



JAVNO  
JASNO  
EFIKASNO  
Projekat za dobru upravu

# Инспекција за информациону безбедност

Аутори: Марија Поповић и Александар Богдановић, Министарство информисања и телекомуникација

Април 2024. године.



Република Србија  
Министарство информисања  
и телекомуникација

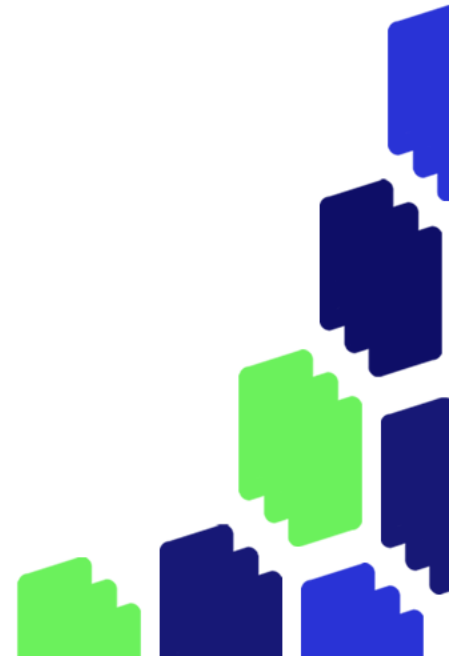
# ЗАКОН И ПОДЗАКОНСКИ АКТИ

- Закон о информационој безбедности: 6/2016-50, 94/2017-9, 77/2019-16;
- Уредба о ближем садржају акта о безбедности ИКТ од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја („Службени гласник РС”, број 94/16);
- Уредба о ближем уређењу мера заштите ИКТ система од посебног значаја („Службени гласник РС”, број 94/16);
- Уредба о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја: 94/2019-51;
- КОНТРОЛНА ЛИСТА 01-Контрола ИКТ система од посебног значаја Закон о информационој безбедности и прописи донети на основу њега.



# Надлежни орган за информациону безбедност

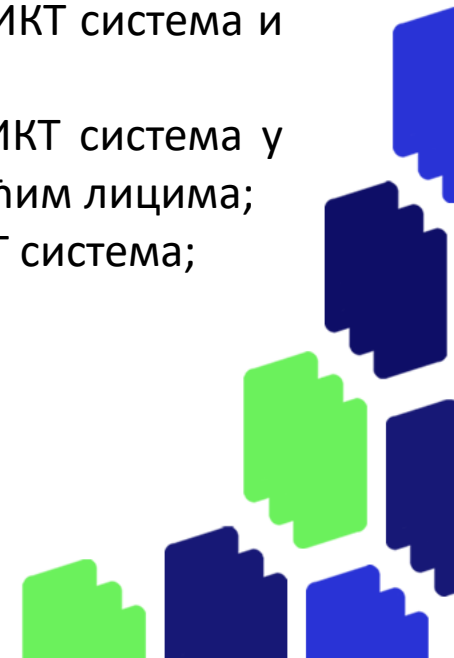
- Припрема подзаконске акте којима се извршава Закон о информационој безбедности;
- Обавља међународну сарадњу у области безбедности ИКТ система, а посебно пружа информације о ризицима и инцидентима који могу да имају међународни карактер;
- Врши надзор над радом Националног ЦЕРТ-а ;
- Врши инспекцијски надзор над применом закона;
- Успоставља и води евиденцију ИКТ система од посебног значаја;
- Предузима превентивне мере за безбедност и заштиту деце на интернету.



# Обавезе оператора ИКТ система од посебног значаја

Оператор ИКТ система је у обавези да:

- 1) упише ИКТ систем од посебног значаја којим управља у **евиденцију** оператора ИКТ система од посебног значаја;
- 2) предузме **мере заштите** ИКТ система од посебног значаја;
- 3) донесе **акт о безбедности** ИКТ система;
- 4) врши **проверу усклађености примењених мера** заштите ИКТ система са актом о безбедности ИКТ система и то најмање **једном годишње**;
- 5) **уреди однос** са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима;
- 6) доставља обавештења о **инцидентима** који значајно угрожавају информациону безбедност ИКТ система;
- 7) достави тачне **статистичке податке о инцидентима** у ИКТ систему.



# Контрола ИКТ система од посебног значаја КЛ-001-03/09

Питања у контролној листи:

Да ли је донет Акт о безбедности?

Да ли је Акт о безбедности донет у складу са постојећим прописима?

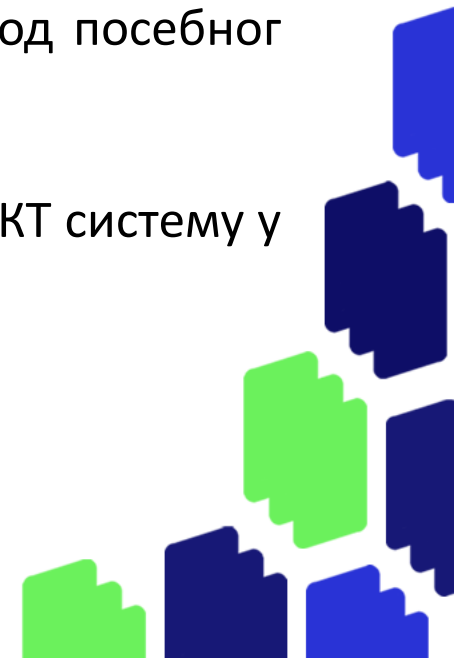
Да ли су примењене мере заштите?

Да ли је извршена годишња провера усклађености примењених мера заштите?

Да ли је у складу са прописима сачињен извештај о годишњој провери ИКТ система од посебног значаја?

Да ли је извршен упис у Евиденцију оператора ИКТ система од посебног значаја?

Да ли су Националном ЦЕРТ-у достављени тачни статистички подаци о инцидентима у ИКТ систему у складу са чланом 11б Закона о информационој безбедности?



# АКТ О БЕЗБЕДНОСТИ

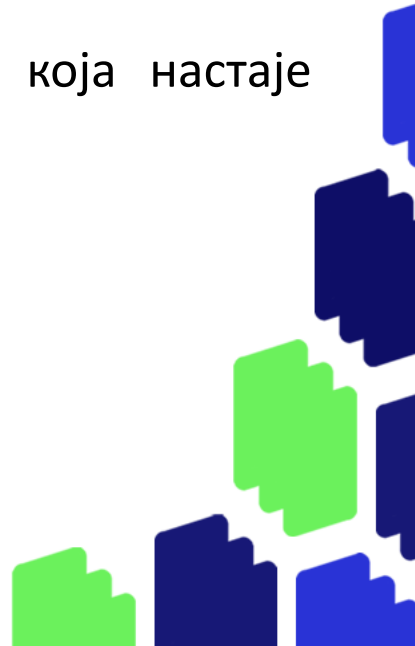
Обавеза доношења Акта о безбедности ИКТ система од посебног значаја

- Оператор ИКТ система од посебног значаја **дужан је да донесе акт о безбедности** ИКТ система од посебног значаја који мора бити усклађен са Законом о информационој безбедности и Уредбом о ближем садржају акта о безбедности;
- Актом о безбедности одређују се **мере заштите, принципи, начин и процедуре постизања** и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја;
- Акт о безбедности може бити донет у форми **правилника, директиве или другој форми** сходно пракси и прописаним условима за појединог оператора ИКТ система;
- Модел акта се налази на сајту Националног ЦЕРТ-а.

# Акт о безбедности

Усклађеност са прописима и провера ИКТ система од посебног значаја

- Оператор ИКТ система је **дужан да врши проверу** ИКТ система, односно **проверу усклађености примењених мера** заштите са Актом о безбедности, мерама заштите прописаним Законом о информационој безбедности и Уредбом о мерама заштите;
- Провера може да се врши **самостално** или уз ангажовање **спољних експерата**;
- Провером се оцењује **адекватност нивоа информационе безбедности** путем провере мера заштите, процедура и одговорности утврђених актом о безбедности;
- Провером се утврђује угроженост или нарушавање информационе безбедности која настаје коришћењем **неодговарајућих поступака и техничких средстава**.

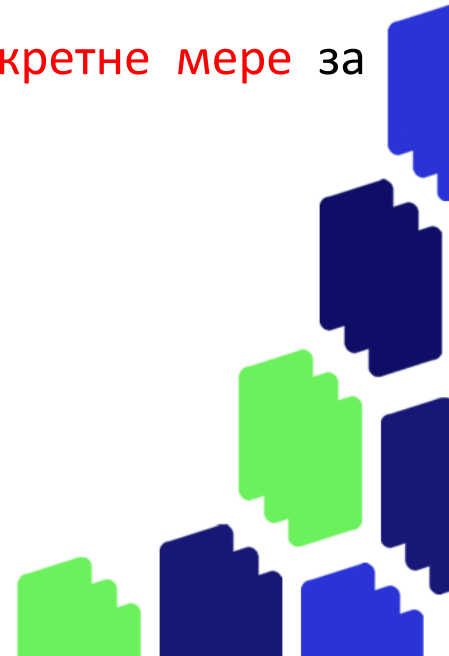




# АКТ о безбедности

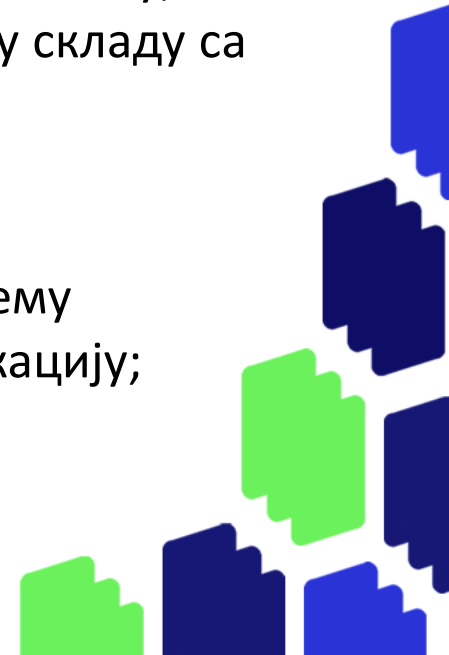
*Мере заштите ИКТ система од посебног значаја*

- Оператори ИКТ система од посебног значаја **дужни су да примене мере заштите** у складу са ЗИБ и Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја;
- Мере заштите одређене су водећи се са стандардима **ISO 27000**;
- Оператори ИКТ система обавезно примењују мере заштите у складу са техничком и организационом структуром ИКТ система:
- Закон и уредба дају оквир, а на операторима ИКТ система је да предвиде **конкретне мере** за заштиту ИКТ система у Акту о безбедности ИКТ система.

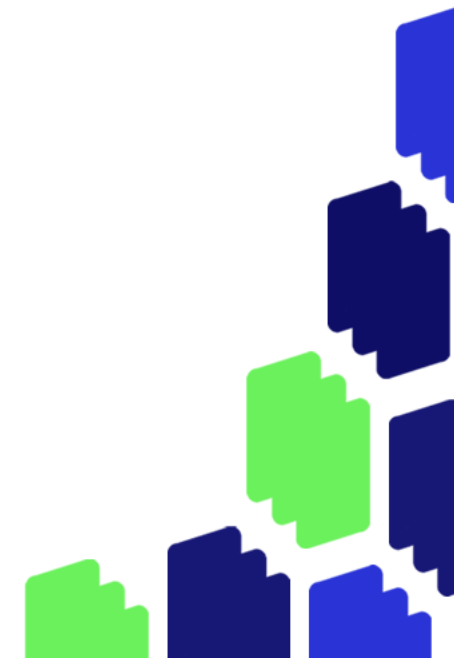


# Мере заштите

- 1) успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;
- 2) постизање безбедности рада на даљину и употребе мобилних уређаја;
- 3) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде;
- 4) заштита од ризика који настају при променама послова или престанка радног ангажовања запослених код оператора ИКТ система;
- 5) идентификовање информационих добара и одређивање одговорности за њихову заштиту;
- 6) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком;
- 7) заштита носача података;
- 8) ограничење приступа подацима и средствима за обраду података;
- 9) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему
- 10) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;



- 11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности односно интегритета података;
- 12) физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система
- 13) заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;
- 14) обезбеђивање исправног и безбедног функционисања средстава за обраду података;
- 15) заштита података и средстава за обраду података од злонамерног софтвера;
- 16) заштита од губитка података;
- 17) чување података о догађајима који могу бити од значаја за безбедност ИКТ система;
- 18) обезбеђивање интегритета софтвера и оперативних система;
- 19) заштита од злоупотребе техничких безбедносних слабости ИКТ система;
- 20) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;



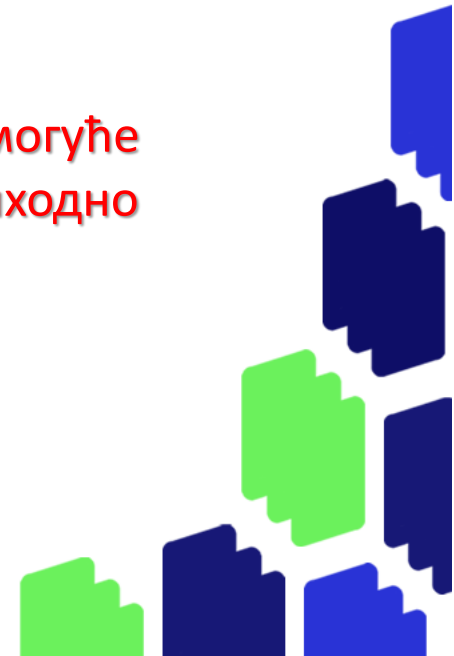
- 21) заштита података у комуникационим мрежама укључујући уређаје и водове;
- 22) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;
- 23) питања информационе безбедности у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
- 24) заштита података који се користе за потребе тестирања ИКТ система односно делова система;
- 25) заштита средстава оператора ИКТ система која су доступна пружаоцима услуга;
- 26) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;
- 27) превенција и реаговање на безбедносне инциденте, адекватна размена информација о безбедносним слабостима ИКТ система, инцидентима и претњама;
- 28) мере које обезбеђују континуитет обављања посла у ванредним околностима.



# АКТ О БЕЗБЕДНОСТИ

## Описи мера заштите

- Описи мера заштите у оквиру акта о безбедности треба да буду груписани у **28 одељака** према називима и редоследу мера заштите из члана 7. став 3. Закона о информационој безбедности.
- Сваки одељак садржи опис мера заштите укључујући процедуре, овлашћења и одговорности учесника у спровођењу мера, а ако су ти описи садржани у другим актима оператора ИКТ система **наводе се упућујуће одредбе на та акта.**
- Уколико неки од услова из Закона о информационој безбедности **није могуће применити или је анализа ризика показала да одређени услов није неопходно применити у пуном обиму**, то је потребно образложити у акту о безбедности.

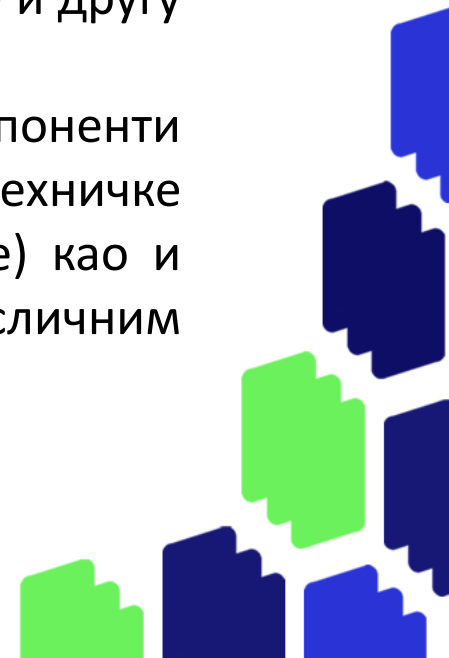


# Начин провере ИКТ система

## Описи мера заштите

Провера се врши тако што се:

- проверава **усклађеност Акта** о безбедности ИКТ система, узимајући у обзир и **акта на која се врши упућивање** са прописаним условима, односно проверава да ли су Актом адекватно предвиђене мере заштите, процедуре, овлашћења и одговорности у ИКТ систему;
- проверава да ли се у оперативном раду адекватно примењују предвиђене мере заштите и процедуре у складу са утврђеним овлашћењима и одговорностима **методама интервјуа** симулације, посматрања, увида у предвиђене евиденције и другу документацију;
- проверавају **безбедносне слабости** на нивоу техничких карактеристика компоненти ИКТ система методом увида у **изабране производе**, архитектуре решења, техничке конфигурације, техничке податаке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

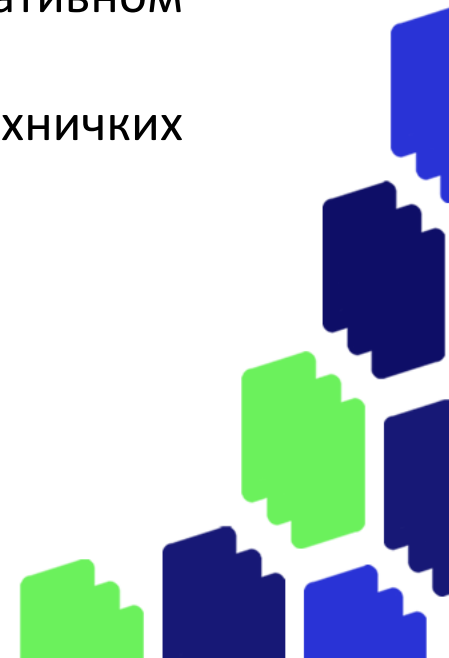


# Начин провере ИКТ система

## *Извештај о провери ИКТ система*

Извештај о провери ИКТ система садржи:

- 1) назив оператора ИКТ система који се проверава;
- 2) време провере;
- 3) подаци о лицима која су вршила проверу;
- 4) извештај о спроведеним радњама провере;
- 5) закључке по питању усклађености Акта о безбедности ИКТ система са прописаним условима;
- 6) закључке по питању адекватне примене предвиђених мера заштите у оперативном раду;
- 7) закључке по питању евентуалних безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система;
- 8) оцена укупног нивоа информационе безбедности;
- 9) предлог евентуалних корективних мера;
- 10) потпис одговорног лица које је спровело проверу ИКТ система.

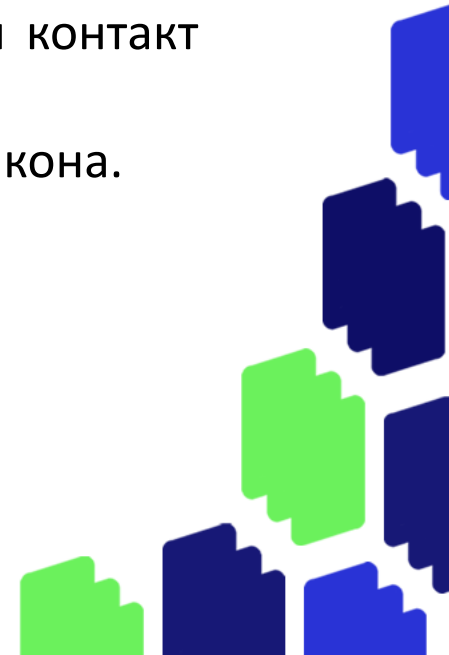


# Евиденција ИКТ система

## *Извештај о провери ИКТ система*

Надлежни орган **успоставља и води евиденцију ИКТ** система од посебног значаја (у даљем тексту: Евиденција) која садржи:

- 1) назив и седиште оператора ИКТ система од посебног значаја;
- 2) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора ИКТ система од посебног значаја;
- 3) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја;
- 4) податак о врсти ИКТ система од посебног значаја, у складу са чланом 6. овог закона.





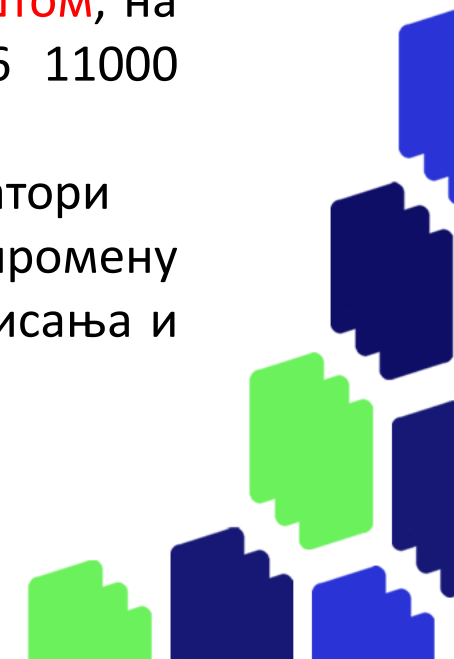
# Евиденција ИКТ система

## Извештај о провери ИКТ система

Упис података у Евиденцију подноси се Министарству:

- Електронским путем, на **Обрасцу 1** и који је објављен на веб страници Министарства информисања и телекомуникација. Захтев се доставља у форми **електронског документа** у оригиналу или у форми овереног дигитализованог акта, у складу са прописима којима се уређује електронски документ, на електронску адресу Министарства информисања и телекомуникација: [evidencijaiktsistema@mit.gov.rs](mailto:evidencijaiktsistema@mit.gov.rs);
- Захтев се може поднети и писаним путем, на Обрасцу 1, непосредно или **ПОШТОМ**, на адресу Министарства информисања и телекомуникација: Немањина 22-26 11000 Београд;

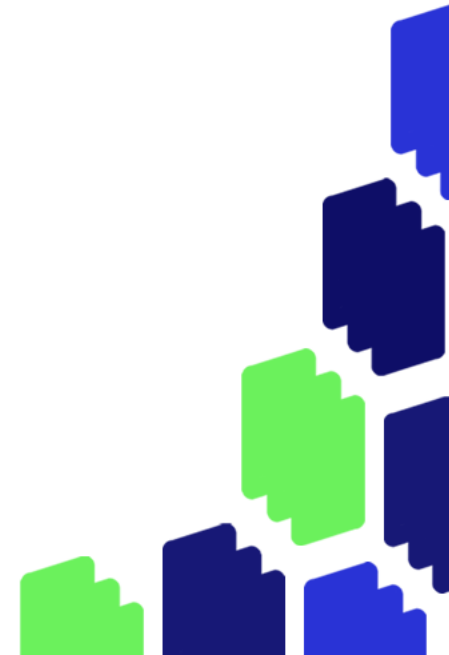
Уколико дође до промене података уписаних у Евиденцију ИКТ система, оператори дужни да у року од **осам дана** од дана настанка промене поднесу Захтев за промену података на **Обрасцу 2** који је објављен на веб страници Министарства информисања и телекомуникација.



# Статистички подаци о свим инцидентима

## *Извештај о провери ИКТ система*

- Оператор ИКТ система од посебног значаја дужан је да достави Националном ЦЕРТ-у **статистичке податке о свим инцидентима** у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.
- Сва детаљнија обавештења о врсти, форми и начину достављања статистичких података можете пронаћи на веб страници националног ЦЕРТ-а: Насловна - Национални ЦЕРТ Републике Србије (cert.rs)
- Врсту статистичких података ближе уређује Национални церт.
- [statistika@cert.rs](mailto:statistika@cert.rs)

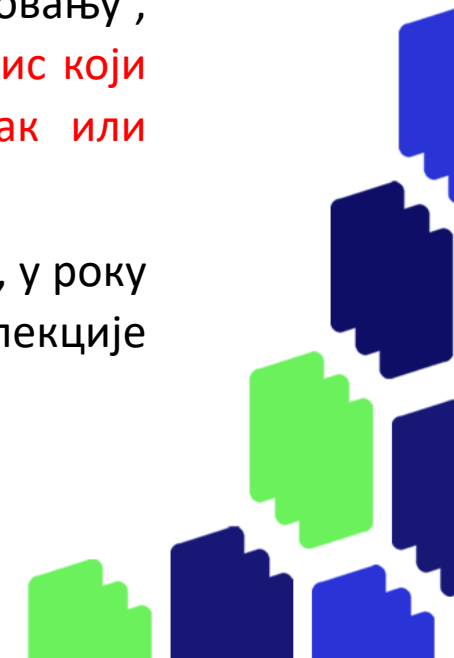


# Превентивно деловање инспекције

## Извештај о провери ИКТ система

### Службена саветодавна посета:

- облик **превентивног деловања инспекције** пружањем стручне и саветодавне подршке, коју инспекција организује ван инспекцијског надзора;
- надзирани субјекат може да захтева превентивно деловање и када се не води поступак инспекцијског надзора, а инспекција је дужна да најкасније у року од **15 дана од дана пријема захтева** поступи по захтеву или обавести надзираног субјекта о разлозима за непоступање по захтеву;
- ако у службеној саветодавној посети уочи пропуст, недостатак или неправилност у пословању, инспекција у року од осам дана након посете сачињава и доставља овом субјекту **допис који садржи препоруке овом субјекту** о томе како да тај пропуст, односно **недостатак или неправилност исправи** и у ком року то треба да учини;
- субјекат обавештава инспекцију о томе да ли је и како је поступио по овим препорукама, у року наведеном у допису; непоступање по овим препорукама, као и необавештавање инспекције може представљати разлог за покретање **инспекцијског надзора**.



**Хвала на пажњи**



**Република Србија**  
Министарство информисања  
и телекомуникација