



# СЛУЖБЕНИ ВОЈНИ ЛИСТ

БРОЈ 32

Београд, 27. новембар 2024.

ГОДИНА СХЛІІІ

Цена овог броја је 354 динара  
Годишња претплата је 17.692 динара

72.

На основу члана 14. став 2, тач. 24) и 25) и став 3. Закона о одбрани („Службени гласник РС”, бр. 116/07, 88/09, 88/09 – др. закон, 104/09 – др. закон, 10/15 и 36/18), министар одбране доноси

## УПУТСТВО О КОРИШЋЕЊУ РАЧУНАРСКЕ МРЕЖЕ ВОЈСКЕ СРБИЈЕ ВОЈНЕТ

### І. УВОДНЕ ОДРЕДБЕ

1. Овим упутством прописује се начин коришћења, планирање, организација, мере безбедности и заштите у раду са Рачунарском мрежом Војске Србије.

2. Рачунарска мрежа Војске Србије је техничко-технолошка целина која обухвата и обједињује најшири скуп рачунарских мрежа које се успостављају за потребе Министарства одбране и Војске Србије на јединственој заједничкој платформи. Скраћени назив ове мреже је ВОЈНЕТ.

3. Намена ВОЈНЕТ је истовремени рад већег броја подмрежа, односно пренос података и информација различите намене у мрежном окружењу, у реалном времену, коришћењем различитих физичких телекомуникационо-информатичких (у даљем тексту: ТкИ) платформи великих капацитета.

4. Циљ успостављања и увођења у употребу ВОЈНЕТ јесте да се омогући ефикаснија и економичнија експлоатација доступних ТкИ ресурса из домена рачунарских мрежа.

5. Овим упутством дефинисани су елементи организације ВОЈНЕТ и прописана правила у планирању, развоју, експлоатацији, одржавању и безбедности ВОЈНЕТ у целини, као и њених саставних делова.

6. По одредбама овог упутства поступају унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије.

### 1. Општи појмови

7. Поједини појмови који се користе у овом упутству имају следеће значење:

- 1) трослојни мрежни модел подразумева модел реализације рачунарских мрежа успоставом слоја окоснице (енгл. *core*), дистрибутивног слоја (енгл. *distribution*) и приступног слоја (енгл. *access*);
- 2) окосница рачунарске мреже је транспортни део мреже чија је основна намена брз и ефикасан пренос података између удаљених локација, са минималном обрадом података;
- 3) дистрибутивни слој рачунарске мреже је намењен да обједини (агрегира) податке са приступног слоја мреже пре слања ка окосници мреже и представља границу између приступног слоја и окоснице. Дистрибутивни слој може садржати елементе приступног слоја;
- 4) приступни слој рачунарске мреже је део мреже на који се директно повезују корисници мреже, било да је у питању појединачни корисник, група радних станица или локална рачунарска мрежа корисника (енгл. *LAN – Local Area Network*);
- 5) подмреже су логички независне целине исте или различите технолошке организације намењене да пруже опште или специфичне мрежне сервисе корисницима;
- 6) центар за обраду података (у даљем тексту: ДАТА центар) је место где постоје инфраструктурни и телекомуникациони услови за постављање и рад рачунарско-серверских система, система за складиштење података и телекомуникационо-информатичке опреме;
- 7) демаркациона тачка је место раздвајања између две подмреже или две равни, односно тачка у којој престаје надлежност једног и почиње надлежност другог техничког носиоца;

- 8) чвор је елемент који представља инфраструктурно обједињавање хардверске и софтверске компоненте на одређеној локацији (стационарни телекомуникационо-информатички центар – у даљем тексту: СТКИЦ; стационарно телекомуникационо-информатичко чвориште – у даљем тексту: СТКИЧ; телекомуникационо-информатички центар – у даљем тексту: ТКИЦ и ДАТА центар);
- 9) сервис је врста програма, апликације или неке друге функционалности система која је омогућена у циљу подршке корисничких пословних процеса;
- 10) надзор и управљање је процес сталног праћења параметара битних за стабилно и непрекидно функционисање система, рачунарских мрежа и сервиса, уз примену поступака за унапређење и прилагођавање корисничким потребама, као и реаговања на настале проблеме;
- 11) администрирање рачунарске мреже је управљање ресурсима рачунарске мреже, односно компонентама од којих се мрежа састоји.

## 2. Основни појмови ВОЈНЕТ

8. ВОЈНЕТ је саставни део телекомуникационо-информационог система Војске Србије (у даљем тексту: ТКИС ВС). Реализована је према трослојном мрежном моделу, са наменом преноса података великим брзинама и способношћу подршке рада већег броја подмрежа.

9. Окосница ВОЈНЕТ представља техничко-технолошку целину која својом структуром и елементима обезбеђује темељну основу за развој и функционисање већег броја независних подмрежа.

10. Дистрибутивна и приступна раван ВОЈНЕТ представљају техничко-технолошке целине, организоване као саставни део логичких подмрежа дефинисаних унутар ВОЈНЕТ, које се успостављају према намени и техничким потребама подмрежа ВОЈНЕТ, а у складу са планским документима Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије (у даљем тексту: УТИ (Ј-6) ГШ ВС) и/или других корисника у оквиру Министарства одбране и Војске Србије надлежних за планирање.

11. Подмреже ВОЈНЕТ представљају техничко-технолошку целину ВОЈНЕТ, које користе засебне хардверске, физички одвојене ТКИ капацитете у дистрибутивној и приступној равни ВОЈНЕТ, док за окосницу користе дељене физичке ТКИ капацитете окоснице ВОЈНЕТ. Намењене су за ефикасно руковођење и командовање, имплементацију и експлоатацију сервиса, апликација и информациононих система у Министарству одбране и Војсци Србије.

12. Подмреже ВОЈНЕТ класификују се у односу на примењене модалитете криптозаштите мрежне инфраструктуре и у односу на намену.

13. У односу на примењене модалитете криптозаштите мрежне инфраструктуре, у скупу подмрежа ВОЈНЕТ постоје заштићене мреже и универзалне мреже.

14. Заштићене мреже су подмреже ВОЈНЕТ у којима је за потребе криптозаштите информација примењено хардверско и/или софтверско решење развијено и имплементирано од стране установе надлежне за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије.

15. Универзалне мреже су подмреже ВОЈНЕТ у којима је примењено неко од комерцијалних решења за криптозаштиту информација уз одобрење установе надлежне за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије и сагласност УТИ (Ј-6) ГШ ВС, или подмреже у којима није примењено техничко решење за криптозаштиту информација (КЗИ) – отворене мреже.

16. У односу на намену, у скупу подмрежа ВОЈНЕТ постоје мреже опште намене и мреже посебне намене.

17. Мреже опште намене су подмреже ВОЈНЕТ које представљају јединствену физичку и логичку платформу формирану за потребе већег броја организационих целина и на којој су активни сервис и апликације најмање два различита тактичка носиоца.

18. Мреже посебне намене су подмреже ВОЈНЕТ које су формиране на захтев и за потребе једне унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије и на којој су активни искључиво сервис и апликације те организационе целине.

19. Елементи ВОЈНЕТ су: чворови, хардверске компоненте, софтверске компоненте, линкови и помоћна средства.

20. Хардверске компоненте ВОЈНЕТ чине пасивна мрежна опрема (бакарни и оптички каблови, конектори и др.), активна мрежна опрема (рутери, сичеви и др.), серверска инфраструктура, радне станице за управљање и надзор, кориснички рачунари, као и остала ТКИ опрема намењена за функционисање ВОЈНЕТ.

21. Софтверске компоненте ВОЈНЕТ чине системски, апликативни и сервисни софтвер, датотеке, конфигурационе скрипте и остали софтвер неопходан за рад и управљање хардверским компонентама ВОЈНЕТ.

22. Линкови ВОЈНЕТ су телекомуникациони капацитети остварени преко ТКИС, а намењени за повезивање најмање два чвора мреже.

23. Помоћна средства су техничка и друга средства намењена за рад и функционисање ВОЈНЕТ која се не могу сврстати у хардверске и софтверске компоненте.

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

25. Апликативни софтвер обухвата: општи апликативни софтвер (текст-процесори, табеларни алати, графички алати и сл.) и наменски апликативни софтвер (пословни информациони системи, командно-информациони системи, географски информациони системи, апликације и сл.).

26. Сервиси у ВОЈНЕТ и подмрежама ВОЈНЕТ могу бити: системски сервиси, сервиси командовања и сервиси подршке.

27. Системски сервиси су сервиси који обезбеђују основне функционалности ВОЈНЕТ и сваке подмреже понаособ, као и рад сервиса командовања, сервиса подршке и наменског апликативног софтвера.

28. Безбедносни сервиси су системски сервиси којима се услед великог значаја у ВОЈНЕТ посвећује посебна пажња и чија је примена регулисана важећим упутствима и правилима о криптозаштити, инструкцијама о примени мера безбедности у рачунарским мрежама, и инструкцијама за спречавање отицања тајних података у рачунарским мрежама.

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

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

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

## II. ЕЛЕМЕНТИ ОРГАНИЗАЦИЈЕ ВОЈНЕТ

### 1. Тактички и технички носиоци ВОЈНЕТ

32. Функционисање ВОЈНЕТ регулишу следећа документа: Доктрина телекомуникационо-информатичког обезбеђења, Главни пројекат рачунарске мреже Војске Србије, План телекомуникационо-информатичког обезбеђења, Наређење за телекомуникационо-информатичко обезбеђење у делу који се односи на надлежности у функционисању телекомуникационо-информационог система, Правилник о одређивању тактичких и техничких носилаца наоружања и војне опреме и осталих средстава у Министарству одбране и Војсци Србије, ово упутство, као и остала акта од значаја за функционисање ВОЈНЕТ у целини или подмрежама.

33. Надлежности тактичких и техничких носилаца прописују се посебно за окосницу ВОЈНЕТ, а посебно за подмреже у односу на класификацију подмрежа према намени, што има за циљ да обезбеди синхронизован и усклађен рад, ефикасност управљања мрежом, ефикасност експлоатације мрежних ресурса, ефикасну дистрибуцију сервиса, као и обезбеђење захтеваног нивоа безбедности и заштите информација на свим слојевима мрежне структуре ВОЈНЕТ.

34. Тактички носилац је унутрашња јединица Министарства одбране и Војске Србије овлашћена и надлежна за покретање развоја и набавку система и средстава, њихово усавршавање, усвајање у наоружање и војну опрему (у даљем тексту: НВО), опремање, расподелу и одређивање употребе.

35. Технички носилац је унутрашња јединица Министарства одбране и Војске Србије која прописује и организује експлоатацију, одржавање и ремонт средстава, учествује у процесу опремања Војске Србије кроз истраживање, развој, производњу и ремонт. Технички носилац дефинише елементе интегралне логистичке подршке и прати поступке њихове уградње током процеса опремања средствима НВО, у складу са одговарајућим стандардом одбране Републике Србије.

36. Осим тактичког и техничког носиоца у мрежи ВОЈНЕТ и њеним подмрежама одређују се: администратор мреже (подмреже), администратор заштите мреже (подмреже), тактички и технички носилац сервиса, администратор сервиса, носилац послова развоја и унапређења, носилац послова развоја и унапређења криптозаштите података и носилац превенције безбедносних ризика.

37. Могуће је одредити једног тактичког или техничког носиоца или носиоца послова за више мрежа истовремено.

38. На нивоу целе мреже ВОЈНЕТ одређују се заједнички носиоци следећих послова:

- 1) носилац послова развоја и унапређења ВОЈНЕТ;
- 2) носилац послова развоја и унапређења криптозаштите података ВОЈНЕТ;
- 3) носилац превенције безбедносних ризика ВОЈНЕТ.

#### 1.1. Тактички и технички носилац окоснице ВОЈНЕТ

39. Тактички носилац окоснице ВОЈНЕТ је УТИ (J-6) ГШ ВС која планира и организује рад у окосници ВОЈНЕТ, регулише развој, опремање, унапређење организације рада, безбедност и заштиту у окосници ВОЈНЕТ.

40. Технички носилац окоснице ВОЈНЕТ је Бригада везе која је одговорна за реализацију и имплементацију планова и других докумената прописаних од стране тактичког носиоца, као и за обезбеђење техничког функционисања окоснице ВОЈНЕТ, обезбеђење непрекидности рада хардвера и софтвера у окосници ВОЈНЕТ, надзор и управљање, примену мера безбедности и заштите информација и администрирање окоснице ВОЈНЕТ.

41. Центар за командно-информационе системе и информатичку подршку (у даљем тексту: ЦКИСИП) носилац је развоја и унапређења окоснице ВОЈНЕТ.

42. Јединица надлежна за телекомуникационо-информатичко обезбеђење Ратног ваздухопловства и против-ваздухопловне одбране је носилац ТкИ обезбеђења непрекидности функционисања елемената окоснице ВОЈНЕТ у својој надлежности.

43. Установа надлежна за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије је носилац развоја и унапређења криптозаштите у ВОЈНЕТ.

44. Центар за превенцију безбедносних ризика у рачунарским мрежама Војске Србије (у даљем тексту: ЦЕРТ ВС) је носилац организације и превенције безбедносних ризика у ВОЈНЕТ у складу са Решењем о образовању Посебне радне групе за безбедност информационо-комуникационих система у Министарству одбране.

#### 1.2. Тактички и технички носиоци подмрежа опште намене ВОЈНЕТ

45. На основу својих надлежности, УТИ (Ј-6) ГШ ВС тактички је носилац за подмреже опште намене и одговорна је за планирање и организацију рада, као и за регулисање развоја, опремања и унапређења организације рада, безбедност и заштиту подмрежа опште намене ВОЈНЕТ.

46. Носилац развоја и унапређења подмрежа опште намене ВОЈНЕТ је ЦКИСИП.

47. Бригада везе је технички носилац за подмреже опште намене, закључно са демаркационом тачком.

48. Установа надлежна за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије је носилац развоја и унапређења криптозаштите у подмрежама опште и посебне намене ВОЈНЕТ.

49. Носилац превенције безбедносних ризика у подмрежама опште намене ВОЈНЕТ је ЦЕРТ ВС.

#### 1.3. Тактички и технички носиоци подмрежа посебне намене ВОЈНЕТ

50. Тактички и технички носиоци подмрежа посебне намене ВОЈНЕТ јесу унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и/или команде оперативног нивоа Војске Србије (корисници) које формирају подмреже за своје специфичне намене.

51. Тактички и технички носиоци подмрежа посебне намене ВОЈНЕТ одговорни су за планирање, развој, организацију, регулативу, опремање, безбедност и заштиту, као и за даљи развој и унапређење подмрежа које су формирали за своје специфичне намене.

52. Тактичке и технике носиоце подмрежа посебне намене ВОЈНЕТ одређује УТИ (Ј-6) ГШ ВС у својству тактичког носиоца окоснице ВОЈНЕТ, посебним актом, а на предлог унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и/или команде оперативног нивоа Војске Србије (корисника) који захтева формирање подмреже за своје специфичне намене.

53. Тактички носилац подмреже посебне намене својим актом регулише сва питања од значаја за организацију рада у мрежи и посебно одређује: администратора подмреже и администратора заштите подмреже.

54. Уколико послови развоја и унапређења мрежа посебне намене, послови развоја и унапређења криптозаштите података и послови превенције безбедносних ризика поседују значајне специфичности у односу на окосницу ВОЈНЕТ, тактички носилац подмреже ће их посебно регулисати. Уз прибављање сагласности тактичког носиоца окоснице ВОЈНЕТ све специфичности, као и поступање у вези са њима, тактички носилац подмреже посебне намене ће посебно регулисати.

#### 1.4. Тактички и технички носилац сервиса у ВОЈНЕТ

55. Тактички носилац сервиса је унутрашња јединица Министарства одбране и Војске Србије овлашћена и надлежна за покретање развоја, увођење у употребу, усавршавање, дистрибуцију, коришћење и регулисање употребе сервиса који се имплементира у ВОЈНЕТ.

56. Технички носилац сервиса је унутрашња јединица Министарства одбране и Војске Србије која спроводи експлоатацију и одржавање сервиса имплементираних у ВОЈНЕТ.

57. Тактички носилац системских сервиса у мрежама опште намене је УТИ (Ј-6) ГШ ВС и одговорна је за планирање, организацију, дистрибуцију, коришћење и регулисање њихове употребе.

58. Технички носилац системских сервиса у мрежама опште намене (укључујући и хардверске компоненте за реализацију сервиса) је ЦКИСИП и одговоран је за експлоатацију и одржавање непрекидности системских сервиса.

59. Унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије, команде, јединице и установе Војске Србије, одређују се за тактичке носиоце сервиса из своје функције у мрежама опште намене, исказују потребу и, уз сагласност УТИ (Ј-6) ГШ ВС, уводе у употребу сервис, планирају, организују и регулишу употребу сервиса из своје функције.

60. У мрежама опште намене унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије, команде, јединице и установе Војске Србије су технички носиоци сервиса из своје функције, надлежни за успоставу, одржавање и експлоатацију сервиса.

61. Тактички носилац системског сервиса унутар мрежа посебне намене је унутрашња јединица Министарства одбране, ужа унутрашња јединица Генералштаба Војске Србије, команда, јединица и установа Војске Србије, која је тактички носилац подмреже посебне намене.

62. У мрежама посебне намене унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије, команде, јединице и установе Војске Србије одређују се за тактичке носиоце сервиса из своје функције, исказују потребу и, уз сагласност УТИ (Ј-6) ГШ ВС, уводе у употребу сервис, планирају, организују и регулишу употребу сервиса из своје функције.

63. У мрежама посебне намене унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије, команде, јединице и установе Војске Србије су технички носиоци сервиса из своје функције, надлежни за успоставу, одржавање и експлоатацију сервиса.

64. Праћење нових технологија у циљу подршке развоју и унапређењу сервиса реализује ЦКИСИП. Пружање подршке тактичким и техничким носиоцима сервиса у случају потребе и на захтев носилаца регулише УТИ (Ј-6) ГШ ВС.

#### 1.5. Послови тактичких и техничких носилаца и носилаца послова и сервиса у мрежама и подмрежама ВОЈНЕТ

65. Послови тактичких и техничких носилаца и носилаца послова и сервиса у мрежама и подмрежама ВОЈНЕТ, као и послови администратора на различитим нивоима администрације мрежом и сервисима, овим се упутством усмеравају и начелно уређују. Сваки тактички носилац детаљно успоставља организацију рада укључујући и регулисање поступака, прописивање процедура и успостављање контроле у складу са надлежностима и овлашћењима.

66. На основу надлежности тактичког носиоца окоснице ВОЈНЕТ, УТИ (Ј-6) ГШ ВС одговорна је за доделу капацитета и за регулисање начина и услова коришћења заједничких ресурса у складу са потребама корисника и могућностима окоснице ВОЈНЕТ које су на располагању.

67. Као највиши стручни орган за ВОЈНЕТ, УТИ (Ј-6) ГШ ВС у складу са својом функцијом и надлежностима, кроз документа Плана ТКИОБ и друга документа, регулише следеће:

- 1) пружање системских основа организације рада ВОЈНЕТ и њених саставних делова;
- 2) управљање адресним простором у ВОЈНЕТ;
- 3) одобравање увођења и дефинисање начина успостављања, као и техничке карактеристике подмрежа ВОЈНЕТ;
- 4) одобравање увођења нових сервиса и дефинисање начина имплементације, у складу са надлежностима према нивоу мрежног окружења у коме се сервис успоставља;
- 5) израду стручних упутстава, техничких инструкција и прилога за рад у ВОЈНЕТ;
- 6) планирање, организовање и контролисање примене безбедносних механизма и заштите у ВОЈНЕТ и подмрежама ВОЈНЕТ;
- 7) планирање, организовање и вршење контроле рада у ВОЈНЕТ;
- 8) у складу са насталим потребама предлагање и реализовање измене овог упутства.

68. Бригада везе као технички носилац окоснице ВОЈНЕТ и технички носилац подмрежа опште намене обавља следеће задатке:

- 1) обезбеђује телекомуникационе ресурсе за функционисање ВОЈНЕТ;
- 2) обезбеђује непрекидно функционисање система преноса;
- 3) обезбеђује функционисање ВОЈНЕТ у окосници и дистрибутивној равни;
- 4) врши надоградњу окоснице и дистрибутивне равни ВОЈНЕТ и активира подмреже ВОЈНЕТ у сарадњи са ЦКИСИП и установом која је надлежна за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије;
- 5) врши надзор и управљање окосницом ВОЈНЕТ и подмрежама опште намене ВОЈНЕТ;
- 6) технички имплементира и одржава решења за КзИ на свом нивоу;
- 7) примењује мере безбедности и заштите;
- 8) сарађује по налогу тактичког носиоца окоснице ВОЈНЕТ на изради нових процедура, изради стручних упутстава, техничких инструкција и прилога за рад у ВОЈНЕТ.

69. Као носилац послова развоја и унапређења ВОЈНЕТ, ЦКИСИП обавља следеће задатке:

- 1) испитује употребљивост нових хардверских и софтверских компонента ВОЈНЕТ ради унапређења функционалности ВОЈНЕТ;
- 2) пројектује и по потреби подржава имплементацију специфичних решења подмрежа ВОЈНЕТ;
- 3) учествује у дефинисању параметара и начина имплементације нових подмрежа ВОЈНЕТ;
- 4) пројектује, имплементира, обезбеђује непрекидно функционисање и унапређивање ДАТА центара стратегијског нивоа, на које се ослања ВОЈНЕТ;
- 5) сарађује по налогу тактичког носиоца окоснице ВОЈНЕТ при изради нових процедура, изради стручних упутстава, техничких инструкција и прилога за рад у ВОЈНЕТ.

70. Установа надлежна за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије обавља послове синтезе, анализе, имплементације и верификације шифарских система намењених за криптозаштиту података у оквиру подмрежа ВОЈНЕТ предвиђених за размену тајних података. Сарађује по налогу тактичког носиоца окоснице ВОЈНЕТ на изради нових процедура, изради стручних упутстава, техничких инструкција и прилога за рад у ВОЈНЕТ.

71. ЦЕРТ ВС обавља следеће задатке:

- 1) врши процену претњи и ризика по безбедност ВОЈНЕТ и подмрежа;
- 2) прописује процедуре за поступање у случају безбедносних инцидената;
- 3) прикупља и размеђује информације о могућим ризицима и обавештава, упозорава и саветује одговорна лица за окосницу и подмреже ВОЈНЕТ;
- 4) управља инцидентима;
- 5) предлаже регулативна акта у области информационе безбедности у ВОЈНЕТ;
- 6) врши избор, тестирање и примену техничких, физичких и организационих мера заштите, опреме и програма;
- 7) врши надзор имплементације и примене безбедносних процедура (мера заштите);
- 8) сарађује по налогу тактичког носиоца окоснице ВОЈНЕТ на изради нових процедура, изради стручних упутстава, техничких инструкција и прилога за рад у ВОЈНЕТ;
- 9) извршава друге послове у домену информационе безбедности у ТКИС ВС.

72. Администратор ВОЈНЕТ је стручно лице или тим, одређен одлуком тактичког носиоца, које је одговорно за:

- 1) праћење, контролу и координацију послова и пружање помоћи у раду администратора подмрежа, администратора сервиса и техничких носилаца осталих елемената ВОЈНЕТ;
- 2) сарадњу са ЦЕРТ ВС у процени претњи и ризика по ВОЈНЕТ, предлагање мера безбедности и заштите и налагање примене сигурносних механизма;
- 3) поступање у случају нарушавања функционалности приоритетних подмрежа и сервиса узрокованих неправилним радом подмрежа нижег приоритета, уз могућност привременог блокирања делова окоснице ВОЈНЕТ, сегмената подмрежа, као и целокупне подмреже или појединачног сервиса који узрокује проблем, до тренутка отклањања узрока проблема.

73. Администратор заштите ВОЈНЕТ је стручно лице или тим, одређен одлуком тактичког носиоца које је одговорно за:

- 1) контролу и примену мера безбедности и заштите у ВОЈНЕТ;
- 2) процену претњи и ризика по ВОЈНЕТ;
- 3) сарадњу са ЦЕРТ ВС;
- 4) предлагање мера безбедности и заштите и имплементирање сигурносних механизма;
- 5) поступање у случају нарушавања интегритета, безбедности и заштите окоснице ВОЈНЕТ узрокованих неправилним радом подмрежа нижег приоритета, уз могућност привременог блокирања делова окоснице ВОЈНЕТ, сегмената подмрежа, као и целокупне подмреже или појединачног сервиса који узрокује проблем, до тренутка отклањања узрока проблема;
- 6) у случају нарушавања безбедности ВОЈНЕТ, пријављивање безбедносног инцидента надлежном органу Војнобезбедносне агенције;
- 7) вођење евиденције безбедносних инцидената у ВОЈНЕТ.

74. Администратор подмреже ВОЈНЕТ је стручно лице или тим, одређен одлуком тактичког носиоца подмреже, одговорно за:

- 1) прописивање административне процедуре и инструкције за рад подмреже у оквиру ВОЈНЕТ;
- 2) примену процедура и поступање по инструкцијама које је донео тактички носилац подмреже, администратор ВОЈНЕТ или тактички носилац ВОЈНЕТ у сопственој надлежности, а које се односе на подмрежу;
- 3) планирање хардверско софтверских ресурса за подмрежу;
- 4) инсталирање и обезбеђење функционисања потребног хардвера и софтвера у подмрежи;
- 5) израду и ажурирање Плана ТКИОБ у делу који се односи на подмрежу за коју је надлежан;
- 6) припрему података за израду захтева тактичког носиоца подмреже за активирање/деактивирање приступних тачака подмреже на окосници ВОЈНЕТ и прикључака подмреже;
- 7) координирање активности на подмрежи са Администратором ВОЈНЕТ;
- 8) сарадњу са осталим администраторима и ЦЕРТ ВС приликом процене претњи и ризика по безбедност компонента подмреже у својој подмрежи;
- 9) предлагање мера безбедности и заштите, имплементирање сигурносних механизма и контролу спровођење мера;
- 10) уједно вршење послова администратора једног или више сервиса по одлуци тактичког носиоца сервиса.

75. Администратор заштите подмреже ВОЈНЕТ је стручно лице или тим, одређен од стране УТИ (Ј-6) ГШ ВС, одговорно за:

- 1) контролу примене мера безбедности и заштите у подмрежи ВОЈНЕТ;
- 2) процену претњи и ризика по подмрежу ВОЈНЕТ;
- 3) сарадњу са ЦЕРТ ВС;
- 4) предлагање мера безбедности и заштите и имплементирање сигурносних механизма;
- 5) у случају нарушавања интегритета, безбедности и заштите подмреже ВОЈНЕТ, узрокованих неадекватним радом, може извршити привремено блокирање делова подмреже ВОЈНЕТ, као и целокупне подмреже или појединачног сервиса који узрокује проблем, до тренутка отклањања узрока проблема;
- 6) у случају нарушавања безбедности подмреже ВОЈНЕТ, пријављивање безбедносног инцидента надлежном органу Војнобезбедносне агенције;
- 7) вођење евиденције безбедносних инцидената у подмрежи ВОЈНЕТ.

76. Администратор корисника подмреже ВОЈНЕТ је стручно лице или тим, одређен од стране унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије као корисника локалне рачунарске мреже, одговорно за рад локалне рачунарске мреже у складу са правилима и прописима.

77. Администратор корисника подмреже ВОЈНЕТ има следеће обавезе:

- 1) инсталира и обезбеђује функционисање потребног хардвера у складу са пројектом локалне рачунарске мреже, као и потребног софтвера у локалној рачунарској мрежи, иза демаркационе тачке подмреже;
- 2) врши израду и ажурирање Плана ТкИОб у делу који се односи на локалну рачунарску мрежу за коју је надлежан;
- 3) координира активности, задатке и обавезе у вези са функционисањем локалне рачунарске мреже са администратором подмреже и администратором/администраторима сервиса;
- 4) организује прикључење рачунара крајњих корисника сервиса у локалну рачунарску мрежу ради коришћења одобрених сервиса и апликација;
- 5) организује и изводи обуку крајњих корисника за употребу и оптимално коришћење функционалности локалне рачунарске мреже;
- 6) води евиденцију безбедносних инцидената у локалној рачунарској мрежи за коју је одговоран;
- 7) уједно обавља послове администратора једног или више сервиса у подмрежи ВОЈНЕТ, у складу са одлуком тактичког носиоца сервиса;
- 8) учествује у изради процене претњи и ризика по безбедност компонената локалне рачунарске мреже, предлаже мере безбедности и заштите, имплементира сигурносне механизме и контролише спровођење мера.

78. Администратор сервиса у подмрежи ВОЈНЕТ је стручно лице које је одредио тактички носилац сервиса, одговорно за рад сервиса, усклађен са правилима и прописима.

Администратор сервиса у подмрежи ВОЈНЕТ има следеће задатке:

- 1) одговоран је за обезбеђење непрекидности рада сервиса;
- 2) координира рад са администратором подмреже;
- 3) кроз План ТкИОб реализује, редовно ажурира и доставља измене прилога, додатака и инструкција везаних за рад сервиса;
- 4) одобрава приступ сервису и води евиденцију корисника;
- 5) прати евентуалне проблеме у раду сервиса;
- 6) предлаже тактичком носиоцу сервиса унапређење сервиса.

## 2. Врсте подмрежа ВОЈНЕТ

79. Подмреже ВОЈНЕТ се реализују успостављањем адекватних логичких целина и припадајуће физичке инфраструктуре на дистрибутивној и приступној равни ВОЈНЕТ.

80. Све подмреже ВОЈНЕТ, начелно, успостављају се као логичке подмреже директно ослоњене на окосницу ВОЈНЕТ.

81. Класификацију подмрежа ВОЈНЕТ могуће је извршити у односу на модалитет заштите, у односу на намену, у односу на време трајања и/или у односу на друге особине специфичних карактеристика мреже или сервиса, при чему класификовање подмрежа не сме утицати на наведени принцип реализације физичке топологије мрежне инфраструктуре која подразумева директно ослањање подмрежа на окосницу ВОЈНЕТ.

82. Класификација подмрежа у односу на намену користи се као основ за одређивање надлежности при одређивању тактичких и техничких носилаца.

83. Класификација подмрежа у односу на модалитет заштите користи се као основ за примену политика безбедности у подмрежама, а посебно за одређивање могућности и начина међусобних интерконекција.

84. Класификација подмрежа према времену трајања користи се као основ за издавање сагласности за прикључење на подмрежу од стране надлежног тактичког носиоца.

85. Класификација подмрежа ВОЈНЕТ у односу на модалитет заштите: Заштићене и Универзалне мреже. Универзалне мреже могу бити отворене или мреже са комерцијалном заштитом.

86. У отвореним универзалним мрежама постоји могућност примене технологија за заштиту IP-тунела чиме се остварује заштита појединих удаљених сегмената мреже. На овакав начин може се остварити заштита појединих сервиса или делова мреже чиме универзалне мреже у односу на модалитет заштите могу бити реализоване и као отворене са заштићеним сервисима (примена комерцијалне криптозаштите).

### 2.1. Специфичности заштићених подмрежа

87. Заштићеном подмрежом, у смислу одредаба овог упутства, подразумева се само она мрежна инфраструктура у којој је за потребе криптозаштите информација примењено хардверско и/или софтверско решење развијено и имплементирано од стране установе надлежне за развој, имплементацију и верификацију криптографских производа у Министарству одбране и Војсци Србије.

88. Универзална мрежа са комерцијалном заштитом представља подмрежу ВОЈНЕТ заштићену комерцијалним, јавно доступним методама и средствима којом се не преносе тајни подаци, али се преносе подаци који имају одређен значај и чији садржај не би требало да буде у потпуности доступан.

89. Рачунарска опрема која се користи у једној заштићеној или универзалној подмрежи не може се користити на другој заштићеној или универзалној подмрежи у било којем облику.

90. Није дозвољено изношење рачунарске опреме која је намењена за рад у заштићеним подмрежама ван војних објеката или земљишних просторија размештаја војних јединица у којима се ради с том опремом, осим уз одобрење УТИ (J-6) ГШ ВС, уз поштовање прописаних организационо-техничких и безбедносних правила, механизма и процедура.

91. Забрањен је било који облик контакта или довођења у физички додир, интерконекција и повезивање на било којем слоју мрежне архитектуре, било које заштићене подмреже са универзалним мрежама (подмрежама са комерцијалним типом заштите или подмрежама без заштите).

### 2.2. Специфичности универзалних подмрежа

92. Универзална подмрежа намењена је за пренос отворених података и података без степена тајности. Универзална подмрежа ослања се по овом питању на основни ниво заштите успостављен на физичкој платформи ВОЈНЕТ.

93. Повезивање универзалне подмреже са комерцијалним системом заштите или отворене универзалне подмреже са рачунарским мрежама других ималаца, односно са мрежама других државних органа, организација, служби и јавним мрежама, није дозвољено.

Интерконекција из става 1. ове тачке могућа је искључиво уз обострано одобрење УТИ (J-6) ГШ ВС и Војно-безбедносне агенције уз поштовање организационо-техничких и безбедносних правила, механизма и процедура које ће дефинисати ове две целине, у оквирима своје надлежности, уз неопходан пристанак односно сагласност друге стране за интерконекцију.

94. Мреже других ималаца, других државних органа, организација и служби, у смислу заштите информација, потребно је посматрати као јавно доступне мреже и према њима се тако и односити у безбедносном смислу.

## 3. Типови подмрежа ВОЈНЕТ и прикључака на окосницу према времену трајања

95. По времену трајања подмреже ВОЈНЕТ могу бити:

- 1) сталне (у функцији су непрекидно, а реализују се у складу са плановима развоја мреже и по захтеву унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије);
- 2) привремене (успостављају се по потреби и на одређено време, а реализују се по захтеву унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије).

96. Прикључак подмреже на окосницу ВОЈНЕТ служи да се подмрежа ВОЈНЕТ, односно локације мрежа тактичког носиоца повежу кроз окосницу ВОЈНЕТ.

97. По времену трајања прикључци подмреже на окосницу ВОЈНЕТ могу бити:

- 1) стални (у функцији су непрекидно, а реализују се у складу са захтевом унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије и одобрењем УТИ (J-6) ГШ ВС;
- 2) привремени (успостављају се по потреби и на одређено време, а реализују се у складу са захтевом унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије или команде, јединице и установе Војске Србије и одобрењем УТИ (J-6) ГШ ВС).



#### 4. Приоритети

98. Телекомуникационо-информациони ресурси ВОЈНЕТ су ограничени и према њима се треба односити одговорно и рационално приликом доделе појединачним подмрежама и сервисима.

99. Доделу ТкИ ресурса подмрежи или сервису могуће је извршити варијабилним аутоматским софтверским методама или доделом фиксних ресурса.

100. Приликом расподеле ТкИ ресурса приоритет имају мреже намењене командовању и сервисима командовања и мреже намењене за реализацију безбедносне и контраобавештајне заштите Министарства одбране и Војске Србије, у складу са законом.

### III. ЕКСПЛОАТАЦИЈА ВОЈНЕТ

#### 1. Поступак за увођење нових подмрежа ВОЈНЕТ

101. Предлог за увођење нове подмреже ВОЈНЕТ могу поднети унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије преко надлежног тактичког носиоца за област на коју би се тражена подмрежа односила.

102. Унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије достављају надлежном тактичком носиоцу окоснице ВОЈНЕТ захтев за увођење нове подмреже ВОЈНЕТ из своје надлежности, а у циљу повећања функционалних способности Министарства одбране и оперативних и функционалних способности Војске Србије.

103. Захтев за увођење подмреже ВОЈНЕТ садржи следеће информације:

- 1) предвиђену специфичну намену подмреже;
- 2) образложење специфичне намене подмреже;
- 3) дефинисан тип подмреже;
- 4) дефинисане сервисе које мрежа обезбеђује;
- 5) специфичне техничке захтеве;
- 6) организационе целине које би биле корисници подмреже;
- 7) чворове (СТКИЦ/СТКИЧ/ТКИЦ) ка којима се агрегирају локални корисници, број корисника по чвору;
- 8) локације хардверско софтверских елемената кључних за сервисе у подмрежи мрежи, локације корисника и капацитет потребан за повезивање ових елемената;
- 9) расположиве хардверске и софтверске ресурсе за ову намену;
- 10) расположиве људске ресурсе за управљање подмрежом.

104. УТИ (Ј-6) ГШ ВС, у сарадњи са тактичким носиоцем/предлагачем и техничким носиоцем, разматра захтев из тачке 103. овог упутства ради процене оправданости увођења нове подмреже, могућности коришћења неке од већ постојећих подмрежа, процене потребних хардверских, софтверских и ТкИ ресурса у ВОЈНЕТ, након чега се врши верификација нове подмреже или одбијање захтева.

105. Верификација нове подмреже ВОЈНЕТ и одобравање њеног увођења у употребу у надлежности је УТИ (Ј-6) ГШ ВС. УТИ (Ј-6) ГШ ВС врши планирање у окосници ВОЈНЕТ ради обезбеђења услова за прикључење нове подмреже ВОЈНЕТ. УТИ (Ј-6) ГШ ВС тактичком носиоцу подмреже доставља одобрење за успоставу подмреже ВОЈНЕТ, а техничком носиоцу окоснице ВОЈНЕТ доставља одобрење за формирање нове подмреже и прикључење на ВОЈНЕТ са планом успоставе подмреже ВОЈНЕТ на даљу реализацију.

106. Тактички носилац подмреже ВОЈНЕТ или сервиса у подмрежи, обраћа се техничком носиоцу окоснице ВОЈНЕТ са захтевом за повезивање локација на подмрежу ВОЈНЕТ.

107. Тактички носилац подмреже ВОЈНЕТ ажурира податке о конфигурацији мреже, сервисима и услугама које подмрежа пружа и доставља их УТИ (Ј-6) ГШ ВС.

#### 2. Поступак прикључења новог корисника у подмрежу ВОЈНЕТ

108. Унутрашње јединице Министарства одбране, уже унутрашње јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије достављају тактичком носиоцу подмреже захтев за повезивање на подмрежу у надлежности тактичког носиоца, а у циљу искоришћења сервиса и услуга из подмреже.

109. Захтев за увођење новог корисника у подмрежу ВОЈНЕТ садржи следеће податке:

- 1) локацију новог корисника подмреже ВОЈНЕТ;
- 2) капацитет/интерфејс потребан за повезивање новог корисника;
- 3) сервисе и ресурсе којима би приступао нови корисник у подмрежи ВОЈНЕТ;
- 4) расположиве хардверске и софтверске ресурсе за приступ подмрежи ВОЈНЕТ;
- 5) администратора локалне рачунарске мреже.

110. По добијању захтева из тачке 109. овог упутства тактички носилац разматра захтев ради процене оправданости увођења новог корисника у подмрежу ВОЈНЕТ. У случају оправданости прикључења корисника тактички

носилац доставља захтев техничком носиоцу окоснице ВОЈНЕТ за проверу могућности физичког и логичког прикључења новог корисника на ВОЈНЕТ.

111. У случају да не постоји оправданост прикључења, тактички носилац доставља одговор подносиоцу захтева са образложењем одбијања прикључења новог корисника.

112. Технички носилац окоснице ВОЈНЕТ, по добијању захтева за проверу техничких могућности повезивања новог корисника на ВОЈНЕТ, врши проверу могућности прикључења новог корисника и у року од 15 дана доставља одговор тактичком носиоцу подмреже ВОЈНЕТ.

113. Тактички носилац подмреже ВОЈНЕТ у случају постојања техничке могућности за повезивања новог корисника на ВОЈНЕТ доставља налог за прикључење новог корисника у подмрежу ВОЈНЕТ техничком носиоцу и подносиоцу захтева. Технички носилац и корисник успостављају неопходне капацитете до демаркационе тачке, а повезивање на демаркациону тачку врши администратор локалне рачунарске мреже корисника. Опрему за прикључење новог корисника на окосницу ВОЈНЕТ обезбеђује тактички носилац подмреже ВОЈНЕТ.

### **3. Поступак за увођење нових сервиса и апликација у подмрежу ВОЈНЕТ**

114. Тактички носилац подмреже ВОЈНЕТ доставља УТИ (Ј-6) ГШ ВС захтев за увођење новог сервиса или апликације у ВОЈНЕТ, односно подмрежу ВОЈНЕТ, из своје надлежности и наводи разлоге за увођење нових сервиса или апликације у подмрежу ВОЈНЕТ.

115. УТИ (Ј-6) ГШ ВС, у сарадњи са тактичким носиоцем и предлагачем, разматра захтев ради процене потребних хардверских, софтверских и ТкИ ресурса.

116. Верификацију новог сервиса или апликације врши УТИ (Ј-6) ГШ ВС, након чега одобрава увођење у употребу.

117. Одобрење за увођење новог сервиса или апликације у ВОЈНЕТ 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 ВОЈНЕТ, односно подмрежи ВОЈНЕТ, као и одговорност током експлоатације сервиса и апликације као надзор и управљање кључних чворова сервиса или апликације.

118. Пре одобравања и увођења новог сервиса могуће је одобрити период експерименталног рада – издавањем привременог одобрења за функционисање сервиса ради тестирања функционалности и утицаја на мрежу и друге, већ задејствоване сервисе.

### **4. Коришћење сервиса/апликација у ВОЈНЕТ**

119. Коришћење појединачног сервиса/апликације у ВОЈНЕТ, подмрежи ВОЈНЕТ, начин одржавања и могућност приступа, дефинише тактички носилац сервиса или апликације кроз посебна упутства или кроз инструкције Плана ТкИОб.

120. Тактички носилац дефинише упутства за сервисе/апликације уколико се они имплементирају на подмрежи намењеној за потребу сервиса и апликација различитих тактичких носилаца или ако је сервис или апликација намењена већем броју унутрашњих јединица Министарства одбране, ужих унутрашњих јединица Генералштаба Војске Србије и команди, јединица и установа Војске Србије којима намена, односно производ сервиса/апликације није основна функција.

121. Захтев за коришћење појединачног сервиса/апликације у ВОЈНЕТ доставља се тактичком носиоцу подмреже ВОЈНЕТ. У прилогу захтева достављају се подаци о прикључку који ће користити појединачне сервисе или апликације.

122. Тактички носилац сервиса/апликације дефинише инструкције Плана ТкИОб за рад са сервисом/апликацијом уколико је исти намењен тактичком носиоцу и више или ниже потчињеним саставима којима је намена, односно производ сервиса/апликације основна функција.

123. Приликом коришћења сервиса/апликација, корисници су у обавези да се придржавају дефинисаних упутстава и инструкција Плана ТкИОб за рад са сервисом или апликацијом у ВОЈНЕТ, односно подмрежама ВОЈНЕТ.

124. Прописивање и спровођење мера безбедности и заштите података за појединачне сервисе или апликације у надлежности је тактичког носиоца подмреже ВОЈНЕТ.

### **5. Документација подмреже и сервиса/апликација**

125. Тактички носилац подмреже у обавези је да документима Плана ТкИОб реализује, редовно ажурира и доставља УТИ (Ј-6) ГШ ВС измене прилога, додатака и инструкција, којима ће детаљно описати подмрежу.

126. Прилозима, додацима и инструкцијама из тачке 125. овог упутства, морају бити обухваћени следећи садржаји:

- 1) глобална логичка шема подмреже;
- 2) списак активних локација са опремом на локацијама;
- 3) физичко-логичка шема подмреже на свакој локацији;

- 4) адресни план подмреже са наведеним специфичним параметрима подмреже;
- 5) организација сервиса у подмрежи;
- 6) каталог сервиса и услуга у подмрежи;
- 7) мере безбедности и заштите у подмрежи.

127. Поред садржаја из тачке 126. овог упутства тактички носилац може креирати додатне садржаје како би детаљније описао подмрежу у својој надлежности.

128. Тактички носилац сервиса у обавези је да кроз План ТкИОб реализује, редовно ажурира и доставља УТИ (Ј-6) ГШ ВС измене (прилоге, додатке и инструкције), кроз које ће детаљно описати сервис, односно сервисе чији је носилац.

129. Тактички носилац подмреже/сервиса у обавези је да обезбеди надзор и управљање подмрежом и сервисима за које је надлежан.

#### IV. БЕЗБЕДНОСТ И ЗАШТИТА ВОЈНЕТ

##### 1. Опште одредбе

130. Рачунарска мрежа ВОЈНЕТ спада у виталне објекте Министарства одбране и Војске Србије које треба штитити.

131. Циљ примене мера безбедности и заштите у ВОЈНЕТ је заштита њене окоснице, као и подмрежа које се ослањају на окосницу, од нарушавања поверљивости, интегритета, расположивости, аутентичности и непоредности података који се креирају, складиште, обрађују и размењују унутар ВОЈНЕТ.

132. Безбедносним инцидентом у ВОЈНЕТ сматра се нарушавање три главна принципа информационе безбедности (поверљивост, интегритет и расположивост) коришћењем рањивости и недостатака у безбедносним механизмима примењеним на људе, операције и технологије.

133. Потенцијалним претњама нарушавања функционисања ВОЈНЕТ сматрају се елементарне непогоде, људски извори претњи (унутрашњи и спољашњи), претње проузроковане случајним оштећењем и претње из окружења (дугорочни прекиди напајања електричном енергијом, загађење околине и сл.).

134. Потенцијални људски извори претњи могу бити унутрашњи и/или спољашњи. Унутрашњим се сматрају сва лица која имају директан контакт са ВОЈНЕТ, а спољашњим сва остала лица.

135. Претњама безбедности проузрокованих случајним оштећењем сматрају се: ненамерне грешке, неискупство, грешке у хардверским и софтверским елементима и незгоде.

136. Инцидентом се сматра унутрашња или спољна околност или догађај у ВОЈНЕТ којим се угрожава или нарушава информациона безбедност, односно има значајан утицај на нарушавање информационе безбедности.

137. Под мерама безбедности и заштите ВОЈНЕТ сматрају се мере, радње и поступци којима се смањује рањивост система и умањују безбедносни ризици.

138. Опште мере безбедности прописује УТИ (Ј-6) ГШ ВС у сарадњи са ЦЕРТ ВС, у својству планског органа.

139. Посебне мере прописују технички носиоци окоснице ВОЈНЕТ и подмрежа, као и тактичко-технички носиоци сервиса, уз сагласност надлежног органа Војнобезбедносне агенције.

##### 2. Одговорност

140. Администратори ВОЈНЕТ одговорни су за примену свих прописаних мера безбедности и заштите.

141. Администратори подмрежа одговорни су за примену свих прописаних мера безбедности и заштите унутар подмреже.

142. Тактичко-технички носиоци окоснице ВОЈНЕТ, подмрежа и сервиса одговорни су за примену општих мера и прописивање и примену посебних мера безбедности и заштите у ВОЈНЕТ.

143. Органи и лица која учествују у планирању, развоју, унапређењу, одржавању и експлоатацији ВОЈНЕТ у обавези су да се придржавају прописаних мера безбедности и заштите ВОЈНЕТ.

144. Војнобезбедносна агенција учествује у планирању, организовању и контроли мера безбедности и заштите ВОЈНЕТ и планира, организује и спроводи мере контраобавештајне заштите ВОЈНЕТ у складу са прописима.

##### 3. Избор људства

145. За рад на елементима окоснице ВОЈНЕТ одређују се лица са одговарајућим квалификацијама, завршеним специјалистичким курсевима и сагласности УТИ (Ј-6) ГШ ВС.

146. За рад на елементима подмреже ВОЈНЕТ одређују се лица са одговарајућим квалификацијама, завршеним специјалистичким курсевима и сагласности тактичког носиоца подмреже.

147. За лица која су предвиђена за администраторе на елементима ВОЈНЕТ врши се одговарајућа безбедносна провера, у складу са прописима.

#### 4. Остало

148. Уколико се утврди неусклађеност мера безбедности и заштите ВОЈНЕТ, односно неодговарајућа примена прописаних мера безбедности и заштите, извештава се надлежни орган о природи и озбиљности повреде безбедности и заштите ВОЈНЕТ и, по потреби, захтева се хитно спровођење мера за отклањање недостатака.

149. У случају грубог нарушавања мера безбедности и заштите ВОЈНЕТ може се наложити мера искључења са ВОЈНЕТ до отклањања недостатака.

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

151. Функцију контроле мера безбедности регулисаће надлежни старешина на свом нивоу. Контролу примене мера безбедности вршити у складу са тачкама које се односе на примену мера безбедности у тренутно успостављеним подмрежама ВОЈНЕТ (нпр. РАМКО, РАМОН и итд.).

152. Строго је забрањено да се подаци и информације које су једном пренете кроз елементе система заштићене мреже поново преносе кроз елементе универзалне мреже. Изузетно, уколико за овим постоји потреба, потребно је обезбедити да се ти подаци и информације не преносе у изворном облику.

#### V. ЗАВРШНА ОДРЕДБА

153. Ово упутство ступа на снагу осмог дана од дана објављивања у „Службеном војном листу”.

Број 8001-3

У Београду, 25. новембра 2024. године

Министар одбране  
**Братислав Гашић**, с. р.

#### 73.

На основу члана 4. тачка 3) Правилника о материјалној стандардизацији у Министарству одбране и Војсци Србије („Службени војни лист”, број 24/18), помоћник министра одбране за материјалне ресурсе доноси

### РЕШЕЊЕ О ДОНОШЕЊУ РЕВИДИРАНИХ СТАНДАРДА ОДБРАНЕ

1. Доносе се следећи ревидирани стандарди одбране Републике Србије:

– СОРС 1029/24: Електромагнетне сметње ЗАХТЕВИ

– СОРС 1762/24: Електромагнетне сметње МЕРЕЊА.

2. Стављају се ван снаге ранија издања стандарда одбране Републике Србије, СОРС 1029/89, СОРС 4077/89 и СОРС 1762/89.

3. Стандарде одбране из тачке 1. овог решења штампа Дирекција за стандардизацију, кодификацију и метрологију Управе за одбрамбене технологије Сектора за материјалне ресурсе Министарства одбране.

4. Стандарди одбране из тачке 1. овог решења почињу да се примењују осмог дана од дана објављивања у „Службеном војном листу”.

Број 110-7

У Београду, 21. новембра 2024. године

Помоћник министра одбране  
за материјалне ресурсе  
**др Ненад Милорадовић**, с. р.

#### 74.

На основу члана 54. тачка 11) подтачка (3) Статута Универзитета одбране у Београду („Службени војни лист”, број 22/20), а у вези са чланом 78. став 3. Закона о високом образовању („Службени гласник РС”, бр. 88/17, 27/18 – др. закон, 73/18, 67/19, 6/20 – др. закони, 11/21 – аутентично тумачење, 67/21, 67/21 – др. закон и 76/23), Сенат Универзитета одбране у Београду на 153. седници одржаној дана 20. новембра 2024. године, доноси

### ПРАВИЛНИК О ПОСТУПКУ И УСЛОВИМА ДОДЕЛЕ ЗВАЊА И ПРАВА ЛИЦА ИЗБРАНОГ У ЗВАЊЕ ПРОФЕСОР ЕМЕРИТУС

#### I. УВОДНЕ ОДРЕДБЕ

## Члан 1.

Овим правилником ближе се уређују услови и поступак за доделу звања професор емеритус на Универзитету одбране у Београду (у даљем тексту: Универзитет), као и друга питања у вези са доделом звања професор емеритус.

## II. УСЛОВИ И ПОСТУПАК ЗА ДОДЕЛУ ЗВАЊА ПРОФЕСОР ЕМЕРИТУС

## Услови за доделу звања професор емеритус

## Члан 2.

Звање професор емеритус може се доделити лицу које испуњава следеће услове у складу са Законом о високом образовању (у даљем тексту: Закон):

- 1) да је изабран за наставника Универзитета у звању редовни професор;
- 2) да је пензионисан у претходне две школске године;
- 3) да има најмање 20 година радног стажа на универзитету;
- 4) да се посебно истакао својим научним радом и да је био руководиоца најмање два успешно оцењена научна пројекта;
- 5) да је стекао међународну репутацију;
- 6) да је постигао резултате у обезбеђивању наставно-научног подмлатка у области за коју је изабран и да је био ментор на најмање три одбрањене докторске дисертације.

Радни стаж на универзитету из става 1. овог члана обухвата и ефективни радни стаж у војним високошколским установама пре оснивања Универзитета.

## Члан 3.

Ближи критеријуми за доделу звања професор емеритус јесу:

- 1) сагласност кандидата;
- 2) поштовање кодекса професионалне етике;
- 3) радни стаж кандидата у настави на Универзитету;
- 4) заслуге за развој наставне и научне делатности односно за оспособљавање наставног кадра и научног подмлатка на Универзитету;
- 5) посебне заслуге за развој, напредак и углед Универзитета.

## Члан 4.

За доделу звања професор емеритус неопходна је писана сагласност предложеног кандидата.

## Члан 5.

Редовни професор може бити кандидат за звање професор емеритус уколико није правноснажном пресудом осуђен за кривично дело из члана 64. став 5. Закона и уколико није прекршио кодекс професионалне етике односно друге одговарајуће прописе Универзитета или друге високошколске установе.

## Члан 6.

Звање професор емеритус може се доделити лицу које је било најмање десет година у радном односу са пуним радним временом у високошколској јединици Универзитета која га предлаже.

Радни однос из става 1. овог члана обухвата и радни однос са пуним радним временом у војној високошколској установи пре оснивања Универзитета.

## Члан 7.

Заслуге за развој наставне и научне делатности односно за оспособљавање наставног кадра и научног подмлатка на Универзитету утврђују се на основу мишљења Наставно-научног већа високошколске јединице која предлаже кандидата за доделу звања професор емеритус.

Заслуге кандидата за развој научне делатности на Универзитету јесу:

- 1) радови објављени у водећим међународним и домаћим научним часописима;
- 2) чланство у уредништву научног часописа;
- 3) чланство у научног одбору научног скупа;
- 4) руковођење или учешће у научноистраживачким пројектима који су оцењени као успешни.

## Члан 8.

Посебне заслуге за развој, напредак и углед Универзитета кандидат за доделу звања професор емеритус јесу обављање функција у органима Универзитета односно високошколске јединице Универзитета и чланства у научним институцијама и удружењима.

Предност за доделу звања професор емеритус имају чланови Српске академије наука и уметности и лица која су обављала функцију ректора Универзитета или декана високошколске јединице Универзитета.

### Поступак доношења одлуке о додели звања професор емеритус

#### Члан 9.

Надлежна катедра подноси наставно-научном већу високошколске јединице Универзитета предлог кандидата са документима којима се доказује испуњеност услова за доделу звања професор емеритус.

Наставно-научно веће високошколске јединице Универзитета доноси одлуку о предлогу кандидата за доделу звања професор емеритус са образложењем испуњености услова прописаних овим правилником, коју доставља Сенату Универзитета.

Уз одлуку из става 2. овог члана достављају се и следећи докази о испуњености услова из чл. 2. и 3. овог правилника:

- 1) писана сагласност предложеног кандидата за доделу звања професор емеритус;
- 2) биографија кандидата;
- 3) копија одлуке о избору кандидата за наставника универзитета у звању редовни професор;
- 4) копија решења о пензионисању кандидата;
- 5) мишљење наставно-научног већа високошколске јединице Универзитета о међународној репутацији и заслугама кандидата за развој наставне и научне делатности односно за оспособљавање наставног кадра и научног подмлатка на Универзитету;
- 6) списак објављених радова кандидата са категоријама и коефицијентима, одређеним у складу са Правилником о поступку, начину вредновања и квантитативном исказивању научноистраживачких резултата истраживача које доноси министарство надлежно за науку;
- 7) одлука наставно-научног већа високошколске јединице Универзитета којом је ауторско дело кандидата верификовано као монографија у складу са критеријумима из Правилника о поступку и начину вредновања и квантитативном исказивању научноистраживачких резултата истраживача;
- 8) потврде високошколских установа о менторствима одбрањених докторских дисертација;
- 9) потврде високошколских установа о резултатима кандидата у реализацији научноистраживачких пројеката;
- 10) потврде уредништва међународних и домаћих научних часописа о чланству кандидата у уредништву;
- 11) потврде организатора међународних и домаћих научних скупова о чланству кандидата у научном одбору скупа;
- 12) остала документа којима се доказују заслуге кандидата (чланство у академијама наука и уметности, избор гостујућег професора универзитета, предавања по позиву и др.).

Међународна репутација кандидата вреднује се на основу учешћа у успешно оцењеним међународним научноистраживачким пројектима, параметара цитираниости у научним часописима међународног значаја (количина објављених радова, кумулативни импакт фактор, *h*-индекс, *i10*-индекс и др.), објављених монографија међународног значаја, предавања по позиву на страним универзитетима и међународним научним скуповима, чланству у међународним научним односно стручним организацијама и другим одговарајућим међународно признатим резултатима.

#### Члан 10.

Сенат Универзитета у року од 45 дана од пријема предлога из члана 9. овог правилника образује Комисију за проверу испуњености услова за доделу звања професор емеритус (у даљем тексту: Комисија).

Комисија се састоји од три или пет редовних професора изабраних за научну област предложеног кандидата, од којих је најмање један са другог универзитета.

Комисија у року од 45 дана од образовања подноси Извештај о испуњености услова за доделу звања професор емеритус (у даљем тексту: Извештај) са свим документима на основу којих је израђен Извештај.

Изузетно од става 3. овог члана, Комисија може донети Закључак о одлагању разматрања предлога кандидата за доделу звања професор емеритус (у даљем тексту: Закључак) ради прибављања додатних докумената потребних за израду Извештаја, који доставља Сенату Универзитета и наставно-научном већу високошколске јединице која је предложила кандидата. Наставно-научно веће високошколске јединице у року од 30 дана од пријема Закључка доставља Комисији тражена додатна документа.

Рок за подношење Извештаја продужава се за период од доношења Закључка до пријема додатних докумената из става 4. овог члана.

Извештај се ставља на увид јавности у трајању од 30 дана објављивањем на интернет страници Универзитета.

## Члан 11.

Сенат Универзитета доноси одлуку о додели звања професор емеритус на основу предлога наставно-научног већа високошколске јединице и Извештаја.

Одлука о додели звања професор емеритус доноси се на основу већине гласова од укупног броја редовних професора који су чланови Сената Универзитета.

Сенат Универзитета доставља кандидату одлуку о додели звања професор емеритус преко високошколске јединице Универзитета која је предложила кандидата.

Звање професор емеритус је доживотно и не може се накнадно одузети.

**Права и обавезе професора емеритуса**

## Члан 12.

Права и обавезе професора емеритуса уређују се уговором који закључује декан надлежне високошколске јединице на основу сагласности ректора Универзитета.

Укупан број ангажованих професора емеритуса не може бити већи од 3% од укупног броја ангажованих наставника универзитета у школској години.

Накнада за рад професора емеритуса, који изводи наставу на мастер академским студијама и докторским студијама исплаћује се под истим условима као и лицима из члана 93. став 2. Закона.

Професор емеритус има право да:

- 1) учествује у извођењу свих облика наставе из уже научне области за коју је изабран у оквиру студијских програма академских студија другог и трећег степена;
- 2) буде ментор или члан комисија у поступку пријаве, израде и одбране завршних радова на академским студијама другог и трећег степена;
- 3) учествује у научноистраживачком раду на Универзитету;
- 4) буде члан комисија за избор у звање наставника и сарадника;
- 5) буде члан стручних органа Универзитета или високошколских јединица.

Професор емеритус може се ангажовати на високошколској установи која није у саставу Универзитета само уз претходно одобрење Сената Универзитета.

Високошколска јединица која је предложила доделу звања професор емеритус обезбеђује простор, опрему и остале услове за остваривање права професора емеритуса.

**Повеља „Професор емеритус“**

## Члан 13.

Ректор Универзитета уручује професору Повељу „Професор емеритус“ на свечаности поводом обележавања Дана Универзитета.

Одлуку о изгледу и садржини Повеље „Професор емеритус“ доноси Сенат Универзитета.

**Евиденција**

## Члан 14.

Универзитет води Евиденцију о додели звања професор емеритус на обрасцу који утврђује ректор Универзитета.

Евиденција из става 1. овог члана чува се трајно.

**III. ПРЕЛАЗНА И ЗАВРШНА ОДРЕДБА**

## Члан 15.

Даном ступања на снагу овог правилника престаје да важи Правилник о поступку и условима доделе звања и права лица изабраног у звање професор емеритус („Службени војни лист“, број 38/21).

## Члан 16.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном војном листу“.

Број 23-362

У Београду, 25. новембра 2024. године.

Председавајући Сената  
бригадни генерал

проф. др **Бобан Ђоровић**, дипл. инж. с. р.

## С А Д Р Ж А Ј

	Страна
72. <b>Упутство</b> о коришћењу рачунарске мреже Војске Србије ВОЈНЕТ .....	557
73. <b>Решење</b> о доношењу ревидираних стандарда одбране .....	568
74. <b>Правилник</b> о поступку и условима доделе звања и права лица изабраног у звање професор емеритус ..	568

---

МИНИСТАРСТВО ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ  
„Службени војни лист”, 11000 Београд, Бирчанинова 5  
Главни и одговорни уредник Татјана Оровић, проф.  
Телефон: 011/3203-133 (32-133)  
Телефон/факс: 011/2910-162  
Штампа: Војна штампарија, Београд, Ресавска 40б

---

