



**Република Србија**  
**КАНЦЕЛАРИЈА ЗА ИНФОРМАЦИОНЕ**  
**ТЕХНОЛОГИЈЕ И ЕЛЕКТРОНСКУ УПРАВУ**

Број: 003579252 2024 10258 005 000 011 001

Датум: 06. април 2026. године

**ПЛАН СТРУЧНОГ НАДЗОРА ЗА 2026. ГОДИНУ**  
**над применом Закона о информационој безбедности**  
**и радом оператора ИКТ система од посебног значаја одређених Законом**

**1. УВОД**

Годишњи план стручног надзора за 2026. годину Канцеларије за информационе технологије и електронску управу донет је у складу са чланом 10. Закона о инспекцијском надзору („Службени гласник РС”, бр. 36/15, 44/18-др. закон и 95/18).

Стручни надзор над применом Закона о информационој безбедности ("Службени гласник РС", бр. 91/25, у даљем тексту: ЗИБ), и радом оператора ИКТ система од посебног значаја одређених ЗИБ-ом, до 1. јануара 2027. године врше овлашћена лица Канцеларије за информационе технологије и електронску управу, сагласно овлашћењима утврђеним чл. 49. и чл. 56. ЗИБ-а.

У Канцеларији за информационе технологије и електронску управу, овлашћена су два (2) државна службеника, у својству лица за обављање стручног надзора над применом прописа у области информационе безбедности и радом оператора ИКТ система од посебног значаја одређених ЗИБ-ом.

Годишњи план стручног надзора доноси се на основу прикупљених података и праћења и анализирања стања из свог делокруга и процењеног ризика, и исти ће бити спроведен кроз оперативне (шестомесечне, тромесечне и месечне) планове стручног надзора.

**2. ОБЛИЦИ СТРУЧНОГ НАДЗОРА**

**Теренски и канцеларијски стручни надзор**

Теренски стручни надзор се врши изван службених просторија Канцеларије за информационе технологије и електронску управу, непосредним увидом у објекте, просторије, уређаје и друге предмете, акте и документацију надзираног субјекта, као и узимањем писаних и усмених изјава од одговорних лица и сведока о питањима која су од значаја за утврђивање чињеничног стања.

Канцеларијски стручни надзор се врши у службеним просторијама Канцеларије за информационе технологије и електронску управу, увидом у пословне књиге и другу документацију надзираног субјекта која се односи на обављање послова који су предмет

стручног надзора, као и увидом у податке о надзираном субјекту прибављене по службеној дужности.

### 3. ВРСТЕ СТРУЧНОГ НАДЗОРА

#### Редован, ванредан и контролни стручни надзор

Овлашћена лица Канцеларије за информационе технологије и електронску управу ће, према планираним активностима, у 2026. години вршити редован стручни надзор, ванредне стручне надзоре, као и контролне стручне надзоре у циљу утврђивања извршења мера наложених или предложених у поступку редовног или ванредног стручног надзора.

### 4. НАДЗИРАНИ СУБЈЕКТИ И УЧЕСТАЛОСТ ВРШЕЊА СТРУЧНОГ НАДЗОРА

Надзирани субјекти су оператори ИКТ система од посебног значаја одређени ЗИБ-ом, односно, оператори ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима.

Стручни надзори ће се вршити како у седишту, тако и у пословним јединицама надзираних субјеката.

Редовни стручни надзори ће се вршити код оних оператора ИКТ система од посебног значаја одређених ЗИБ-ом који су на основу делатности које обављају процењени као приоритетни и важни и у којима је због тога потребно успоставити и одржавати адекватан ниво информационе безбедности.

Ванредни стручни надзори ће се вршити као приоритетни, уколико се оцени да се хитно морају предузимати одређене мере и уколико се дође до сазнања о постојању незаконитости.

После сваког поступка редовног или ванредног стручног надзора, који је окончан налагањем или предлагањем одређених мера, врши се контролни стручни надзор, којим се утврђује извршење мера наложених или предложених у поступку редовног или ванредног стручног надзора.

### 5. ПРЕДМЕТ СТРУЧНОГ НАДЗОРА

У складу са датим овлашћењима, лица овлашћена за стручни надзор над применом прописа у области информационе безбедности и радом оператора ИКТ система од посебног значаја одређених ЗИБ-ом, ће приликом редовних, односно ванредних надзора, утврђивати и контролисати следеће:

1. адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај;
2. ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите;
3. да ли је извршена годишња провера усклађености примењених мера заштите;

4. адекватност спровођења процеса провере усклађености примењених мера ИКТ система са актом о безбедности;
5. да ли се примењују препоруке и мере у случају инцидената који значајно угрожавају информациону безбедност.

## 6. УЧЕСТАЛОСТ ВРШЕЊА СТРУЧНОГ НАДЗОРА И НАДЗИРАНИ СУБЈЕКТИ

Годишњим планом стручног надзора за 2026. годину обухваћене су следеће активности овлашћених лица, односно редовни стручни надзори и студијске посете код надзираних субјеката, и то по кварталима:

Р.Б.	Надзирани субјект	Степен ризика
<b>I квартал</b>		
-	-	-
<b>II квартал</b>		
1.	Министарство информисања и телекомуникација	Средњи
2.	Министарство рударства и енергетике	Средњи
<b>III квартал</b>		
1.	Републички сеизмолошки завод	Средњи
2.	Управа за заједничке послове републичких органа	Средњи
3.	Републички хидрометеоролошки завод	Средњи
4.	Градска општина Чукарица	Средњи
<b>IV квартал</b>		
1.	Министарство туризма и омладине	Средњи
2.	Министарство за људска и мањинска права и друштвени дијалог	Средњи
3.	Национална академија за јавну управу	Средњи
4.	Градска општина Обреновац	Средњи

## 7. МЕРЕ СТРУЧНОГ НАДЗОРА

Овлашћено лице Канцеларије за информационе технологије и електронску управу ће, у зависности од утврђеног стања у поступку стручног надзора, а сходно овлашћењима утврђеним законом, наложити отклањање утврђених неправилности, недостатака или пропуста у примени прописа у области информационе безбедности, о томе обавестити надзираног субјекта и одредити му рок у коме је дужан да их отклони.

Рок за отклањање утврђених неправилности, недостатака или пропуста не може бити краћи од осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање.

Ако овлашћено лице утврди да надзирани субјекат није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте, поднеће пријаву инспекцији.

## 8. ПРЕВЕНТИВНО ДЕЛОВАЊЕ

Превентивно деловање биће остварено објављивањем контролних листа и планова стручног надзора, као и организовањем службених саветодавних посета и других активности усмерених ка подстицању и подржавању законитости и безбедности поступања у области информационе безбедности.