

ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЈЕДНОСТИ

Члан 1.

Овим законом дефинише се информациона безбједност која се обезбјеђује примјеном мјера и стандарда информационе безбједности.

Члан 2.

(1) Одредбе овог закона примјењују:

- а) републички органи,
- б) органи јединица локалне самоуправе,
- в) правна лица која врше јавна овлашћења и
- г) друга правна и физичка лица која остварују приступ или поступају са подацима у електронском облику републичких органа, органа јединица локалне самоуправе и правних лица која врше јавна овлашћења.

(2) Одредбе овога закона не примјењују се у оним случајевима гдје се другим законима прописује употреба документа на папиру и на податке чија се информациона безбједност обезбјеђује у складу са прописима којима се уређује тајност података.

Члан 3.

Поједини изрази који се користе у овом закону имају сљедеће значење:

- а) информациона безбједност – стање повјерљивости, цјеловитости и доступности података,
- б) податак – то је информација, порука и документ сачињен, послат, примљен, забиљежен, складиштен или приказан електронским, оптичким или сличним средством, укључујући пренос путем интернета и електронске поште,
- в) повјерљивост податка – податак који је доступан само лицима која су овлашћена да остваре приступ или даље поступају са тим податком,
- г) цјеловитост податка – подразумијева очување постојања, тачности и комплетности податка, као и заштиту процеса или програма који спречавају неовлашћено мијењање податка,
- д) доступност податка – подразумијева могућност да овлашћени корисници могу приступити податку увијек када за тим имају потребу, и
- ђ) ЦЕРТ – Computer Emergency Response Team – то је међународно признат термин, а подразумијева посебну организациону јединицу за дјеловање у хитним случајевима, чији је задатак координација превенције и заштите од рачунарских безбједносних инцидената на интернету и других ризика безбједности информационих система органа и других физичких и правних лица.

Члан 4.

- (1) Мјере информационе безбједности су општа правила којима се обезбјеђује основна заштита података на физичком, техничком и организационом нивоу.
- (2) Влада Републике Српске (у даљем тексту: Влада) утврђује мјере информационе безбједности из става 1. овог члана.

Члан 5.

- (1) Мјере из члана 4. овог закона спроводе се у складу са стандардима информационе безбједности.
- (2) Министар науке и технологије (у даљем тексту: министар), на приједлог Агенције за информационо друштво Републике Српске (у даљем тексту: Агенција), доноси правилник којим се уређују стандарди информационе безбједности.

Члан 6.

- (1) Мјере информационе безбједности утврђују се у складу са врстом податка, ризицима за његову безбједност и врстом заштите.
- (2) Информациона безбједност обухвата мјере за:
 - а) физичку заштиту,
 - б) заштиту података и
 - в) заштиту информационог система.

Члан 7.

Физичка заштита обухвата заштиту објекта, простора и уређаја у којем се налазе подаци.

Члан 8.

- (1) Заштита податка обухвата превенцију и отклањање штете од губитка, откривања или неовлашћене измјене података.
- (2) Заштита из става 1. овог члана односи се на:
 - а) правила за поступање са подацима,
 - б) садржај и начин вођења евиденције о извршеним приступима подацима и
 - в) надзор који се тиче безбједности података.

Члан 9.

Заштита информационог система обухвата заштиту података који се обрађују, складиште или преносе у информационом систему, као и заштиту повјерљивости, цјеловитости и доступности информационог система у процесу планирања, пројектовања, изградње, употребе, одржавања и престанка рада тог система.

Члан 10.

Координацију превенције и заштите од рачунарских безбједносних инцидената на интернету и других ризика безбједности информационих система органа и других правних и физичких лица из члана 2. став 1. овог закона врши Агенција, преко посебне организационе јединице за дјеловање у хитним случајевима – ЦЕРТ.

Члан 11.

(1) Органи и друга правна и физичка лица из члана 2. став 1. овог закона могу организовати превенцију и заштиту својих информационих система од рачунарских безбједносних инцидената на интернету и других ризика безбједности тих система.

(2) ЦЕРТ усклађује рад органа и других правних и физичких лица из става 1. овог члана.

Члан 12.

Уколико настану безбједносни рачунарски инциденти на информационим системима органа и других правних и физичких лица из члана 2. став 1. овог закона, ЦЕРТ усклађује поступање тих органа примјеном мјера информационе безбједности.

Члан 13.

(1) Надзор над примјеном овог закона врши Министарство науке и технологије, а стручни надзор врши Агенција.

(2) Ради вршења надзора, органи и друга правна и физичка лица из члана 2. став 1. овог закона дужни су да одговорном лицу органа управног и стручног надзора омогуће приступ простору, рачунарској опреми и уређајима, као и да без одлагања ставе на увид или доставе потребне податке и документацију у вези са предметом надзора.

Члан 14.

Влада ће у року од шест мјесеци од дана ступања на снагу овог закона донијети уредбу о мјерама информационе безбједности из члана 4. став 2. овог закона.

Члан 15.

Министар ће у року од шест мјесеци од дана ступања на снагу овог закона, на приједлог Агенције, донијети правилник којим се уређују стандарди информационе безбједности из члана 5. став 2. овог закона.

Члан 16.

Агенција ће у року од шест мјесеци од дана ступања на снагу овог закона формирати посебну организациону јединицу за дјеловање у хитним случајевима – ЦЕРТ из члана 10. овог закона.

Члан 17.

Ступањем на снагу овог закона престаје да важи Закон о информационом систему Републике Српске („Службени гласник Републике Српске“, број 38/98).

Члан 18.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Српске“.

Број:
Датум:
Бања Лука

ПРЕДСЈЕДНИК
НАРОДНЕ СКУПШТИНЕ
Мр Игор Радојичић