

На основу члана 8. став 5. Закона о информационој безбедности („Службени гласник РС”, број 6/16) и члана 42. став 1. Закона о Влади („Службени гласник РС”, бр. 55/05, 71/05 – исправка, 101/07, 65/08, 16/11, 68/12 – УС, 72/12, 7/14 – УС и 44/14),

Влада доноси

УРЕДБУ

о ближем садржају акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја

Предмет Уредбе

Члан 1.

Овом уредбом уређује се ближи садржај акта о безбедности информационо-комуникационих система од посебног значаја, начин провере информационо-комуникационих система од посебног значаја и садржај извештаја о провери информационо-комуникационог система од посебног значаја.

Акт о безбедности ИКТ система од посебног значаја

Члан 2.

Оператор ИКТ система од посебног значаја (у даљем тексту: Оператор ИКТ система) дужан је да донесе акт о безбедности ИКТ система од посебног значаја (у даљем тексту: акт о безбедности) који мора бити усклађен са законом и овом уредбом.

Садржај Акта о безбедности

Члан 3.

Актом о безбедности, у складу са законом, 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 (у даљем тексту: ИКТ систем).

Уколико су поједина питања из става 1. овог члана уређена другим актима оператора ИКТ система, акт о безбедности треба да садржи упућујуће одредбе на та акта.

Мере заштите

Члан 4.

Мере заштите одређене актом о безбедности морају бити усклађене са мерама заштите из члана 7. Закона о информационој безбедности и актом Владе којима су мере заштите ближе уређене (у даљем тексту: Уредба о мерама заштите).

Описи мера заштите у оквиру акта о безбедности треба да буду груписани у 28 одељака према називима и редоследу тачака из члана 7. став 3. Закона о информационој безбедности.

Сваки одељак из става 2. овог члана 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 члана 7. став 3. 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.

Измена Акта о безбедности

Члан 5.

Акт о безбедности мора да буде усклађен са променама у окружењу и у самом ИКТ систему.

Промене у окружењу и у самом ИКТ систему су оне промене које могу довести до повећане изложености ИКТ система безбедносним ризицима, услед наступања техничко-технолошких, кадровских, организационих промена у ИКТ систему и догађаја на глобалном и националном нивоу који могу нарушити информациону безбедност, као и оне промене које стварају могућности за унапређење мера заштите.

У случају промена из става 2. овог члана, уколико је то потребно, врши се измена Акта о безбедности, односно прилагођавање и унапређење мера заштите, начина и процедура постизања и одржавања адекватног нивоа безбедности ИКТ система, као и преиспитивање овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система.

Провера ИКТ система

Члан 6.

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.

Оператор ИКТ система је дужан да проверу врши најмање једном годишње и да о томе сачини извештај.

Провера се врши тако што се:

- 1) 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;

2) 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;

3) врши провера безбедносних слабости на нивоу техничких карактеристика компоненти ИКТ система методом увида у изабране производе, архитектуре решења, техничке конфигурације, техничке податке о статусима, записе о догађајима (логове) као и методом тестирања постојања познатих безбедносних слабости у сличним окружењима.

Садржај извештаја о провери ИКТ система

Члан 7.

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.

Прелазна одредба

Члан 8.

Акт о безбедности доноси се у року од 90 дана од дана ступања на снагу ове уредбе.

Завршна одредба

Члан 9.

Ова уредба ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

05 број 110-9465/2016-1

У Београду, 17. новембра 2016. године

Влада

Председник,
Александар Вучић, с.р.