

## КОНТРОЛНА ЛИСТА

Чињенично стање и утврђене, описане и документоване неправилности (ако су утврђене) биће евидентиране у записнику о инспекцијском надзору чији је саставни део ова контролна листа

<b>Предмет инспекцијског надзора</b>	<b>мере обезбеђивања у ваздухопловству које се односе на сајбер претње, обезбеђивање критичних објеката, инфраструктуре и система</b>
<b>Објекат инспекцијског надзора</b>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<b>Област: Глава 2, Одељак 5. дела II Националног програма, Програм за контролу квалитета мера обезбеђивања у ваздухопловству</b>				
Део II, Националног програма, 5.5. Унутрашња контрола квалитета Да ли је субјект израдио годишњи план унутрашње контроле квалитета, утврђен у складу са идентификованим слабим тачкама система обезбеђивања у ваздухопловству и проценом ризика? Ако је одговор да, да ли субјект у складу са тим планом, спроводи унутрашњу контролу квалитета мера обезбеђивања у ваздухопловству за које је надлежан?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли је субјект подговорио спровођење појединих мера обезбеђивања за које је надлежан? Ако је одговор да, да ли субјект периодично спроводи контролу квалитета примене тих мера у циљу утврђивања да ли се оне спроводе у складу са сопственим програмом за обезбеђивање у ваздухопловству и да ли су ове контроле наведене у годишњем плану унутрашње контроле квалитета тог субјекта?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли о свим спроведеним контролама квалитета субјект води евиденцију?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли о налазима унутрашње контроле квалитета одговорно лице за обезбеђивање унутар тог субјекта по захтеву обавештава Директорат?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли је субјект: 1) именовао лице одговорно за унутрашњу контролу квалитета, независно од оперативних руководиоца? 2) припремио, спровео и да ли одржава контролу квалитета, као и обезбеђење квалитета у циљу	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>провере усаглашености постојећих мера обезбеђивања у ваздухопловству са захтевима Националног програма?</p> <p>3) успоставио процес анализе и извештавања о уоченим одступањима?</p> <p>4) израдио и применио корективни план за отклањање уочених одступања? и</p> <p>5) израдио годишњи извештај о активностима унутрашње контроле квалитета?</p>				
<b>Област: Глава 14, Одељак 14.1. дела III Националног програма, Примена и циљ</b>				
<p>Део III, Националног програма, 14.1. Да ли је субјект, у свом програму за обезбеђивање у ваздухопловству идентификовао критичне објекте, критичну инфраструктуру, критичне информационе и комуникацијско технолошке системе и податке и предвидео мере које се односе на њихову заштиту, укључујући и заштиту од сајбер претњи у цивилном ваздухопловству?</p> <p>Ако да, да ли је осим система који су од стране надлежних органа идентификовани као критични, субјект одредио и следеће:</p> <p>1) системе и податке који могу да се идентификују као критични у погледу ваздухопловне безбедности су:</p> <ul style="list-style-type: none"> <li>- системе за управљање ваздушним саобраћајем;</li> <li>- системе за отпрему летова (DCS);</li> <li>- комуникационе, навигационе и друге безбедносно-критичне системе ваздухоплова; и</li> <li>- системе за управљање ваздухопловом, контролу и отпрему ваздухоплова;</li> </ul> <p>2) системе и податке који могу да се идентификују као критични у погледу обезбеђивања у ваздухопловству, као што су:</p> <ul style="list-style-type: none"> <li>- базе података о регулисаним агентима и/или познатим пошиљаоцима;</li> <li>- системи за контролу приступа и надзорни системи;</li> <li>- систем за видео-надзор;</li> <li>- систем за упаривање путника и пртљага; и</li> </ul>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>- опрема за обезбеђивања било да је умрежена или да се користи самостално;</p> <p>3) системе и податке који могу да се идентификују као критични у погледу олакшица у ваздушном саобраћају, као што су:</p> <ul style="list-style-type: none"> <li>- резервациони систем авио-превозиоца и системи за регистрацију путника и пртљага, робе и поште;</li> <li>- системе за приказ информација о летовима;</li> <li>- системе за сортирање и праћење предатог пртљага; и</li> <li>- систем за контролу преласка државне границе и систем који користи царина?</li> </ul> <p><b>Напомена:</b> Упутство за примену захтева обезбеђивања у ваздухопловству приликом изградње нових или реконструкције постојећих објеката на аеродрому и ван њега дато је у Прилогу III-1-Ђ Националног програма. Упутство за заштиту од сајбер претњи дато је у Прилогу III-14-A Националног програма.</p>				
<b>Област: Глава 14, Одељак 14.2. дела III Националног програма, Контроле обезбеђивања</b>				
<p>Део III, Националног програма, 14.2.1.</p> <p>Да ли субјект примењује мере заштите критичних објеката, инфраструктуре и система на основу обављене локалне процене ризика?</p> <p><b>Напомена:</b> Мере за контролу приступа критичним објектима, инфраструктури и системима су еквивалентне мерама дефинисаним у одељку 1.3. главе 1. дела III Националног програма.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<p>Део III, Националног програма, 14.2.2.1.</p> <p>Да ли пружалац услуга у ваздушној пловидби, оператери аеродрома, авио-превозиоци, пружаоци услуга земаљског опслуживања, регулисани снабдевачи залиха намењених потрошњи током лета, познати снабдевачи залиха намењених потрошњи током лета, регулисани агенти, познати пошиљаоци и стални пошиљаоци, као и снабдевачи залиха намењених потрошњи на аеродрому,</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>идентификују критичне информационе и комуникацијско-технолошке системе у ваздухопловству и податке и примењују мере заштите тих система и података од сајбер напада?</p> <p>Ако да, да ли се мерама заштите омогућава:</p> <p>1) смањење вероватноће остваривања сајбер претњи;</p> <p>2) препознавање ситуације да се догодио сајбер напад и откривање таквог напада;</p> <p>3) реаговање на сајбер напад како би се ограничиле његове последице;</p> <p>и</p> <p>4) брзи повратак система и података у стање пре напада?</p> <p><b>Напомена:</b> Мере заштите критичних информационих и комуникацијско-технолошких система у ваздухопловству и података се одређују на основу обављене процене ризика за коју је одговоран оператер аеродрома, авио превозилац или други субјект на кога се односи. Ове мере заштите морају да буду координиране и усклађене са постојећим мерама обезбеђивања у ваздухопловству и њиховом применом се чува интегритет и поверљивост података.</p>				
<p>Део III, Националног програма, 14.2.3.</p> <p>Да ли субјект, укључујући пружаоце услуга у ваздушној пловидби (ANSP), оператер аеродрома, авио-превозилац, регулисани агент, познати пошilhалац, регулисани снабдевач залиха намењених потрошњи током лета, примењује мере за идентификацију и процену ризика и одговарајућу заштиту релевантних система и података о информацијама од значаја за ваздухопловство, узимајући у обзир ризик идентификован на националном нивоу, као и ризике који се односе на организацију и пословне процесе субјекта?</p> <p><b>Напомена:</b> Успостављањем и применом одговарајућих мера за управљање ризиком обезбеђује се:</p> <p>а) ублажавање идентификованих ризика;</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>б) препознавање инцидента када се догоде; и</p> <p>в) реаговање и ограничавање последице таквог напада.</p>				
<p>Део III, Националног програма, 14.2.4.</p> <p>Да ли су мере које се примењују у циљу заштите критичних информационих и комуникацијско-технолошких система и података од неовлашћеног утицаја одређене на основу процене ризика за сваки систем појединачно, коју обавља субјект у сарадњи са Националним центром за превенцију безбедносних ризика у ИКТ системима Републике Србије (ЦЕРТ)?</p> <p>Ако да, да ли је за идентификацију претње и процену ризика од сајбер напада примењено следеће:</p> <p>1) одређивање веродостојних сценарија којима се дефинишу: мете, битни подаци (тј. критичне информације), могуће врсте напада (нпр. прекидање рада система, унос лажних података), могући починиоци (нпр. инсајдери);</p> <p>2) предвиђање најтежих могућих последица (нпр. људске и финансијске губитке, итд.);</p> <p>3) дефинисање мера за ублажавање последица од сајбер напада (нпр. физичке, процедуре, ИТ мере итд.);</p> <p>4) дефинисање осталих слабих тачака; и</p> <p>5) одређивање могућности да се такав напад успешно спроведе?</p> <p><b>Напомена:</b> Овом проценом се утврђује и процењује у којој мери ови напади олакшавају извршење других врста незаконитог ометања (нпр. ометање или онеспособљавање битних информационих система који се користе у ваздухопловству, као што је систем за контролу приступа или система за пренос података у ваздушној пловидби).</p> <p>За одређене системе и податке, процена ризика треба да се обавља узимајући у обзир постојећу методологију за процену ризика у погледу безбедности (<i>safety</i>).</p>				
<b>Област: Глава 14, Одељак 14.3. дела III Националног програма, Организација</b>				
Део III, Националног програма, 14.3.1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
Да ли је субјект успоставио успоставе систем за управљање <i>cyber</i> безбедношћу?				
Део III, Националног програма, 14.3.1.1. Да ли је субјект успоставио систем за управљање информационом безбедношћу ( <i>ISMS</i> )? Ако да, да ли је тај систем усклађен са постојећим системом управљања обезбеђивања у ваздухопловству ( <i>SeMS</i> ) и/или системом управљања безбедношћу ( <i>SMS</i> )?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.3.1.2. Да ли је субјект одредио руководиоца као одговорног лица за <i>ISMS</i> ? Ако да, да ли тај руководиоца има одговарајућу обуку у вези са заштитом од сајбер претњи?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.3.1.3. Да ли је субјект успоставио координацију између лица одговорног за информациону безбедност и именованог руководиоца за обезбеђивање у ваздухопловству, односно <i>safety manager</i> -а? <b>Напомена:</b> Различите организационе јединице субјекта ( <i>IT</i> , оперативне делатности, обезбеђивање у ваздухопловству, ваздухопловна безбедност ( <i>safety</i> ), набавке, центар за обуку итд.) треба да имају координацију у вези са <i>cyber</i> безбедношћу. Одговарајуће мере треба да буду искоординисане и у складу са постојећим мерама обезбеђивања у ваздухопловству, као и мерама безбедности ( <i>safety</i> ).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли је субјект одредио лице за везу са релевантним државним органима и субјектима који се баве <i>cyber</i> безбедношћу?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<b>Област: Глава 14, Одељак 14.4. дела III Националног програма, Култура у везиса <i>cyber</i> безбедношћу</b>				
Део III, Националног програма, 14.4. Да ли је субјект обезбедио довољно ресурса како би се успоставила, применила и одржавала на одговарајућем нивоу култура у вези <i>cyber</i> безбедности, односно како би се обезбедило да су послови у вези	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>са <i>cyber</i> безбедношћу поверени лицу које поседује одговарајуће знање и искуство како у области ваздухопловства, тако и у области <i>cyber</i> безбедности?</p> <p>Ако да, да ли је на основу „потребе да знају“ сво особље и ангажована трећа лица упознато са релевантним ризицима у вези <i>cyber</i> безбедности?</p> <p><b>Напомена:</b> Обука у вези са заштитом од електронских претњи треба да се спроведе за особље и ангажована трећа лица која имају приступ подацима или системима за које постоји процена да су критични за безбедно и обезбеђивано одвијање посла.</p>				
<b>Област: Глава 14, Одељак 14.5. дела III Националног програма, Мере обезбеђивања</b>				
<p>Део III, Националног програма, 14.5.1.</p> <p>Да ли су мреже које се користе за критичне системе и податке у ваздухопловству издвојене од мрежа које су доступне јавности?</p> <p><b>Напомена:</b> Када критични системи у ваздухопловству морају да се повежу на друге оперативне системе, ове везе треба смањити на минимум. Ако издвајање није могуће, везе и приступ морају да буду све време да буду заштићени од мрежа којима је приступ слободан.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<p>Део III, Националног програма, 14.5.2.</p> <p>Да ли су оператер аеродрома, авио-превозилац и остали субјекти, одредили одговорно лице за заштиту критичних система у ваздухопловству?</p> <p>Ако да, да ли је обезбеђено да су та лица одговарајуће одабрана и оспособљена?</p> <p><b>Напомена:</b> Мере заштите критичних система у ваздухопловству морају да буду координисане и усклађене са постојећим мерама за обезбеђивање у ваздухопловству.</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<p>Да ли су лица која су одговорна за набавку, заштиту и одржавање критичних система и њихових делова, осим обуке прописане у пододељку 11.3.6 главе 11. дела III Националног програма, завршила и одговарајућу обуку у вези заштите од сајбер претњи?</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
Да ли је за сва лица која имају приступ критичној инфраструктури, системима или подацима и/или обављају послове у вези са заштитом тих система и/или имају администраторска права за приступ критичној ИТ инфраструктури субјекта, обављена безбедносна провера?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.5.3. Да ли субјекти примењују мере обезбеђивања које одговарају концепцији, имплементацији, начину рада и размештају критичног система у ваздухопловству? <b>Напомена:</b> Приликом измена постојећих критичних система у ваздухопловству морају се у највећој могућој мери узети у обзир мере обезбеђивања у ваздухопловству?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.5.4. Да ли су субјекти предузели одговарајуће мере заштите података и ланца снабдевања уређајима (хардвер) и рачунарским програмима (софтвер) који се користе за рад критичних система у ваздухопловству, односно за рад са подацима од значаја за ваздухопловство? <b>Напомена:</b> Приликом прибављања таквих система субјекти морају да захтевају детаљне податке о мерама обезбеђивања које примењују потенцијални снабдевачи.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.5.5. Да ли је приступ критичним системима и подацима контролисан у сваком тренутку и ограничен само на особље са оперативним потребама? <b>Напомена:</b> Ово се односи и на сва лица ангажована уговором. Субјектима се допушта коришћење даљинске контроле приступа битним подацима и критичним системима у ваздухопловству, под унапред уређеним и безбедним условима.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли субјект спречава да снабдевачи неовлашћено приступе овим системима након што су их испоручили?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	



ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
Део III, Националног програма, 14.5.6. Да ли су инциденти који се односе на сајбер нападе, а који могу да имају утицај на ваздухопловну безбедност и на обезбеђивање у ваздухопловству пријављују и анализирају?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли субјекти надгледају све ICT системе, сав мрежни саобраћај и све кориснике како би идентификовали необичне активности и неовлашћени приступ који би могли да укажу да се планира или да је започет сајбер напад?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли се одговор сајбер инциденте укључује у свеобухватно реаговање у кризним ситуацијама и управљање кризном ситуацијом?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли се инциденти пријављују Директорату?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.5.7. Да ли субјекти евидентирају и анализирају инциденте који су последица сајбер напада и обезбеђују процену ризика и одговарајући одговор на ове инциденте? <b>Напомена:</b> Субјекти су дужни да о оваквим инцидентима извештавају Директорат, сходно пропису о пријављивању догађаја у цивилном ваздухопловству.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма, 14.5.8. Да ли се ISMS сваког субјекта заснива и спроводи према прихваћеним стандардима и смерницама? <b>Напомена:</b> Ово треба да се потврди независном сертификацијом или интерном сертификацијом према стандардима за сертификацију.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Да ли се процесом набавке услуга које се пружају од стране трећих лица или процес набавке производа, који су проценом ризика оцењени као услуге и производи од највећег значаја за безбедно и обезбеђивано обављање послова, обезбеђује да пружене услуге и набављени производи имају одговарајућу заштиту од сајбер претњи?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Део III, Националног програма,	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

ПИТАЊА	ДА	НЕ	Н/П	КОМЕНТАР
<p>14.5.9.  Да ли субјект са осталим субјектима размењује информације у вези са ризицима који се односе на <i>cyber</i> безбедност?</p> <p><b>Напомена:</b> ова размена укључује размену информација о уобичајеним или заједничким ризицима, методама и резултатима процене ризика, плановима поступања у односу на процењени ризик, информација о инцидентима и slabим тачкама, као и информација о резултатима <i>cyber</i> обезбеђења. Ова размена информација треба да се врши само са поузданим партнерима, при чему се примењују прописи о тајности података.</p>				

**Напомена:**

Надзирани субјект/  
Присутно лице:

Инспектор: