ДРУГИ ДРЖАВНИ ОРГАНИ И ДРЖАВНЕ ОРГАНИЗАЦИЈЕ

2746

На основу члана 196. и члана 241. став 1. тачка 1) Закона о здравственом осигурању („Службени гласник РС”, бр. 25/19, 92/23 и 109/25 – др. закон) и члана 17. став 2. Статута Републичког фонда за здравствено осигурање („Службени гласник РС”, бр. 57/23 и 46/26),

Управни одбор Републичког фонда за здравствено осигурање, на седници одржаној 30. јуна 2026. године, донео је

ПРАВИЛНИК

о допуни Правилника о ценама здравствених услуга на секундарном и терцијарном нивоу здравствене заштите

Члан 1.

У Правилнику о ценама здравствених услуга на секундарном и терцијарном нивоу здравствене заштите („Службени гласник РС”, бр. 88/21, 97/21, 109/21, 132/21, 47/22, 82/22, 123/22, 128/22, 1/23, 59/23, 96/23, 15/24, 13/25 и 41/26) у Прилогу 1. после услуге под шифром „90595-00”, додаје се нова услуга, која гласи:

„

Шифра услуге	Назив услуге	Цена
50124-011	Интраартикуларна апликација фиксне комбинације плазме обогаћене тромбоцитима и хијалуронске киселине у лечењу гонартрозе	27.596,26

”.

Члан 2.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

30-01/2 број 020-187/2026
У Београду, 30. јуна 2026. године

Управни одбор
Републичког фонда за здравствено осигурање

Заменик председника,
Александра Потпаревић, с.р.

2747

На основу члана 11. став 4. Закона о информационој безбедности („Службени гласник РС”, број 91/25),

Савет Регулаторног тела за електронске комуникације и поштанске услуге, на 60. седници четвртог сазива одржаној 24. јуна 2026. године, доноси

ПРАВИЛНИК

о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја

Члан 1.

Овим правилником утврђује се општа методологија за процену ризика у приоритетним и важним информационо-комуникационим системима од посебног значаја (у даљем тексту: ИКТ системи од посебног значаја).

Члан 2.

Акт о процени ризика ИКТ система од посебног значаја израђује се у складу са општом методологијом за процену ризика, која је дата је у Прилогу 1. овог правилника и чини његов саставни део.

Актом о процени ризика из става 1. овог члана врши се процена ризика у ИКТ системима од посебног значаја с обзиром на степен изложености ризику, величину оператора ИКТ система од посебног значаја и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај.

Члан 3.

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.

Члан 4.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

Број 001970499 2026 59011 005 000 012 005 04 002
У Београду, 24. јуна 2026. године

Председник Савета,
Драган Ковачевић, с.р.

ПРИЛОГ 1.

ОПШТА МЕТОДОЛОГИЈА ЗА ПРОЦЕНУ РИЗИКА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

1. Увод

Општа методологија за процену ризика у приоритетним и важним ИКТ системима од посебног значаја (у даљем тексту: методологија) представља оквир за спровођење обавезе процене ризика прописане Законом о информационој безбедности („Службени гласник РС”, број 91/25, (у даљем тексту: ЗИБ)). У складу са Законом оператори ИКТ система од посебног значаја дужни су да донесу Акт о процени ризика за ИКТ системе (у даљем тексту: акт о процени ризика) израђен у складу са овом методологијом. Методологија обезбеђује јединствен и стандардизован приступ процени ризика и примењује се као основни методолошки оквир, а посебно је намењена операторима ИКТ система од посебног значаја који немају интерним актом уређену процену ризика. Заснива се на ITSRM методологији Европске комисије (одлука Комисије (EU, Euratom) 2017/46 од 10. јануара 2017. године о сигурности комуникационих и информационих система у Европској комисији), ENISA „*Interoperable EU Risk Management Toolbox”* и међународним стандардима NIST SP 800-30 Rev.1 и ISO/IEC 27005:2022. Примена методологије има за циљ правовремено и ефикасно доношење одлука о примени мера заштите, као и смањење ризика и последица безбедносних инцидената.

Ова методологија представља смернице за спровођење процене ризика у ИКТ системима од посебног значаја. Операторима ИКТ система од посебног значаја, који већ имају успостављену процену ризика засновану на сценаријима, процесима или другом методолошком приступу, она служи као референтни оквир за проверу усклађености, а не као обавеза за поновно спровођење процене. Услови усклађености постојеће процене са захтевима ове методологије детаљније су дефинисани у тачки 5. методологије.

Акт о процени ризика обезбеђује систематску идентификацију, анализу и процену ризика по информациону безбедност ИКТ система, у складу са законом, узимајући у обзир степен изложености ризику, величину и значај оператора, вероватноћу и озбиљност безбедносних инцидената, као и њихов потенцијални друштвени и економски утицај. На основу овог акта доноси се акт