напомена:

1. У ред 1 уноси се назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије која захтева увођење новог сервиса или апликације.
2. У ред 2 уноси се назив сервиса или апликације.
3. У ред 3 уноси се сврха коришћења сервиса или апликације.
4. У ред 4 уноси се кратак опис функционалности сервиса или апликације.
5. У ред 5 уносе се подаци о тактичком носиоцу.
6. У ред 6 уносе се подаци о техничком носиоцу.
7. У ред 7 уносе се следећи подаци: посебни хардверско-софтверски захтеви за функционисање сервиса или апликације, захтеви за функционисање сервиса или апликације који се односе на систем за управљање базом података, захтеви за функционисање сервиса или апликације који се односе на чеони део сервиса или апликације, захтеви за функционисање сервиса или апликације који се односе на мрежне протоколе и приступне механизме, подаци о порту и *IP* адреси сервера на којем се извршава сервис или апликација и подаци о осталим техничким детаљима сервиса или апликације.
8. У ред 8 уносе се подаци о одговорном лицу.
9. У ред 9 уноси се податак о врсти сервиса или апликације. Статус сервиса или апликације може бити: А – активан (извршава се), Т – тестирање (у фази тестирања), М – модификација (у фази надоградње) и Н – неактиван (тренутно се не извршавају у РАМКО).

Прилог 12

Одобрење за увођење сервиса или апликације у РАМКО

1	Назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије		
2	Назив сервиса или апликације		
3	Сврха коришћења сервиса или апликације		
4	Образложење одобрења		
5	Верификовани захтеви за функционисање сервиса или апликације	Хардверско-софтверски	
		Систем за управљање базом података	
		Клијентски део сервиса или апликације	
		ODBC, OLE DB, …	
		IP адреса, порт	
		Остало	
6	Одговорно лице	Чин, име и презиме	
		Организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије	
		Контакт телефон	

Напомена:

1. У ред 1 уноси се назив организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије којој је одобрено увођење новог сервиса или апликације.
2. У ред 2 уноси се назив сервиса или апликације.
3. У ред 3 уноси се сврха коришћења сервиса или апликације.
4. У ред 4 уноси се образложење одобрења.
5. У ред 5 уносе се следећи подаци: посебни хардверско-софтверски захтеви за функционисање сервиса или апликације, захтеви за функционисање сервиса или апликације који се односе на систем за управљање базом података, захтеви за функционисање сервиса или апликације који се односе на чеони део сервиса или апликације, захтеви за функционисање сервиса или апликације који се односе на мрежне протоколе и приступне механизме, подаци о порту и *IP* адреси сервера на којем се извршава сервис или апликација и подаци о осталим техничким детаљима сервиса или апликације.
6. У ред 6 уносе се подаци о одговорном лицу.

Прилог 13

МЕРЕ БЕЗБЕДНОСТИ И ЗАШТИТЕ РАМКО

1. Физичка заштита елемената РАМКО и окружења у којем се налазе

Физичким мерама безбедности и заштите мора бити обезбеђен приступ свим компонентама РАМКО.

Физички приступ опреми за пренос података у РАМКО је дозвољен само надлежним лицима уз јасно дефинисане одговорности.

Компоненте у *WAN* мрежи РАМКО смештају се у посебне просторије (стационарни центри везе и рачунски центар). Приступ просторијама је обезбеђен сигурносним бравама или идентификационим картицама.

Физички приступ телекомуникационим, мрежним уређајима и уређајима за заштиту треба раздвојити посебним ормарима. Уколико ово није могуће или није практично, применити мере логичке заштите (заштита приступа лозинком или печаћење уређаја).

У просторијама у којима се налазе уређаји треба да се обезбеде услови у погледу температуре, притиска и влажности ваздуха.

Опрема за пренос података и сервери морају бити прикључени на уређаје за непрекидно напајање.

У просторијама где су смештени опрема за пренос података и сервери, ако је то могуће, треба инсталирати опрему за гашење пожара, систем за детекцију пожара и поплава и видео надзор.

У просторијама у којима су смештени опрема за пренос података и сервери могу бити само цевоводи који су неопходни за рад и који се могу затворити на безбедном и приступачном месту.

Лица која користе опрему морају бити оспособљена за предузимање потребних мера у случају пожара, поплаве, нестанка струје или других врста опасности.

Електричне инсталације у просторијама у којима је смештена опрема морају бити уграђене и одржаване у складу са прописима и техничким нормативима за посебну заштиту електромагнетских уређаја од пожара. Поред тога, треба обезбедити заштитно уземљење свих електропроводних компонената опреме и уградити заштитни струјни прекидач.

2. Безбедност и заштита оперативног система сервера и радне станице

На сервере и радне станице треба инсталирати оперативни систем који је одобрила Управа за телекомуникације и информатику, а његово ажурирање новом верзијом, функционалним и безбедносним побољшањима (закрпама) радити само након њихове верификације у тестном окружењу.

За праћење рањивости у оперативним системима, апликацијама, сервисима и системима за управљање базама података који су прописани овим упутством одговорни су органи информатичког обезбеђења.

За тестирање, верификовање и дистрибуцију нових верзија оперативних система и функционалних и безбедносних побољшања одговоран је ЦКИСИП.

Тестирање, верификовање и дистрибуцију функционалних и безбедносних побољшања за серверски оперативни систем вршити најмање два пута годишње или по указаној потреби.

Одговорно лице за функционисање РАМКО преузима нова функционална и безбедоносна побољшања оперативних система.

Онемогућити или деинсталирати све непотребне сервисе оперативног система (серверског и корисничког) како не би успоравали рад оперативног система или не би били искоришћени за спровођење напада на РАМКО.

Забрањује се инсталирање сервиса оперативних система који нису у функцији РАМКО.

Пријаву корисника у РАМКО реализовати аутентикационим механизмом логовања применом корисничког имена и лозинке или применом напредних механизама аутентикације (нпр.: *smart* картице са дигиталним сертификатима, биометријски механизми за аутентикацију и сл.).

Корисничким налозима у доменској рачунарској мрежи управља одговорно лице за функционисање РАМКО, а на појединачним радним станицама управља лице које дужи радну станицу.

Администраторским налозима појединачних радних станица управља одговорно лице за функционисање РАМКО.

Када један рачунар користи више корисника, за сваког корисника треба отворити кориснички налог и доделити му лозинку.

Администратор корисника РАМКО дефинише права приступа дељеним ресурсима на мрежи и имплементира их креирањем корисничких група и корисничких налога и применом механизама контроле приступа информатичким ресурсима.

Правити историју дневничких записа серверског оперативног система, сервиса и апликација и најмање једном недељно копирати на CD/DVD медиј. Историју дневничких записа чувати на безбедном месту годину дана.

Одговорно лице за функционисање РАМКО у организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије одговара за безбедност и заштиту: података на серверу, конфигурационих фајлова, дневничких записа, сервиса и апликација инсталираних на серверски оперативни систем и контролу корисничких радних станица.

Корисник је одговоран за безбедност података на радној станици и приступ радној станици.

Забрањује се преузимање безбедносних шаблона са Интернета или других извора за оперативне системе.

Забрањено је удаљено администрирање оперативног система, сервиса, апликација или база података у другој организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије, осим у случају када орган информатичког обезбеђења РАМКО из ЦКИСИП пружа помоћ одговорном лицу за РАМКО друге организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије и само уз његову сагласност.

3. Безбедност и заштита сервиса електронске поште

Након инсталације сервиса електронске поште обрисати или онемогућити све сервисе који су инсталирани у оквиру апликације електронске поште, а нису потребни за функционисање сервиса електронске поште.

Обрисати дате примере, тест фајлове, непотребну документацију и опасне или непотребне команде у апликацији за електронску пошту.

Тестирање, верификовање и дистрибуцију функционалних и безбедносних побољшања за сервис електронске поште вршити два пута годишње или по указаној потреби. ЦКИСИП је одговоран за тестирање, верификовање и дистрибуцију функционалних и безбедносних побољшања.

Безбедносне шаблоне које произвођач апликације за електронску пошту доставља уз инсталацију и безбедносни шаблони које администратор преузме са Интернета морају се пре примене тестирати и верификовати. ЦКИСИП је једини одговоран за креирање нових шаблона, преузимање, тестирање, верификовање и дистрибуцију безбедносних шаблона организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије.

Одговорним лицима за РАМКО у организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије дозвољено је да инсталирају само безбедносне шаблоне добијене званичним путем од Управе за телекомуникације и информатику.

Контрола приступа апликацији за електронску пошту и контрола приступа оперативном систему мора да буде рестриктивна да би се онемогућио приступ информацијама које нису за јавну употребу, као што су: системски фајлови, конфигурациони фајлови, безбедносни фајлови, дневнички записи и фајлови података.

Контролу приступа апликације за електронску пошту и контролу приступа оперативном систему подесити тако да једна другу не потиру.

Сервис електронске поште подесити тако да не исцрпљује ресурсе сервера на којем је инсталиран.

Забрањује се дистрибуирање активног садржаја и извршних фајлова путем електронске поште.

Корисник је одговоран за слање информација и података дефинисаног степена тајности. Електронском поштом у РАМКО могу се преносити подаци и информације степеноване највише степеном поверљивости „СТРОГО ПОВЕРЉИВО“.

Прописати поступак у случају добијања електронске поште од непознатог пошиљаоца.

Клијентски програм електронске поште подесити тако да се захтева аутентикација приликом пријема и слања порука.

За тестирање, верификовање, имплементацију и дистрибуцију функционалних и безбедносних побољшања за клијентски програм електронске поште у својим и потчињеним организационим јединицама надлежна

су одговорна лица за РАМКО у организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије.

Конфигурацију сервиса електронске поште треба подесити тако да прави дневничке записе који ће омогућити надгледање и контролу порука које се размењују приликом повезивања и слања порука између серверске и клијентске апликације електронске поште.

Дневничке записе анализирати и на основу добијених резултата побољшавати функционалност и безбедност сервиса електронске поште.

Правити све неопходне заштитне копије сервиса електронске поште које ће омогућити брз и ефикасан опоравак овог сервиса у случају престанка његовог рада или губитка података проузрокованог нападима или другим нежељеним догађајима.

4. Безбедност и заштита *Web* сервиса

Сви кориснички програми и сервиси који нису потребни за функционисање *Web* сервиса морају бити деинсталирани.

Тестирање, верификовање и дистрибуцију функционалних и безбедносних побољшања за серверске технологије које се користе (активне серверске странице и систем за управљање базама података) вршити два пута годишње или по указаној потреби. ЦКИСИП је одговоран за тестирање, верификовање и дистрибуцију функционалних и безбедносних побољшања.

Сви подразумевани налози на апликативном серверу и серверу базе података морају бити обрисани, искључени или им се мора променити подразумевана лозинка.

Пре инсталације апликације *Web* сервера, серверска радна станица мора бити конфигурисана у складу са безбедношћу и заштитом серверског оперативног система.

Апликација *Web* сервера не сме бити покренута са администраторским привилегијама.

Web сервер може да генерише и шаље *e-mail* поруке, али не сме да их прима.

Комуникација са *Web* сервером је дозвољена само на порту на којем се извршава *Web* сервис. Сви портови који нису потребни морају бити искључени.

За аутентикацију страна у комуникацији и енкрипцији између клијента и сервера користити искључиво сигурне протоколе (*SSL* и *TLS*).

На клијентским рачунарима користити службене *Web* претраживаче. *Web* претраживаче конфигурисати са највишим нивоом сигурности који омогућава функционисање апликације.

У случају нежељеног догађаја, отказа сервера или сервиса није дозвољено аутоматско рестартовање без интервенције администратора.

Забранити коришћење активних садржаја, а ако је њихово коришћење неопходно дефинисати локације са којих их је дозвољено учитавати.

5. Безбедност и заштита опреме за пренос података и комуникационе инфраструктуре

Приступ елементима комуникационе инфраструктуре мора бити обезбеђен физичким мерама безбедности и заштите.

Приступ свим рачунарско-комуникационим уређајима (рутери, свичеви и сл.) мора бити обезбеђен лозинкама. Подразумеване лозинке произвођача морају бити промењене.

Дозвољен је саобраћај само између познатих рутера.

Рутери морају бити конфигурисани тако да дозволе само саобраћај по потребним протоколима. На интерфејсима рутера морају бити имплементиране контролне листе приступа. Сви интерфејси који се не користе морају бити искључени.

Удаљени приступ и конфигурисање уређаја су дозвољени коришћењем безбедних протокола.

6. Безбедност и заштита од злонамерних програма и кода

Управа за телекомуникације и информатику као тактични носилац одговорна је за избор, набавку, тестирање и дистрибуцију антивирусног софтвера.

Антивирусни програм инсталирати на свим серверима РАМКО и радним станицама. За инсталирање и конфигурисање антивирусног програма и обезбеђивање ажурне антивирусне базе одговара одговорно лице за РАМКО у организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије.

Антивирусни програм ажурирати једном недељно, по потреби, и чешће.

Корисници и одговорна лица за РАМКО у организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије, у оквиру својих надлежности, морају редовно да проверавају садржај диска на злонамерне програме, ажурирају антивирусну базу и отклањају пронађене злонамерне програме.

Забрањује се инсталирање софтвера на сервере и радне станице РАМКО који није прописан овим упутством.

Забрањује се коришћење апликација и сервиса који имају имплементиран нежељени код или га позивају из апликације.

Апликације и сервисе пре стављања у функцију на РАМКО треба тестирати на функционалност и безбедност. За тестирање апликација и сервиса за РАМКО одговорна је Управа за телекомуникације и информатику, а спроводи га технички носилац ЦКИСИП.

7. Заштитне копије

Заштитне копије корисницима РАМКО обезбеђују корисничке податке, функционалност сервиса и апликација након уништења или оштећења која су настала услед непријатељских напада, отказа хардвера, грешака корисника, природних катастрофа и других несрећа.

Под заштитним копијама подразумева се прављење резервних копија корисничких података, конфигурационих и *log* фајлова, критичних фајлова за функционисање оперативних система (серверских, корисничких и комуникационих) или целих оперативних система, апликација, сервиса и базе података.

Заштитне копије треба да омогуће брзо и ефикасно враћање у функцију система у случају нежељених догађаја.

Заштитне копије треба радити у време када се не умањује расположивост сервиса, апликација, база података и комуникационих капацитета РАМКО.

У организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије, зависно од могућности, применити један модел или више модела за чување података. Модели за чување података су: неструктуирани модел, модел потпуних и делимичних заштитних копија и модел континуиране заштите података.

Неструктуирани модел подразумева прављење резервних копија за минимум података који су неопходни за опоравак.

Модел потпуних и делимичних резервних копија подразумева прављење целовите копије у датом тренутку, а затим прављење мањих копија у односу на целовиту копију. Овај модел омогућава рестаурацију података у тачно одређеним временским тачкама у односу на целовиту копију.

Модел континуиране заштите омогућава да систем сам евидентира сваку промену и аутоматски направи копије података у реалном времену (*RAID-1, RAID-5* и синхронизовано прављење резервних копија на другој локацији).

Заштитне копије треба радити по процени одговорног лица и интензитета промена битних података за функционисање РАМКО. Заштитне копије се раде по насталој промени (дневна, недељна и месечна).

За чување заштитних копија користити магнетне траке, екстерне харддискове и CD/DVD медије. Изузетно, за прављење копија конфигурационих фајлова и оперативног система активне комуникационе опреме применити удаљено копирање на безбедну локацију.

Успоставити ротациону шему поновног коришћења медија за прављење резервних копија.

Чувати најмање три задње резервне копије. Медији за чување резервних копија који су стари најмање три генерације могу се поново користити.

Резервне копије обележити (назив и време прављења резервне копије) и чувати их закључане у металној каси на другој локацији. Резервне копије се могу чувати и на месту настанка, али мора постојати и резервна копија на другој локацији на основу које се може урадити опоравак.

Исправност резервних копија и процедуру израде заштитних копија тестирати најмање једном у шест месеци, а по процени и чешће.

Надлежни орган информатичког обезбеђења, односно одговорно лице за РАМКО у организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије извршава следеће задатке:

1) процењује осетљиве и критичне податке за које је потребно правити резервне копије;

2) прави план прављења резервних копија;

3) прави заштитне копије серверског оперативног система и података које организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије презентује преко РАМКО, комуникационог оперативног система и конфигурационих фајлова, апликација, сервиса и база података;

4) верификује успешно прављење резервних копија;

5) води евиденцију урађених резервних копија;

6) одлаже копије на безбедно место;

7) тестира исправност резервних копија и процедуру за прављење заштитних копија;

8) рестаурира податке са резервних копија.

8. Управљање корисничким приступом

Приступ свим ресурсима РАМКО мора бити обезбеђен применом механизама аутентикације и ауторизације. Провера аутентичности се врши на основу онога што корисник зна, поседује или што јесте. Минималан захтев за проверу аутентичности су корисничко име и лозинка.

Лозинка мора да задовољи одређени ниво сложености (употреба малих и великих слова, бројева и специјалних карактера и минимална дужина осам карактера).

Блокирати налог за приступ РАМКО након три неуспешна покушаја пријављивања. Функционалност налога обезбедити искључиво интервенцијом администратора корисника РАМКО.

Трајање лозинке мора бити ограничено, и то на највише 60 дана. Забранити употребу већ коришћених лозинки, као и записивање лозинке и саопштавање лозинке другим лицима.

За сваки ресурс РАМКО мора бити дефинисано ко сме да му приступи и са којим нивоом привилегија (читање, упис и модификација).

9. Стратегија за опоравак од нежељених догађаја

Ова стратегија је намењена да низом унапред планираних и примењивих активности одржава РАМКО у функционалном стању и да у случају нежељеног догађаја применом унапред дефинисаних процедура у што краћем року доведе РАМКО у функционално стање.

Ова стратегија састоји се од више планова за опоравак од нежељених догађаја хардверских и софтверских компонената РАМКО.

У систему РАМКО треба израдити планове за опоравак од нежељених догађаја за:

А) Крајње корисничке радне станице у РАМКО. При изради плана опоравка од нежељених догађаја за крајње корисничке радне станице треба обухватити следеће:

1) место одлагања резервне копије података, копије конфигурационих фајлова, апликација и информационих система;

2) софтвер који треба инсталирати на радну станицу;

3) потребне драјвере за радну станицу;

4) упутства за рад на рачунару и информационим системима;

5) списак фолдера које треба копирати;

6) поступак у случају отказа софтвера или хардвера;

7) избор рачунара у организационој јединици који треба реконфигурисати и прилагодити за РАМКО док се не оспособи рачунар намењен за РАМКО;

8) место чувања плана за опоравак од нежељеног догађаја и поступак и лице које рукује планом.

Б) Сервер у РАМКО. При изради плана опоравка од нежељених догађаја за сервере РАМКО треба обухватити следеће:

1) проценити најкритичније апликације, податке, конфигурационе фајлове и системски софтвер за које треба направити резервне копије;

2) место чувања копије;

3) податак о новој локацији на којој ће се задејствовати рад РАМКО сервера у случају немогућности рада на основној локацији;

4) могућност примене и примена *RAID* технологије;

5) податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја;

6) изворе непрекидног напајања електричном енергијом;

7) избор рачунара који ће привремено заменити сервер док се сервер не стави у функцију.

В) РАМКО сервисе, апликације и базе података. При изради плана опоравка од нежељених догађаја за РАМКО сервисе и апликације треба обухватити следеће:

1) постојање документације за сервисе, апликације и базе података;

2) процедуре инсталације и конфигурисања сервиса, апликација и база података;

3) место чувања инсталација сервиса, апликација и база података и резервне копије података;

4) податке о тиму који ће бити ангажован на отклањању последица нежељених догађаја.

Г) Мрежну инфраструктуру РАМКО. При изради плана опоравка од нежељених догађаја за РАМКО мрежну инфраструктуру треба обухватити следеће:

1) документацију за *LAN* и *WAN* (логички и физички дијаграм и копије пројеката);

2) конфигурацију активне мрежне опреме;

3) заштитне копије конфигурационих фајлова и оперативног система активних мрежних уређаја;

4) место чувања документације и резервних копија;

5) постојање резервне мрежне опреме;

6) физичке и логичке линкове за нову локацију (у случају дислокације уређаја због непредвиђеног догађаја);

7) резервне линкове (ако откажу главни линкови);

8) унапред направљене конфигурације за различита сценарија.

У свим организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије које користе РАМКО направити план за опоравак од нежељених догађаја.

Одредити одговорно лице које ће направити план за опоравак од нежељених догађаја и које ће њиме управљати.

План за опоравак од нежељених догађаја најмање једном у шест месеци проверити и ажурирати.

10. Документација

Документација о РАМКО се води у свим организационим јединицама Министарства одбране, организационим јединицама Генералштаба Војске Србије и командама, јединицама и установама Војске Србије које су у рачунарској мрежи РАМКО, у складу са надлежностима.

Организационе јединице Министарства одбране, организационе јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије које користе РАМКО морају да имају следећу документацију:

1) евиденцију резервних копија која треба да садржи: назив организационе јединице, број или ознаку медија, садржај који се налази на медију, датум када је направљена резервна копија, локацију на којој се чува резервна копија, име, презиме и потпис лица које је направило резервну копију;

2) месечни план прављења резервних копија који треба да садржи: назив садржаја за који ће се правити резервна копија и датуме у месецу када ће се правити резервне копије;

3) план мера безбедности и заштите који треба написати са конкретним безбедносним процедурама на основу овог упутства;

4) евиденцију корисничких налога за приступ радној станици, сервису, апликацији, уређају за пренос података, која треба да садржи: име налога, корисничку групу, датум отварања налога, датум суспензије и датум брисања налога;

5) евиденцију имплементираних функционалних и безбедносних побољшања која треба да садржи: назив софтверског ресурса, датум тестирања, датум примене, извор, рачунар на којем је имплементирано побољшање и запажање;

6) евиденцију дељених ресурса на мрежи, која треба да садржи: назив ресурса, где се налазе, ко може да им приступа и са којим привилегијама;

7) евиденцију безбедносних инцидената.

11. Потенцијална места рањивости у РАМКО

А) Потенцијална места рањивости у *WAN* и *LAN* корисника

Редни број	Рањивост	Место најчешће рањивости у *WAN* и *LAN* корисника
1	2	3
1	У инфраструктурним конекцијама и конекцијама корисника	У недокументованим конекцијама, алтернативним наменским и резервним конекцијама за које се не зна сврха. У начину конфигурисања портова на рутеру организације.
2	У мрежној адресној шеми	У погрешном конфигурисању *IP* адреса.
3	У комуникационим уређајима (опште поставке)	У невођењу прегледа *MAC* адреса, мрежним уређајима који нису на безбедним локацијама, управљању лозинкама за мрежне уређаје, управљању мрежним уређајима (резервне копије оперативног система, безбедносна правила, удаљени приступ уређају, управљање портовима) и непостојању упозорења.
4	У рутерима	У управљању аутентикацијом, налозима за рутер и њиховим привилегијама, кључевима за интегритет (*MD5*) и лозинкама. У управљању рутером (удаљеним и локалним приступом) и командама у глобалном конфигурационом моду рутера.
5	У листама за контролу приступа	У погрешно примењеним листама за долазни и одлазни саобраћај, грешкама у приступној листи, пропустима у филтрирању саобраћаја рутера, одржавању, чувању и управљању листама.
6	У заштитним зидовима	У врсти, правилима и филтерима заштитног зида, месту у мрежној топологији, идентификацији и аутентикацији, локалној заштити, конфигурацији, праћењу и администрацији.
7	У систему за идентификовање напада на мрежу	У конфигурацији (мод рада, идентификација корисника, процедура заштитних копија, лог записи и антивирусна заштита).
8	У свичевима и интелигентним хабовима	У конфигурисању налога, лозинки, привилегија и *VLAN* (приступни портови, *tranking*).
9	У удаљеном приступу	У нивоима удаљеног приступа, безбедносним решењима, безбедносним политикама, уговорима са удаљеним корисницима, аутентикацији и ауторизацији (конфигурацији аутентикационог сервера), модемској комуникацији (локација модема, конфигурација *RAS/NAS* сервера) и конфигурацији *VPN*.
10	У управљању мрежом и подршка сервисима	У безбедности конекције између радне станице за управљање и надгледаних уређаја, конфигурацији надгледаних уређаја (различити кориснички налози и лозинке за различита права приступа, подешавању безбедносних аларма), конфигурацији радне станице за управљање, конфигурацији виртуелних приватних мрежа.

Б) Потенцијална места рањивости у сервисима и апликацијама

Редни број	Рањивост	Места најчешће рањивости у сервисима и апликацијама
1	2	3
У *Web* сервисима		
1	У оперативном систему под којим ради *Web* сервер	У избору оперативног система. У закрпама и надградњи оперативног система. У извршавању непотребних сервиса и апликација. У конфигурацији аутентикационог механизама. У тестирању безбедности.
2	У инсталацији и конфигурисању *Web* сервера	У подешавању безбедносних параметара *Web* сервера. У конфигурацији контрола приступа *Web* сервера и оперативног система. У конфигурисању безбедности директоријума *Web* садржаја. У погрешној употреби или непримењености система за проверу интегритета.
3	У *Web* садржају	У расположивости информација на или преко *Web* сервера. У начину објављивања информација на *Web* серверу. У обезбеђивању приватности *Web* корисника (cookies). У присутности активног *Web* садржаја на страни сервера, тј. апликација која се извршава на серверу.
4	У аутентикационим и криптографским технологијама	У избору и конфигурисању аутентикационог механизма. У конфигурисању и имплементацији SSL/TLS. У размени криптографских информација. У избору криптографског алгоритма.
5	У мрежној инфраструктури	У избору локације *Web* сервера у мрежном окружењу. У избору демилитаризоване зоне. У конфигурацији рутера и заштитног зида. У конфигурисању апликације за надгледање система.
6	У администрацији *Web* сервера	У управљању дневничким записима. У процедурама и стратегији прављења заштитних копија. У процедурама за опоравак од компромитовања. У безбедносном тестирању сервера. У удаљеном администрирању сервера.
У апликацијама		
7	У клијентској страни	У пропустима у *Web* претраживачу. У безбедносним подешавањима *Web* претраживача. У присуству активног садржаја на страни клијента. У присуству злонамерних програма.

1	2	3
8	У безбедносним протоколима	У избору безбедносног механизма за очување поверљивости и аутентичности.
9	У пословној логици апликације	У грешкама у функционисању софтвера произвођача. У ретком објављивању закрпа од стране произвођача. У немогућности конфигурисања софтвера према безбедносној политици купца. У грешкама у дизајну и имплементацији. У лошој употреби серверских скриптова. У интерфејсу према *back-end* сервисима.
10	У апликацији	У дизајнерској и програмској логици. У аутентикационом механизму. У преузимању кода.
11	У бази података	У интерфејсу за приступ бази података. У аутентикацији и ауторизацији. У приступу апликационог сервера бази података. У начину смештања података у базу (нешифровани подаци). У избору криптографског алгоритма. У програмерским решењима. У подешавању безбедности базе података.
12	У оперативном систему	У конфигурисању и управљању безбедношћу. У управљању закрпама и ажурирању. У управљању налозима и лозинкама. У праћењу логова и надгледању система од упада. У избору и ажурирању антивирусног софтвера.
У животном циклусу развоја софтвера		
13	У архитектури	У сложеним модулима и лоше дефинисаним интерфејсима. У неизолованости модула (грешка једног модула преноси се на други модул). У примени или изградњи једног безбедносног и заштитног механизма. У комплексности решења.
14	У дизајну	У сложеном коду који треба да обезбеди осетљиве ресурсе. У коришћењу више привилегија него што је потребно. У примени стандардних подешавања. У неограниченој употреби ресурса. У претераном поверењу у клијента. У избору и коришћењу криптографских алгоритама, протокола и производа.

1	2	3
15	У програмирању	У програмском коду коју врши проверу улазних података или непостојању таквог кода за неке улазне податке. У могућности прекидања кода у току извршавања. У начину извршавања кода (промена варијабли у извршењу када се покрену две инстанце у исто време). У управљању грешкама и изузецима. У поступку услед појаве грешке која није разматрана. У начину заштите лозинки и поверљивих информација. У програмирању кода за рад са фајловима. У поступању са привременим фајловима. У позивању процедура и функција.
16	У имплементацији	У неодговорности лица које пише код. У исправљању безбедносне грешке, а не тестирајући код на друге сличне грешке. У коришћењу других алата који нису специфични за програмски језик који се користи. У лаком прелажењу преко упозорења компајлера и интерпретера. У писању замршеног кода. У писању кода независно од безбедносних захтева.
17	У тестирању	У тестирању функционалности, а не и безбедности. У провери безбедности посредног софтвера између апликације и базе. У тестирању рањивости архитектуре и имплементације. У тестирању конфигурације. У ауторизационим и аутентикационим механизмима. У тестирању раније коришћеног кода у другим условима.
18	У окружењу у којем се развија софтвер	У непознавању слабости програмског језика и оперативног система у којем се развија софтвер.

В) Потенцијална места рањивости у избору особља за рад на РАМКО

Редни број	Рањивост	Место најчешће рањивости при избору особља за рад на РАМКО
1	2	3
1	У дефинисању безбедности у оквиру пословних задатака	У генералној одговорности према безбедносним политикама, као и у појединачној одговорности. У избору запослених за радно место и безбедносним политикама које се тада примењују. У избору особља за поверљива радна места. У уговорним обавезама које дефинишу одговорност запосленог према поверљивим информацијама и безбедности и заштити РАМКО за време рада и након престанка рада.

1	2	3
2	У оспособљености запослених	У обучавању запослених из домена информационе безбедности и упознавању безбедносних политика и процедура.
3	У одговорности према насталим безбедносним инцидентима и неправилностима у раду	У процедурама за извештавање о насталим инцидентима као и поступку извештавања. У процедурама, корисничком упутству или извештају о безбедносним слабостима или претњама у систему или сервисима. У процедурама за извештавање о неправилностима рада софтвера. У надгледању и праћењу као и предвиђању нових појава и појава старих слабости, инцидената и неправилности. У дисциплинском поступку према запосленима који нарушавају безбедносне политике и процедуре.

Г) Потенцијална места рањивости у заштитном зиду и *VPN* конекцијама

Редни број	Рањивост	Место најчешће рањивости у заштитном зиду и *VPN* конекцијама
1	2	3
1	У избору заштитног зида и мрежне адресне шеме	У избору врсте заштитног зида и сервиса који се користе. У избору и подешавању мрежне технологије за скривање мрежне адресне шеме.
2	У окружењу заштитног зида	У комплексном дизајну и сложеним функцијама. У избору неадекватних уређаја (уређаја који по својој намени нису заштитни зидови, као рутери и свичеви). У једнолинијској одбрани. У дизајну и конфигурисању демилитаризоване зоне. У избору места сервера у овом окружењу.
3	У безбедносним политикама заштитног зида	У избору безбедносних политика заштитног зида. У имплементацији безбедносних правила. У тестирању и периодичном прегледу безбедносних политика. У избору места имплементације заштитног зида (посебан уређај или у оквиру оперативног система). У одржавању и управљању. У физичкој заштити.
4	У администрацији заштитног зида	У контроли приступа заштитном зиду. У оперативном систему као платформи на којој се извршава заштитни зид. У стратегији отпорности према отказу. У управљању дневничким записима. У поступцима и процедурама у случају безбедносних инцидената. *У Backup* стратегији.
5	У виртуелним приватним мрежама	У избору и подешавању *VPN*. У безбедним мрежним технологијама које се користе за заштиту *VPN*. У аутентикацији. У конфигурисању *VPN* заштићеног саобраћаја.

Д) Потенцијална места рањивости у контролама приступа и криптографским контролама

Редни број	Рањивост	Место најчешће рањивости у контролама приступа и криптографским контролама
1	2	3
У контроли приступа		
1	У контроли приступа	У дефинисању и документовању безбедносних политика. У правилима и правима која садрже безбедносне политике.
2	У корисничкој контроли приступа	У поступку регистрације корисника и доделама привилегија. У управљању привилегијама и корисничким лозинкама. У контроли корисничких права. У одговорности корисника према лозинки и поступцима који нису аутоматизовани, а треба да их спроведе.
3	У контроли приступа мрежи	У безбедносним политикама које се тичу мреже и мрежних сервиса. У аутентикационим механизмима за спољашње конекције. У аутентикацији удаљених појединачних или група рачунара. У периметарској заштити између раздвојених мрежа. У мрежним протоколима који комуницирају ван граница мреже. У безбедности мрежних сервиса.
4	У контроли приступа радној станици	У аутентикацији и ауторизацији корисника. У управљању корисничком лозинком. У системским услужним програмима. У раду са конектованом радном станицом.
5	У контроли приступа апликацији	У безбедносним политикама за контролу приступа апликацији. У управљању корисничким лозинкама.
У криптографској контроли		
6	У криптографској контроли	У безбедносним политикама које користе криптографске методе. У избору осетљивих података и криптографских техника. У некоришћењу дигиталног потписа за безбедност и заштиту аутентичности и интегритета електронских докумената. У некоришћењу сервиса за непорицање. У управљању кључевима.

12. Људски извори претњи, мотивације и врсте напада на електронско пословање

Редни број	Извор претњи	Мотивација	Врста напада
1	2	3	4
1	Легитимни корисник	Прикривање грешака Прикривање незнања Оправдање кашњења Новчана добит	Саботажа софтвера и хардвера Превара и крађа Фалсификовање улазних података Оштећење података Убацивање малициозног кода
2	Спољашња лица	Прикривање немотивисаности за рад Шпијунажа Одмазда и освета Незаконит приступ информацијама	Саботажа софтвера и хардвера Крађа Оштећење података Неауторизовани приступ
3	Инсајдери (слабо обучено, немарно, незадовољно, злонамерно или непоштено особље)	Радозналост Егоизам Новчана добит Освета Ненамерне грешке или пропусти	Напади на особље Уцене и подмићивање Злоупотреба рачунара Крађе и преваре Фалсификовање улазних података Оштећење података Убацивање малициозног кода Упади у систем и саботажа Системске грешке Неауторизовани приступ
4	Непријатељска лица	Изазов за доказивањем Егоизам Побуна	Хакерисање Социјални инжињеринг Упад у систем Неауторизовани приступ
5	Стране обавештајне службе	Подизање тензија Оштећивање система Прибављање потребних информација	Подмићивање Социјални инжињеринг Неауторизовани приступ Упад у систем Прислушкивање
6	Криминалне организације	Остваривање новчане добити	Крађа хардверске и софтверске инфраструктуре Крађа података Оштећење система
7	Терористичке организације	Уцена Уништење Искоришћавање Освета	Информациони рат Напад бојевим средствима Напад на систем (*DDoS*) Пробој у систем
8	Процес дизајна система	Испољавање важности и значаја Уцењивање Остваривање новчане добити	*Trap door* Искоришћавање некомплетне могућности праћења Намерно остављени пропусти за заобилажење безбедности Убацивање малициозног кода

Прилог 14

ОДОБРАВА:

_____
(надлежно лице корисника РАМКО)

Мере безбедности и заштите РАМКО

_____
(организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије)

Редни број	Рањивост	Извор претње	Мера безбедности и заштите
1	2	3	4

ИЗРАДИО:

_____
(администратор корисника РАМКО)

Прилог 15

Евиденција безбедносних инцидената у РАМКО

Редни број	Организациона јединица Министарства одбране, организациона јединица Генералштаба Војске Србије и команда, јединица и установа Војске Србије	Време и датум	Опис и последице	Предузете мере	Лице или лица која су извештена о безбедносном инциденту и време извештавања
1	2	3	4	5	6

Напомена:

1. У колону 1 уноси се редни број.
2. У колону 2 уноси се податак о организационој јединици Министарства одбране, организационој јединици Генералштаба Војске Србије и команди, јединици и установи Војске Србије у којој се догодио безбедносни инцидент.
3. У колону 3 уносе се време и датум када се догодио безбедносни инцидент.
4. У колону 4 уносе се опис и подаци о последицама безбедносног инцидента (шта се тачно догодило, на конкретном рачунару, подаци о лицима која су у вези са инцидентом, да ли има отицања тајних података и сл.).
5. У колону 5 уносе се подаци о мерама које су предузете на отклањању безбедносног инцидента.
6. У колону 6 уносе се подаци о лицима која су извештена о безбедносном инциденту и време извештавања.

С А Д Р Ж А Ј

Страна

МИНИСТАРСТВО ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ
Уредништво „Службеног војног листа“, 11000 Београд, Бирчанинова 5
Одговорни уредник Славица Јерковић, дипл. правник
Главни уредник Нада Сибинчић, проф.
Телефон: 011/3201-979 (23-979) и телефон/факс: 011/3000-200
Штампа: Војна штампарија „Београд“, Београд, Ресавска 40б
ISSN 1821-4088