ISSN 1821-4088
COBISS.SR-ID 49270540

СЛУЖБЕНИ ВОЈНИ ЛИСТ

БРОЈ 21 **Београд, 8. август 2017.** **ГОДИНА CXXXVI**

Цена овог броја је 279 динара
Годишња претплата је 8.693 динара

232.

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

У П У Т С Т В О
О ОРГАНИЗОВАЊУ И УСКЛАЂИВАЊУ ИНТЕРНЕТА ЗА ПОТРЕБЕ МИНИСТАРСТВА ОДБРАНЕ И ВОЈСКЕ СРБИЈЕ

I. УВОДНЕ ОДРЕДБЕ

1. Овим упутством уређује се начин организовања и усклађивања Интернета за потребе Министарства одбране и Војске Србије (у даљем тексту: интернет).

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

1) **Интернет** (Интернационална мрежа) је глобална мрежа, дизајнирана за рачунарску комуникацију на великој територији, која повезује рачунаре у целом свету. То је мрежа великог броја информационих путева у свету, односно мрежа већине рачунарских мрежа WAN (Wide Area Network) у свету. За контролу преноса информација – података дефинисан је посебан протокол TCP/IP (Transmission Control Protocol/Internet Protocol), без обзира на то на којем је корисничком и организационом нивоу конкретна мрежа (појединац, група, колектив, град, држава, континент...);

2) **надлежно лице** је начелник, командант, директор или управник организацијске целине Министарства одбране и организацијске јединице Генералштаба Војске Србије и команде, јединице и установе Војске Србије;

3) **Главни интернет центар** формиран је у Центру за командно-информационе системе и информатичку подршку и обавља стручно, техничко и организационо обезбеђење функционисања интернета у Министарству одбране и Војсци Србије;

4) **администратор интернета** (у даљем тексту: администратор) јесте лице које организује и спроводи активности у вези са радом на интернету у организацијској целини Министарства одбране и команди, јединици и установи Војске Србије и одређује се наредбом надлежног лица;

5) **корисник интернета** је лице у организацијској целини Министарства одбране и команди, јединици и установи Војске Србије коме је одобрено коришћење интернета у Министарству одбране и Војсци Србије.

II. ОРГАНИЗОВАЊЕ ИНТЕРНЕТА

2. У Министарству одбране и Војсци Србије, приступ интернету користи се за:

1) претраживање информационих база и других садржаја;

2) размену електронске поште (e-mail);

3) представљање информација путем јавних презентација (веб-сајт, друштвене мреже и друго);

4) реализацију јавних набавки;

5) друге облике размене информација, сходно конкретним надлежностима организацијских целина Министарства одбране и команди, јединици и установа Војске Србије.

3. За приступ интернету користе се рачунари, рачунарска опрема и спојни путеви намењени искључиво за ову намену.

4. Хардверске и софтверске компоненте радних станица и опреме за рад на интернету дефинисане су Захтевом за опремом која се користи на интернету који је дат у Прилогу 1. овог упутства и чини његов саставни део.

5. Сервиси на интернету су системски сервиси и сервиси подршке:

1) системски сервиси су сервиси који обезбеђују основне функционалности интернета и рад сервиса подршке;

2) сервиси подршке и апликације реализују се по захтеву тактичких носилаца који су одговорни за њихову администрацију и коришћење.

6. Апликације на интернету намењене су за реализацију функционалних задатака организацијских целина Министарства одбране и команди, јединица и установа Војске Србије.

7. Управа за телекомуникације и информатику (J-6) Генералштаба Војске Србије води евиденцију сервиса и апликација на интернету на обрасцу Списак сервиса и апликација који се користе на интернету који је дат у Прилогу 2. овог упутства и чини његов саставни део.

8. Тактички носиоци сервиса на интернету одговорни су за садржаје који су обухваћени конкретним сервисом.

9. Безбедносни механизми за коришћење апликације на интернету уграђују се и примењују унутар апликације, што је обавеза носиоца развоја апликације.

1. Овлашћења у организовању и уређењу интернета

10. Управа за телекомуникације и информатику (J-6) Генералштаба Војске Србије регулише, организује и обезбеђује приступ интернету, опрема, надгледа функционисање и управља интернетом.

Управа за телекомуникације и информатику (J-6) Генералштаба Војске Србије:

1) усваја системске основе приступа интернету;

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

3) организује и опрема кадровски и материјално Главни интернет центар;

4) планира и организује обуку за администраторе и кориснике интернета у Министарству одбране и Војсци Србије;

5) дефинише форму и садржај захтева за рад на интернету;

6) регулише коришћење сервиса електронске поште на интернету;

7) обезбеђује средства и учествује у склапању уговора са једним одабраним провајдером или више одабраних надпровајдера о коришћењу потребних интернет ресурса и услуга;

8) одобрава појединачне или групне прикључке на интернет (други облици повезивања на интернет регулишу се посебним одобрењем Управе за телекомуникације и информатику (J-6) Генералштаба Војске Србије);

9) одобрава коришћење специфичних сервиса на интернету;

10) регулише начин планирања и организације рада на интернету;

11) управља ресурсима на интернету ради обезбеђења доступности приоритетних садржаја за обављање функционалних задатака корисника интернета;

12) надгледа функционисање и дефинише безбедносна правила за коришћење интернета;

13) дефинише хардверске и софтверске компоненте радних станица и опреме за рад на интернету;

14) уводи нове сервисе и апликације на интернету;

15) усмерава и усклађује у стручном погледу рад органа информатичке службе и референата за интернет на свим нивоима и пружа им стручну помоћ;

16) врши контролу рада на интернету из своје надлежности;

17) регулише остала питања у вези са интернетом, из своје надлежности, која нису регулисана овим упутством и другим документима.

11. Центар за командно-информационе системе и информатичку подршку:

1) обезбеђује функционисање Главног интернет центра;

2) администрира интернет домене, сервисе и кориснике интернета прикључених директно на Главни интернет центар;

3) обезбеђује функционисање сервиса и пружање услуга (у својству провајдера) за кориснике интернета;

4) спроводи безбедносна правила за приступ садржајима на интернету;

5) учествује у изради стручних упутстава за рад на интернету и других прописа из ове области;

6) предлаже критеријуме и смернице за коришћење техничких ресурса интернета;

7) изучава, прати и анализира организацију сервиса и протокола за рад на интернету, предлаже начине њиховог усавршавања и отклањање недостатака;

8) организује и спроводи истраживачки рад за праћење развоја хардвера и софтвера за рад на интернету, даје иницијативу и предлаже мере за набавку нових и усавршавање постојећих хардверских и софтверских средстава за рад на интернету;

9) анализира безбедносне проблеме и ризике на интернету и предузима мере за отклањање проблема и смањења ризика;

10) усмерава и усклађује у стручном погледу рад администратора интернета на свим нивоима и пружа стручну помоћ;

11) предлаже Управи за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије надпровајдера за интернет, на основу стручно утврђених критеријума, од којих су најважнији капацитет, поузданост и безбедност везе са надређеним провајдером ван Републике Србије;

12) контролише спровођење мера које су прописане овим упутством;

13) пријављује безбедносне инциденте организационој целини Министарства одбране надлежној за безбедност информационо-комуникационих система;

14) води евиденцију сервиса и апликација на Интернету на обрасцу Евиденција сервиса и апликација на интернету, који је дат у Прилогу 3. овог упутства и чини његов саставни део.

12. Бригада везе, односно јединица за телекомуникације и информатику у Ратном ваздухопловству и противваздухопловној одбрани:

1) обезбеђује функционисање интернета на транспортном и приступном нивоу;

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

3) обезбеђује непрекидно функционисање система преноса;

4) активира прикључке на интернет и прикључује кориснике;

5) надгледа функционисање интернета на транспортном и приступном нивоу и отклања уочене проблеме;

6) процењује претње и ризике по безбедност компоненти интернета у својој надлежности и имплементира сигурносне механизме;

7) води Евиденцију прикључака на интернет и Евиденцију опреме за пренос података на интернету на обрасцима који су дати у прилозима 4. и 5. овог упутства и чине његов саставни део.

13. Орган информатике у организацијској целини Министарства одбране и команди, јединици и установи Војске Србије (односно орган телекомуникационог и информатичког обезбеђења из претпостављене или потчињене целине, уколико организацијска целина Министарства одбране и команда, јединица и установа Војске Србије нема орган информатике у свом саставу):

1) инсталира и подешава рачунаре и рачунарску опрему за приступ интернету у складу са одобрењем за прикључење на интернет;

2) инсталира одобрене програме за заштиту радних станица од злонамерних садржаја и неовлашћеног приступа, као и друге одобрене корисничке програме;

3) примењује мере безбедности и заштите на радним станицама за интернет;

4) контролише функционисање радних станица које су прикључене на интернет;

5) изводи обуку корисника за рад на интернету у оквиру своје организацијске целине Министарства одбране и команде, јединице и установе Војске Србије;

6) контролише крајње кориснике у поштовању мера безбедности и заштите за рад на интернету;

7) води Евиденцију корисника сервиса и апликација (корисничких налога) (уколико је тактички носилац) који је дат у Прилогу 6. овог упутства и чини његов саставни део.

14. Администратор:

1) израђује и ажурира Елаборат за коришћење интернета;

2) дефинише захтев за прикључење корисника на интернет;

3) обједињава захтеве за прикључење корисника и коришћење сервиса од непосредно потчињених састава и прослеђује их надлежном органу за телекомуникационо и информатичко обезбеђење;

4) доставља захтеве у вези са коришћењем сервиса електронске поште на интернет;

5) води Евиденцију радних станица на интернету која је дата у Прилогу 7. овог упутства и чини његов саставни део и евиденције о ресурсима који се користе (рачунари, кориснички налози, налози електронске поште, просторије и друго) на интернету;

6) инсталира и администрира рачунаре (оперативни систем, кориснички програми и антивирусна заштита) и корисничке налоге за рад на интернету;

7) организује и изводи обуку за потребе корисника интернета;

8) контролише спровођење мера које су прописане овим упутством;

9) отклања уочене неисправности или нерегуларности у раду на интернету и у оквиру својих надлежности или их пријављује надлежном органу за телекомуникационо и информатичко обезбеђење уколико нису у његовој надлежности;

10) предузима и друге мере за несметано функционисање интернета у складу са овим упутством и другим документима који уређују коришћење интернета.

III. УСКЛАЂИВАЊЕ ИНТЕРНЕТА

1. Начин прикључења на интернет

15. Корисници интернета из Министарства одбране и Војске Србије у Републици Србији повезују се на интернет преко Главног интернет центра (директним приступом кроз сопствене капацитете или капацитете провајдера) или путем мобилног интернета (3Г, 4Г и друго), а ван Републике Србије коришћењем локално расположивих интернет ресурса.

16. Војнобезбедносна агенција и Војнообавештајна агенција, ради обављања послова из своје надлежности, могу самостално планирати и организовати рад на интернету.

Војнобезбедносна агенција и Војнообавештајна агенција имају опште одобрење за рад на интернету.

Војнобезбедносна агенција и Војнообавештајна агенција могу се повезати на интернет директном везом са провајдером (кроз сопствене телекомуникационо информатичке капацитете или капацитете провајдера) или преко Главног интернет центра.

17. Корисници интернета могу да се повезују на интернет и преко Академске мреже Србије (AMPEC) уз сагласност Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

18. Прикључење корисника на интернет путем бежичног приступа (WiFi) није дозвољено, изузев у посебним случајевима и привремено уз одобрење Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије (међународне вежбе, конференције и друго).

19. Захтев за прикључење на интернет упућује се Управи за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

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

20. Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије, на основу сагледаних материјално-техничких и других услова одобрава прикључење на интернет.

Одобрење за прикључење на интернет дато је у Прилогу 9. овог упутства и чини његов саставни део.

21. На основу одобрења Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије, организацијска целина Министарства одбране и команда, јединица и установа Војске Србије упућује Бригади везе захтев са активирање прикључка на интернет.

Захтев за активирање односно деактивирање прикључка на интернет дат је у Прилогу 10. овог упутства и чини његов саставни део.

22. Минимални услови за прикључење на интернет су: један персонални рачунар или више, повезаних у локалну мрежу, испуњење техничких предуслова за прикључење корисничке локације на Главни интернет центар или путем мобилног интернета, познавање рада на интернету и да је организацијској целини Министарства одбране и команди, јединици и установи Војске Србије прикључак (број радних станица) одобрен у складу са утврђеним критеријумом припадања персоналних рачунара опште намене и пратеће опреме.

2. Планирање и употреба Интернета

23. Планирање и организовање рада на интернету обављају Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије, органи информатике и администратори у организацијским целинама Министарства одбране и командама, јединицама и установама Војске Србије.

24. На стратегијском, оперативном и тактичком нивоу, непосредну подршку за успостављање и коришћења интернета пружају органи информатике или органи за телекомуникационо информатичко обезбеђење.

25. Уколико организацијска целина Министарства одбране и команда, јединица и установа Војске Србије нема орган информатике у свом саставу, претпостављеном или потчињеном саставу, подршку у коришћењу интернета регулише Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

26. У свим организацијским целинама Министарства одбране и командама, јединицама и установама Војске Србије одређује се администратор.

27. Организовање рада на интернету усклађује се са потребама руковођења и командовања и бројем средстава за рад на интернету (рачунари, комуникациона опрема и спојни путеви) сходно утврђеном критеријуму припадања персоналних рачунара опште намене и пратеће опреме у Министарству одбране и Војсци Србије.

28. За опремање и организацију радног места за рад на интернету одговорна је организацијска целина Министарства одбране и команда, јединица и установа Војске Србије.

29. Рад на интернету организује се у складу са одобреним начином и капацитетом за приступ интернету.

30. На основу овог упутства организацијска целина Министарства одбране и команда, јединица и установа Војске Србије израђује Елаборат за интернет који садржи:

1) наређење организацијске целине Министарства одбране и команде, јединице и установе Војске Србије за организовање и усклађивање интернета (распоред опреме за приступ интернету, одређивање администратора и лице које га мења, израда Елабората, упутство за рад на интернету, начин контроле правилности коришћења одобрених ресурса и друго);

2) одобрење за коришћење интернета;

3) упутство за рад на интернету којим се дефинишу радне станице, рачунарска опрема и спојни путеви за приступ интернету, начин прикључења рачунара, препоруке за програме за коришћење расположивих сервиса, начин обраде прикупљених информација, докумената, понашање корисника на интернету и друга питања;

4) пропис који уређује организовање и усклађивање интернета за потребе Министарства одбране и Војске Србије;

5) план мера заштите за рад на интернету;

6) сагласност надлежног органа Војнобезбедносне агенције на План мера заштите за рад на интернету.

31. Тактички носилац доставља Управи за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије захтев за увођење новог сервиса или апликације на интернет из своје надлежности.

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

32. Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије врши верификацију сервиса или апликације и одобрава његово коришћење.

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

33. Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије дефинише безбедносна правила за коришћење интернета и приступ садржајима на интернету.

Организацијска целина Министарства одбране и команда, јединица и установа Војске Србије доставља Управи за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије захтев за приступ садржајима на интернету који је дат у Прилогу 13. овог упутства и чини његов саставни део.

34. Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије може одобрити приступ садржајима на интернету.

Одобрење за приступ садржајима на интернету дато је у Прилогу 14. овог упутства и чини његов саставни део.

3. Мере заштите за рад на интернету

35. Мере заштите за рад на интернету обухватају мере и поступке који се непрекидно и систематски планирају, организују и спроводе у организацијским целинама Министарства одбране и командама, јединицама и

установама Војске Србије у којима је организован рад на интернету, а са основним циљем да се превентивно делује и спречи отицање тајних података (случајно или намерно) и обезбеди овлашћени приступ, доступност и интегритет интернета.

36. Мере заштите за рад на интернету морају бити потпуне, правовремене, непрекидне и усклађене са осталим мерама заштите (безбедности) у организацијским целинама Министарства одбране и командама, јединицама и установама Војске Србије.

37. Посебни циљ мера заштите за рад на интернету је:

1) заштита тајности корисничких налога, односно спречавање неовлашћеним лицима приступ ресурсима на интернету;

2) спречавање неовлашћеног приступања и коришћења података на интернету (приступ базама података, електронској пошти, друштвеним мрежама, презентацијама, онлајн сервисима и друго);

3) спречавање извршења кривичних дела против безбедности рачунарских података ради заштите података и налога корисника интернета;

4) спречавање неовлашћеног приступа рачунарима и базама података других корисника интернета и спречавање намерне дистрибуције злонамерних програма (malware);

5) заштита рачунарске опреме од оштећења и отуђења.

38. На основу овог упутства надлежно лице организацијске целине Министарства одбране и команде, јединице и установе Војске Србије доноси план мера заштите за рад на интернету.

39. Са планом мера заштите за рад на интернету мора бити сагласан надлежни орган Војнобезбедносне агенције.

40. Планом мера заштите за рад на интернету утврђују се превентивне и корективне мере.

41. Циљ превентивних мера заштите за рад на интернету је да спрече угрожавање интернета и смање степен штете, уколико до угрожавања дође.

42. Превентивним мерама заштите за рад на интернету дефинишу се:

1) организациони елементи заштите;

2) физичке мере заштите;

3) техничке мере заштите;

4) противпожарне мере;

5) остале превентивне мере.

43. Хардверско-софтверска заштита од неовлашћеног приступа интернету реализује се на свим интернет ресурсима, у складу са надлежностима.

44. Корективне мере заштите за рад на интернету су у функцији спречавања повећања штете, уколико дође до угрожавања интернета, као и обезбеђења његовог брзог и ефикасног опоравка.

45. У случају угрожавања или злоупотребе интернета надлежна лица, органи информатике, администратори и корисници обезбеђују заштиту и очување података и трагова који би указивали на порекло односно узрок угрожавања или злоупотребе, искључују са интернета локацију на којој је дошло до нарушавања безбедности и врше евидентирање инцидента.

46. У случају нарушавања безбедности, угрожавања или злоупотребе интернета односно појаве безбедносног инцидента, инцидент се неодложно пријављује линијом командовања и линијом: крајњи корисник интернета – администратор – надлежни орган телекомуникационог информатичког обезбеђења – Главни интернет центар – Управа за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

47. Нарушавање безбедности, угрожавање или злоупотребу интернета, односно појаву безбедносног инцидента, администратор неодложно пријављује и надлежном органу Војнобезбедносне агенције.

48. Надлежно лице, орган информатичке службе и администратор планирају, организују и врше контролу примене мера заштите за рад на интернету у организацијској целини Министарства одбране и команди, јединици и установи Војске Србије.

49. Корисници интернета примењују прописане мере заштите за рад на интернету.

50. Тактички носиоци у поступку израде и постављања веб презентације Министарства одбране и Војске Србије испуњавају техничке и безбедносне захтеве Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

Постављање веб презентације врши се по добијању сагласности Управе за телекомуникације и информатику (Ј-6) Генералштаба Војске Србије.

51. На радној станици и опреми за приступ интернету није дозвољена припрема, израда, измена, чување, објављивање и слање тајних података.

52. Органи у организацијским целинама Министарства одбране и командама, јединицама и установама Војске Србије у чијој надлежности су послови опште безбедности:

1) повремено и превентивно контролишу просторије, опрему и кориснике интернета;

2) превентивно, у сарадњи са органом информатичке службе и администратором, упознају кориснике са безбедносним аспектима коришћења интернета и последицама његовог неправилног коришћења;

3) усавршавају се за праћење савремених безбедносних ризика и претњи на интернету.

53. Војнобезбедносна агенција обавља послове безбедносне и контраобавештајне заштите интернета у складу са законом.

54. Управа за телекомуникације и информатику (J-6) Генералштаба Војске Србије може одобрити и употребу другог хардвера и софтвера.

55. На радној станици за рад на интернету мора се користити прописана софтверска заштита (одговарајућа конфигурација интернет опција оперативног система, ажурни антивирусни програми и други програми за спречавање неовлашћеног приступа рачунару преко интернета и спречавања инсталације злонамерних садржаја).

56. Радна станица за рад на интернету не сме се користити у друге сврхе.

57. Радна станица и рачунарске мреже за рад на интернету морају бити физички раздвојени од осталих рачунара и рачунарских мрежа који су на коришћењу у Министарству одбране и Војсци Србије.

58. Основни начин дистрибуције садржаја са интернета је путем штампе на штампачу прикљученом на радну станицу, чиме се онемогућава дистрибуција злонамерних садржаја који се могу налазити у материјалу преузетом са интернета.

59. Изузетно, садржај са интернета може се преузети и у изворном (електронском) облику у складу са планом телекомуникационо информатичког обезбеђења Министарства одбране и Војске Србије.

60. У раду интернета Министарства одбране и Војске Србије не користе се елементи криптозаштите и корисници интернета размењују садржаје који нису шифровани.

Корисницима интернета из Министарства одбране и Војске Србије, на њихов захтев, Управа за телекомуникације и информатику (J-6) Генералштаба Војске Србије може одобрити размену шифрованих садржаја, при чему прописује начин, услове и методе рада.

61. Приликом регистрације за приступ садржајима на интернету не могу се користити исти приступни параметри (корисничко име и лозинка) који се користе за приступ рачунарима и рачунарској опреми за интернет.

62. Корисници интернета у обавези су да чувају од злоупотребе ресурсе који су им дати на коришћење, да се придржавају прописаних правила у коришћењу интернета, да администратору пријаве сваку уочену неисправност или нерегуларност у раду на интернету и одговарају за податке и информације које размењују путем интернета.

63. Ресурси за рад на интернету дати на употребу корисницима су службени ресурси и није дозвољено њихово коришћење у приватне сврхе.

64. На ресурсима за рад на интернету није дозвољено прикључивање и коришћење приватних рачунарских и комуникационих средстава.

65. Против лица која се не придржавају прописаних мера заштите за рад на интернету покреће се одговарајући поступак, у складу са прописима.

IV. ЗАВРШНЕ ОДРЕДБЕ

66. Даном ступања на снагу овог упутства престаје да важи Упутство о коришћењу Интернета у Министарству одбране и Војсци Србије и Црне Горе („Службени војни лист“, број 1/06).

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

Број 9602-1
У Београду, 2. августа 2017. године

Министар одбране
Александар Вулин, с. р.

Прилог 1.

Захтеви за опрему која се користи на интернету

ХАРДВЕР				СОФТВЕР		
Тип опреме	**Компонента**	**Минимална**	**Препоручена**	**Системски**	**Кориснички**	**Антивирусна заштита**
Радна станица	Процесор	*Pentium 3*	*Pentium 4*	*Windows XP Pro with SP3 (*или новији), *Linux*	*Microsoft Office XP (*или новији), *Internet Eksplorer v6 Outlook Express v6* *Firefox*	*ESET EndPoint Security*
	Радна меморија	*256 MB*	*1 GB +*			
	Харддиск	*20 GB*	*80 GB +*			
	Графичка картица	Интегрисана са *8 MB* дељене *RAM* меморије	*PCI VGA Card* са *5121 MB RAM +*			
	Монитор	*15" CRT*	*17" CRT +*			
	Оптички уређај	*CD* читач	*DVD* читач +			
	Тастатура	Стандардна	Стандардна			
	Миш	Оптички	Оптички			
	УПС уређај	–	*650 VA +*			
	Штампач	–	Ласерски ц/б *A4 +*			
	Скенер	–	*A4 +*			
Сервер	Процесор	*Pentium 4*	*Xeon +*	*Windows 2000 Server (*или новији)	Према намени сервера	*ESET EndPoint Security*
	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.

Списак сервиса и апликација који се користе на на интернету

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

Прилог 3.

Евиденција сервиса и апликација на интернету

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	Организацијска целина МО и команда, јединица и установа ВС	Контакт телефон
1	2	3	4	5	6	7	8	9

Прилог 4.

Евиденција прикључака на интернет

_____
(организацијска целина МО и команда, јединица и установа ВС)

Редни број	Корисник (организацијска целина МО и команда, јединица и установа ВС)	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

Прилог 5.

Евиденција опреме за пренос података на интернету

____
(стационарни телекомуникациони центар / чвориште)

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

Прилог 6.

Евиденција корисника сервиса и апликација (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	Организацијска целина и команда, јединица и установа која је издала наређење	Име и презиме	Формацијска дужност	Организацијска целина МО и команда, јединица и установа ВС	Контакт телефон
1	2	3	4	5	6	7	8	9	10

Прилог 7.

Евиденција радних станица на интернету

_____
(организацијска целина МО и команда, јединица и установа ВС)

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

Прилог 8.

Захтев за прикључење на интернет

Назив организацијске целине МО и команде, јединице и установе ВС	
Тип прикључка на Интернет	
Број рачунара на прикључку	
Локација (зграда и просторија у згради) на којој треба обезбедити прикључење на Интернет	
Образложење захтева (навести сервисе и апликације који би се користили и локацију сервера на којима се извршавају)	
Администратор (чин, име, презиме, телефон, функционална дужност и информатички курсеви)	

Прилог 9.

Одобрење за прикључење на интернет

Назив организацијске целине МО и команде, јединице и установе ВС	
Локација (зграда и просторија у згради) на којој се обезбеђује прикључење на Интернет	
Начин прикључења на Интернет (директан приступ, прикључак на ТкИС МО и ВС, *ADSL VPN*)	
Одобрена брзина комуникације / количина података на прикључку	
Тип прикључка на Интернет	
Опсег *IP* адреса за корисника Интернета	
Списак одобрених сервиса и апликација	
Неопходне информације за подешавање рачунара и рачунарске опреме	
Организационо-техничке информације значајне за повезивање	

Прилог 10.

Захтев за активирање односно деактивирање прикључка на интернет

_____
(организацијска целина МО и команда, јединица и установа ВС)

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

Прилог 11.

Захтев за увођење сервиса или апликације на интернет

1	**Назив организацијске целине МО и команде, јединице и установе ВС**		
2	**Назив сервиса или апликације**		
3	**Сврха коришћења сервиса или апликације**		
4	**Образложење захтева**		
5	**Одговорно лице**	**Чин, име и презиме**	
		Назив организацијске целине МО и команде, јединице и установе ВС	
		Контакт телефон	

Прилог 12.

Одобрење за увођење сервиса или апликације на интернет

1	**Назив организацијске целине МО и команде, јединице и установе ВС**		
2	**Назив сервиса или апликације**		
3	**Сврха коришћења сервиса или апликације**		
4	**Образложење одобрења**		
5	**Одговорно лице**	**Чин, име и презиме**	
		Назив организацијске целине МО и команде, јединице и установе ВС	
		Контакт телефон	

Прилог 13.

Захтев за приступ садржајима на интернету

1	**Назив организацијске целине МО и команде, јединице и установе ВС**		
2	**Интернет адреса садржаја**		
3	**Сврха приступа садржају**		
4	**Образложење захтева**		
5	**Одговорно лице**	**Чин, име и презиме**	
		Назив организацијске целине МО и команде, јединице и установе ВС	
		Контакт телефон	

Прилог 14.

Одобрење за приступ садржајима на интернету

1	**Назив организацијске целине МО и команде, јединице и установе ВС**		
2	**Интернет адреса садржаја**		
3	**Сврха приступа садржају**		
4	**Образложење одобрења**		
5	**Одговорно лице**	**Чин, име и презиме**	
		Назив организацијске целине МО и команде, јединице и установе ВС	
		Контакт телефон	

С А Д Р Ж А Ј

Страна

232. **Упутство** о организовању и усклађивању Интернета за потребе Министарства одбране и Војске Србије 465

МИНИСТАРСТВО ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ
„Службени војни лист“, 11000 Београд, Бирчанинова 5
Телефони: 011/3203-133 (32-133) и 011/3201–979 (23–979)
Телефон/факс: 011/3000–200
Штампа: Војна штампарија „Београд“, Београд, Ресавска 40б
ISSN 1821-4088