РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

Број:
Деловодни број:
Датум:
Београд

И З В Е Ш Т А Ј
о резултатима спроведених јавних консултација о Нацрту правилника о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја

На основу члана 37. Закона о електронским комуникацијама („Службени гласник РС”, број 35/23, у даљем тексту: ЗЕК), Регулаторно тело за електронске комуникације и поштанске услуге (у даљем тексту: Регулатор), објављује Извештај о резултатима спроведених јавних консултација о Нацрту правилника о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја, (у даљем тексту: Нацрт правилника).

Доношење наведеног правилника иницирано је доношењем Закона о информационој безбедности („Службени гласник РС”, број 91/25, у даљем тексту: Закон), који је Народна скупштина Републике Србије донела дана 22. октобра 2025. године и који је ступио на снагу 31. октобра 2025. године.

Регулатор је припремио Нацрт правилника и у складу са чл. 36. и 37. ЗЕК-а, спровео јавне консултације у периоду од 29. априла до 29. маја 2026. године, како би све заинтересоване стране биле благовремено и правилно информисане о предложеним решењима, чиме би се омогућило да дају свој допринос даљем унапређењу предложених решења.

Текст Нацрта правилника објављен је на званичној веб презентацији Регулатора https://www.ratel.rs/cyr/blog-posts-view-all/javne-konsultacije-o-nacrtu-pravilnika-o-opstoj-metodologiji-za-procenu-rizika-u-informaciono-komunikacionim-sistemima-od-posebnog-znacaja као и на порталу Е-консултације, а сва заинтересована лица била су у могућности да своја мишљења о предмету јавне консултације доставе у писаном или електронском облику.

Као резултат спроведених јавних консултација, Регулатору је доставио мишљење: CETIN d.o.o. Beograd - Novi Beograd (у даљем тексту: CETIN), Национална алијанса за локални економски развој (у даљем тексту: НАЛЕД), Foreign Investors Council (у даљем тексту: FIC) и A1 Srbija d.o.o. Beograd (у даљем тексту: A1).

У наставку Регулатор даје одговоре на достављена мишљења.

Мишљење учесника јавних консултација – CETIN, НАЛЕД, FIC:	**Одговор Регулатора:**
На Нацрт Правилника	
Имајући у виду члан 1. став 4. члан 54. став 1. и члан 55. став 4. Закона о информационој безбедности, предлажемо да документ не буде подзаконски акт, већ смернице о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја.	***Примедба је размотрена и предлог се не прихвата.*** Одредбама члана 53. Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 99/14, 30/18 – др. закон и 47/18), регулисано је доношење прописа ималаца јавних овлашћења и то тако да када им је исто поверено, они по природи и **називу** морају да одговарају прописима које доносе органи државне управе, а пропис чије им је доношење поверено имаоци јавних

	овлашћења дужни су да објаве у „Службеном гласнику Републике Србије“. Прописи које доносе органи државне управе су, сагласно одредбама члана 15. наведеног закона, правилници, наредбе и упутства. Такође, одредбом члана 8. став 6. ЗЕК-а, прописано је да се, између осталог, у погледу законитости рада Регулатора примењују прописи везани за државну управу. Имајући у виду да су Законом прописане казнене одредбе за недоношење Акта о процени ризика из члана 11.став 1. Закона, као и да се исти сагласно одредби члана 11.став 4. Закона израђује у складу са општом методологијом за процену ризика у приоритетним и важним ИКТ системима од посебног значаја коју доноси орган, односно организација у којој се обављају послови Националног ЦЕРТ-а, неспорно је да, сагласно закону, општа методологија не може имати саветодавни, нити дискрециони, нити алтернативни, нити упућујући, већ правно обавезујући карактер, јер је и сама подзаконски акт, па је треба донети у форми правилника.
А1:	
Предлажемо да се члан 3. Нацрта правилника преформулише тако да гласи: „Процена ризика обухвата идентификацију претњи, рањивости и могућих инцидената, односно сценарија ризика. Идентификација претњи заснива се на Каталогу претњи информационе безбедности из Прилога 2, док се рањивости и могући инциденти документују у односу на конкретне ресурсе, пословне процесе, постојеће мере заштите и контекст оператора“	**Примедба је размотрена и предлог се делимично прихвата.** **Члан 3. сада гласи:** „Процена ризика у ИКТ системима од посебног значаја обухвата идентификацију претњи, рањивости и могућих инцидената. Идентификација претњи заснива се на Каталогу претњи информационе безбедности, који је дат у Прилогу 2. овог правилника и чини његов саставни део, док се рањивости и могући инциденти документују у односу на конкретне ресурсе, пословне процесе и постојеће мере заштите.“ Појашњење: Члан 3. правилника прецизиран је тако да јасно разграничи да се идентификација претњи заснива на Каталогу претњи, док се рањивости и могући инциденти документују у односу на конкретне ресурсе, пословне процесе и постојеће мере заштите. Одговарајућа измена унета је и у општу методологију у одељку о анализи утицаја претњи. Термин „сценарија ризика“ није преузет у правилник јер детаљнија методолошка разрада овог концепта спада у општу методологију, а не у сам текст правилника.

На Општу методологију за процену ризика (у даљем тексту: Методологија) CETIN, НАЛЕД, FIC:	
Брисање делова 4.1.1. Опис система и 4.1.2. Опис информационих система	**Примедба је размотрена и предлог се не прихвата.** Поглавља 4.1.1 и 4.1.2 задржавају се у Методологији јер пружају важан оквир за спровођење процене ризика, посебно за операторе ИКТ систем од посебног значаја који процену ризика спроводе по први пут и којима је потребан структурисан приступ идентификацији система и ресурса као полазне тачке за процену. Елементи описа система су оријентациони и оператор ИКТ система од посебног значаја их прилагођава обиму и специфичностима своје процене. Регулатор се слаже ставом да ови подаци треба да постоје на нивоу система независно од процеса процене ризика стога оба поглавља могу постојати као засебни документи, Методологија их тако и дефинише.
Предлажемо да се термин „вероватноћа догађања“ замени термином „вероватноћа материјализације ризика“ или „вероватноћа остварења ризика“, зато што су ови изрази прецизнији и стручно правилнији у контексту управљања ризицима.	**Примедба је размотрена и предлог се не прихвата.** Термин „вероватноћа догађања“ представља усвојени превод из српског стандарда SRPS ISO/IEC 27005:2017. Методологија користи терминологију усклађену са важећим српским преводом стандарда ради конзистентности са референтним документима на српском језику и избегавања терминолошке конфузије код оператора ИКТ система од посебног значаја.
CETIN, НАЛЕД:	
Предлажемо да се ниво ризика не везује за рок реализације на начин како је наведено, већ да за сваки идентификовани ризик постоји посебна одлука о начину његовог адресирања, у којој ће бити дефинисан и рок за реализацију те одлуке.	**Примедба је размотрена и предлог се прихвата.** Временски оквири наведени у Табели 9 представљају препоручене оквире за доношење одлуке о начину поступања са ризиком, а не обавезујуће рокове за реализацију мера. Усваја се предлог да рок за реализацију мера буде саставни део одлуке о поступању са ризиком, узимајући у обзир расположиве капацитете и ресурсе оператора. У тексту испод Табеле 9 је унета одговарајућа измена.
FIC:	
У табели 1: Регистар ресурса, сматрамо да је потребно додати колону „Значај/Критичност“ и ускладити са тачком 5.2. Регистра ресурса, где је наведено: „Регистар ресурса са најмање следећим подацима: назив, категорија, власник и процена вредности по CIA триади“.	**Примедба је размотрена и предлог се прихвата.** Табела 1 допуњује се колоном „Критичност“ уместо колоне „Остало“, а у одељку 4.2 додата је одговарајућа дефиниција овог елемента, а тачка 5.2 усклађена је са овом изменом. Методологија не прописује обавезне нивое критичности ресурса, оператор ИКТ система од посебног значаја их одређује у складу са специфичностима свог пословања и потребама.

У поглављу 2, дефиниција инцидента је следећа: „Сваки догађај или скуп догађаја који угрожавају или ће вероватно угрозити доступност, интегритет и/или поверљивост података који се чувају, преносе или обрађују, или услуга које се пружају или стављају на располагање путем ИКТ система.“	**Примедба је размотрена и предлог се не прихвата.** Дефиниција инцидента прописна је чланом 2. став 1. тачка 15) Закона о информационој безбедности.
Увести обавезу формалног именовања власника методологије процене ризика и функције одговорне за независну проверу квалитета процене.	**Примедба је размотрена и предлог се не прихвата.** Методологија не прописује начин унутрашњег организовања процеса процене ризика јер се оператори ИКТ система од посебног значаја значајно разликују по величини, зрелости и организационој структури. Одговорност за квалитет процене ризика јасно је успостављена на нивоу руководства оператора ИКТ система од посебног значаја, у складу са чланом 11. Закона. Раздвајање оперативне и контролне функције представља добру праксу коју оператори ИКТ система од посебног значаја могу самостално успоставити, али прописивање ове обавезе на нивоу опште методологије не би било примерено за све категорије оператора ИКТ система од посебног значаја.
Додати обавезу експлицитног дефинисања критичних пословних функција *(critical business services)* и мапирање на ИКТ системе.	**Примедба је размотрена и предлог се не прихвата.** Методологија у одељку 1.1 већ захтева опис главних пословних циљева и процеса, чиме је веза између пословних функција и ИКТ система успостављена у мери неопходној за спровођење процене ризика. Формално дефинисање критичних пословних функција и њихово мапирање на ИКТ системе превазилази обим процене ризика и ближе је домену управљања континуитетом пословања, које ће бити уређено засебним подзаконским актом о мерама заштите.
Увести обавезу документовања извора претњи (*threat intelligence*), укључујући интерне и екстерне изворе (CERT, ISAC, vendor advisories).	**Примедба је размотрена и предлог се не прихвата.** Методологија предвиђа да оператор ИКТ система од посебног значаја може допунити Каталог претњи претњама специфичним за његов контекст, укључујући и оне идентификоване кроз актуелне изворе информација о претњама. Увођење обавезног документовања конкретних извора претњи превазилази обим опште методологије намењене широком кругу оператора ИКТ система од посебног значаја различите зрелости и капацитета. Праћење актуелних информација о претњама представља меру заштите прописану чланом 10 став 4. тачка 19)

	Закона, те ће бити детаљније уређено подзаконским актом о мерама заштите.
Предлажемо измену назива тачке 4.4.4. „Одређивање прихватљивог ризика“ тако да гласи: „Одређивање прихватљивог нивоа ризика“.	**Примедба је размотрена и предлог се не прихвата.** Термин „прихватљиви ризик“ у контексту тачке 4.4.4 усклађен је са терминологијом ISO 31000:2018 и ISO/IEC 27005:2022 где се користи термин „*risk acceptance“* као одређивање нивоа ризика који је организација спремна да прихвати. Предложена измена не би унела суштинску прецизност већ би одступила од усвојене стандардне терминологије.
Предлаже се допуна Табеле 7 додатним пољима за опис сценарија ризика, инхерентни и преостали ризик, власника ризика и статус имплементације мере	**Примедба је размотрена и предлог се не прихвата.** Табела 7 већ садржи колоне за власника ризика и поступање са ризиком. Раздвајање инхерентног ризика (Табела 7) и преосталог ризика (Табела 8) је решење које прати ISO/IEC 27005:2022 и обезбеђује јасну документацију ефикасности примењених мера заштите. Статус имплементације мере спада у домен праћења ризика, а не процене. Методологија не уводи опис сценарија ризика јер примењује процену ризика засновану на средствима.
Увести обавезу формалног одобравања прихватања ризика на адекватном нивоу управљања (нпр. *executive/board* за високе ризике).	**Примедба је размотрена и предлог се не прихвата.** Методологија јасно дефинише да је доношење акта о процени ризика одговорност органа управљања оператора ИКТ система од посебног значаја, чиме је одговорност за одлуке о поступању са ризицима, укључујући прихватање високих ризика, успостављена на највишем нивоу. Прописивање конкретних нивоа одлучивања у зависности од нивоа ризика превазилази обим опште методологије.
У тачки 4.5.5. наводи се да оператор ИКТ система од посебног значаја треба да утврди временски оквир за доношење одлуке о начину поступања са ризиком у односу на ниво озбиљности (Табела 9). Сматрамо да је потребно редефинисати тако да се временски оквир односи на рок за примену мере, а не на рок за доношење одлуке. Додатно, предлажемо да се ниво ризика не везује аутоматски за рок реализације мера на начин како је тренутно наведено, већ да за сваки идентификовани ризик постоји посебна одлука о начину његовог адресирања, у оквиру које ће бити дефинисан примерен рок за спровођење мера.	**Примедба је размотрена и предлог се делимично прихвата.** Временски оквири у Табели 9 задржавају се као препоручени оквири за доношење одлуке о поступању са ризиком јер обезбеђују минималну хитност реаговања у складу са нивоом озбиљности ризика. Усваја се предлог да рок за реализацију мера не произлази аутоматски из нивоа ризика, већ да буде саставни део одлуке о поступању са ризиком, узимајући у обзир расположиве капацитете и ресурсе оператора ИКТ система од посебног значаја. Одговарајућа измена унета је у Методологију испод Табеле 9.
У тачки 4.6 наводи се да се преиспитивање ризика спроводи једном годишње.	**Примедба је размотрена и предлог се не прихвата.**

Предлажемо да се размотри смањење периода на квартално или полугодишње.	Годишња ревизија представља минималну учесталост у складу са Законом о информационој безбедности и ISO/IEC 27005:2022, оператори ИКТ система од посебног значаја могу самостално одлучити да врше ревизију чешће у складу са својим потребама и проценом ризика. Методологија, такође, предвиђа обавезну ванредну ревизију у случају значајних промена у претњама, рањивостима, технолошком или организационом окружењу, чиме је обезбеђена правовремена реакција без прописивања додатног административног терета за све операторе ИКТ система од посебног значаја.
Предлаже се допуна тачке на следећи начин (означено црвеном): Документована идентификација претњи релевантних за ресурсе у опсегу процене, са назнаком извора претње и циљаног ресурса. Оператор ИКТ система од посебног значаја може користити сопствени каталог претњи уколико покрива исте основне категорије претњи као Каталог претњи из ове методологије. Евиденција релевантних претњи које су процењене да имају утицај на ресурс може се водити и у оквиру финалног регистра ризика.	**Примедба је размотрена и предлог се не прихвата.** Тачка 5.3 не прописује засебан документ за евиденцију претњи, већ само документовану идентификацију претњи релевантних за ресурсе у опсегу процене. Оператор ИКТ система од посебног значаја је слободан да ту евиденцију интегрише у регистар ризика или у засебан документ у складу са својим потребама, те сматрамо да нема потребе за додатно прецизирање у Методологији.
Предлог да се тачка 5.7. измени тако да гласи: „Закон о заштити података о личности заснива се на претпоставци да је увек јасно где се налазе подаци о личности, ко их обрађује и ко је одговоран за њихову обраду. Коришћење дистрибуираних и географски дислоцираних ИКТ окружења може отежати идентификацију стварне локације где се подаци о личности обрађују, као и разграничење улога учесника обраде података, утврђивање применљивог права и надлежност регулаторних органа за заштиту података о личности. Пренос података о личности у друге државе, односно омогућавање права приступа лицима ван територије Републике Србије може довести до ризика неусклађености са прописима из области	**Примедба је размотрена и предлог се не прихвата.** Тренутни опис претње 5.7 конзистентан је са нивоом општости примењеним у свим осталим претњама у Каталогу претњи. Детаљна разрада ризика везаних за прекогранични пренос података о личности и примену ЗоЗПЛ превазилази Каталога претњи и спада у домен усклађености са прописима који регулишу заштиту података о личности.

заштите података о личности – законитост преноса (да ли постоји примерени ниво заштите државе у коју се преносе подаци о личности), примена одговарајућих мера заштите, остваривања права лица чији се подаци обрађују и др.“	
А1:	
У Прилогу 1. – Општа методологија за процену ризика у ИКТ системима од посебног значаја, у глави 1. Увод, потребно је детаљније дефинисати део који се односи на поверљивост Акта о процени ризика, односно „да се он може давати искључиво на увид лицима која су законом овлашћена да га захтевају, без могућности достављања или прослеђивања ван оператора ИКТ система од посебног значаја“. Ради отклањања недоумица у пракси приликом примене, потребно је изричито дефинисати, да ли при изради Акта о процени ризика искључиво лица запослена у Оператору ИКТ система од посебног значаја врше израду овог документа, или је могуће да у његовој изради учествују и нека трећа лица нпр. добављач (*vendor*), и ако је потврдан одговор, да ли постоје неки услови приликом ангажовања таквог лица које је неопходно испунити у циљу заштите поверљивости приликом израде Акта о процени ризика.	**Примедба је размотрена и предлог се не прихвата.** Питање ангажовања трећих лица у активностима у вези са ИКТ системом од посебног значаја, укључујући израду акта о процени ризика, уређено је чланом 7. став 1. тачка 6) Закона, којим је прописана обавеза оператора ИКТ система од посебног значаја да уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите ИКТ система у складу са законом, уколико им поверава активности у вези са ИКТ системом од посебног значаја. Детаљније уређивање овог питања у оквиру опште методологије за процену ризика превазилазило би оквир подзаконског акта.