ПРЕГЛЕД ОДРЕДАБА КОЈЕ СЕ МЕЊАЈУ

Значење појединих термина

Члан 2.

Поједини термини у смислу овог закона имају следеће значење:

1) информационо-комуникациони систем (ИКТ систем) је технолошко-организациона целина која обухвата:

(1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;

(2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;

(3) податке који се ~~ПОХРАЊУЈУ~~ ВОДЕ, ЧУВАЈУ, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

(4) организациону структуру путем које се управља ИКТ системом;

2) оператор ИКТ система је правно лице, орган ~~ЈАВНЕ~~ власти или организациона јединица органа ~~ЈАВНЕ~~ власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

4) тајност је својство које значи да податак није доступан неовлашћеним лицима;

5) интегритет значи очуваност изворног садржаја и комплетности податка;

6) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

7) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

8) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9) ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

10) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

11) инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

12) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

13) тајни податак је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

14) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

15) орган ~~ЈАВНЕ~~ власти је државни орган, орган аутономне покрајине, орган јединице локалне самоуправе, организација ~~КОЈОЈ~~ И ДРУГО ПРАВНО ИЛИ ФИЗИЧКО ЛИЦЕ КОМЕ је поверено вршење јавних овлашћења~~, ПРАВНО ЛИЦЕ КОЈЕ ОСНИВА РЕПУБЛИКА СРБИЈА, АУТОНОМНА ПОКРАЈИНА ИЛИ ЈЕДИНИЦА ЛОКАЛНЕ САМОУПРАВЕ, КАО И ПРАВНО ЛИЦЕ КОЈЕ СЕ ПРЕТЕЖНО, ОДНОСНО У ЦЕЛИНИ ФИНАНСИРА ИЗ БУЏЕТА~~;

16) служба безбедности је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;

17) самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;

18) компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

19) криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

20) криптозаштита је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

21) криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

22) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

23) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

24) информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, ЗАПИСЕ О КОРИШЋЕЊУ ХАРДВЕРСКИХ КОМПОНЕНТИ, ПОДАТАКА ИЗ ДАТОТЕКА И БАЗА ПОДАТАКА И СПРОВОЂЕЊУ ПРОЦЕДУРА АКО СЕ ИСТИ ВОДЕ, унутрашње опште акте, процедуре и слично;

25) УСЛУГА ИНФОРМАЦИОНОГ ДРУШТВА ЈЕ УСЛУГА У СМИСЛУ ЗАКОНА КОЈИМ СЕ УРЕЂУЈЕ ЕЛЕКТРОНСКА ТРГОВИНА;

26) ПРУЖАЛАЦ УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА ЈЕ ПРУЖАЛАЦ УСЛУГЕ У СМИСЛУ ЗАКОНА КОЈИМ СЕ УРЕЂУЈЕ ЕЛЕКТРОНСКА ТРГОВИНА.

ОБРАДА ПОДАТАКА О ЛИЧНОСТИ

ЧЛАН 3А

У СЛУЧАЈУ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ ПРИЛИКОМ ВРШЕЊА НАДЛЕЖНОСТИ И ИСПУЊЕЊА ОБАВЕЗА ИЗ ОВОГ ЗАКОНА ПОСТУПА СЕ У СКЛАДУ СА ПРОПИСИМА КОЈИ УРЕЂУЈУ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ.

Тело за координацију послова информационе безбедности

Члан 5.

У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада оснива Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, ~~ЦЕРТ-А РЕПУБЛИЧКИХ ОРГАНА И НАЦИОНАЛНОГ ЦЕРТ-А~~ НАРОДНЕ БАНКЕ СРБИЈЕ, ЦЕНТРА ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА У ОРГАНИМА ВЛАСТИ И НАЦИОНАЛНОГ ЦЕНТРА ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА.

У функцији унапређења појединих области информационе безбедности формирају се стручне радне групе Тела за координацију у које се укључују и представници других органа ~~ЈАВНЕ~~ власти, привреде, академске заједнице и невладиног сектора.

Одлуком којом оснива Тело за координацију Влада одређује и његов састав, задатке, рок у коме оно подноси извештаје Влади и друга питања која су везана за његов рад.

ИКТ системи од посебног значаја

Члан 6.

ИКТ системи од посебног значаја су системи који се користе:

1) у обављању послова у органима ~~ЈАВНЕ~~ власти;

2) за обраду ПОСЕБНИХ ВРСТА података ~~КОЈИ СЕ~~ О ЛИЧНОСТИ, у ~~СКЛАДУ СА ЗАКОНОМ~~ СМИСЛУ ЗАКОНА који уређује заштиту података о личности~~, СМАТРАЈУ НАРОЧИТО ОСЕТЉИВИМ ПОДАЦИМА О ЛИЧНОСТИ;~~

3) у обављању делатности од општег интереса и ДРУГИМ ДЕЛАТНОСТИМА И то у СЛЕДЕЋИМ областима:

(1) ЕНЕРГЕТИКА:

- производња, пренос и дистрибуција електричне енергије;
- ~~(2)~~ производња и прерада угља;
- ~~(3)~~ истраживање, производња, прерада, транспорт и дистрибуција нафте и ~~(4)~~ промет нафте и нафтних деривата;
- истраживање, производња, прерада, транспорт и дистрибуција природног и течног гаса.

(2) САОБРАЋАЈ:

- железнички, поштански, водени и ваздушни саобраћај;

(3) ЗДРАВСТВО:

- здравствена заштита

(4) БАНКАРСТВО И ФИНАНСИЈСКА ТРЖИШТА:

- послови финансијских институција

5) ДИГИТАЛНА ИНФРАСТРУКТУРА:

- размена интернет саобраћаја;
- управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)

(6) ДОБРА ОД ОПШТЕГ ИНТЕРЕСА:

- коришћење, управљање, заштита и унапређивање добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја);

(7) УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА:

- УСЛУГЕ ПЛАТФОРМЕ ЗА ЕЛЕКТРОНСКУ ТРГОВИНУ;
- УСЛУГЕ ИНТЕРНЕТ ПРЕТРАЖИВАЊА;
- УСЛУГЕ РАЧУНАРСТВА У ОБЛАКУ (CLOUD COMPUTING SERVICE);
- УСЛУГЕ СЕРВИСА ЗА ЕЛЕКТРОНСКУ РАЗМЕНУ ПОДАТАКА (ELECTRONIC DATA INTERCHANGE – EDI);

(8) ОСТАЛЕ ОБЛАСТИ:

- електронске комуникације;
- издавање службеног гласила Републике Србије;
- управљање нуклеарним објектима;
- производња, промет и превоз наоружања и војне опреме;
- управљање отпадом;
- комуналне делатности;
- ПРОИЗВОДЊА И СНАБДЕВАЊЕ ХЕМИКАЛИЈАМА.

4) У ПРАВНИМ ЛИЦИМА И УСТАНОВАМА КОЈЕ ОСНИВА РЕПУБЛИКА СРБИЈА, АУТОНОМНА ПОКРАЈИНА ИЛИ ЈЕДИНИЦА ЛОКАЛНЕ САМОУПРАВЕ ЗА ОБАВЉАЊЕ ДЕЛАТНОСТИ ИЗ ТАЧКЕ 3) ОВОГ СТАВА.

~~13) 14) УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА НАМЕЊЕНЕ ДРУГИМ ПРУЖАОЦИМА УСЛУГА ИНФОРМАЦИОНОГ ДРУШТВА У ЦИЉУ ОМОГУЋАВАЊА ПРУЖАЊА ЊИХОВИХ УСЛУГА.~~

Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу ~~ПОСЛОВА И~~ делатности из става 1. тачка 3) овог члана.

ОБАВЕЗЕ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ЧЛАН 6А

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА У СКЛАДУ СА ОВИМ ЗАКОНОМ У ОБАВЕЗИ ЈЕ 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 СТАТИСТИЧКЕ ПОДАТКЕ О ИНЦИДЕНТИМА У ИКТ СИСТЕМУ.

ЕВИДЕНЦИЈА ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ЧЛАН 6Б

НАДЛЕЖНИ ОРГАН УСПОСТАВЉА И ВОДИ ЕВИДЕНЦИЈУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА (У ДАЉЕМ ТЕКСТУ: ЕВИДЕНЦИЈА) КОЈА САДРЖИ:

1) НАЗИВ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

2) ИМЕ И ПРЕЗИМЕ, СЛУЖБЕНА АДРЕСА ЗА ПРИЈЕМ ЕЛЕКТРОНСКЕ ПОШТЕ И КОНТАКТ ТЕЛЕФОН АДМИНИСТРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

3) ИМЕ И ПРЕЗИМЕ, СЛУЖБЕНА АДРЕСА ЗА ПРИЈЕМ ЕЛЕКТРОНСКЕ ПОШТЕ И 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.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ИКТ СИСТЕМ ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИМ УПРАВЉА УПИШЕ У ЕВИДЕНЦИЈУ ИЗ СТАВА 1. ОВОГ ЧЛАНА.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА НАДЛЕЖНОМ ОРГАНУ ДОСТАВИ ПОДАТКЕ ИЗ СТАВА 1. НАЈКАСНИЈЕ 90 ДАНА ОД ДАНА УСВАЈАЊА ПРОПИСА ИЗ ЧЛАНА 6. СТАВА 2. ОВОГ ЗАКОНА, ОДНОСНО 90 ДАНА ОД ДАНА УСПОСТАВЉАЊА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА.

НАДЛЕЖНИ ОРГАН СТАВЉА НА РАСПОЛАГАЊЕ НАЦИОНАЛНОМ ЦЕНТРУ ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (У ДАЉЕМ ТЕКСТУ: НАЦИОНАЛНИ ЦЕРТ) АЖУРНУ ЕВИДЕНЦИЈУ ИЗ СТАВА 1. ОВОГ ЧЛАНА.

Мере заштите ИКТ система од посебног значаја

Члан 7.

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и ~~МИНИМИЗАЦИЈА~~ СМАЊЕЊЕ штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

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 и разумеју своју одговорност;

4) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица 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 из члана 3. овог закона;

7) заштиту носача података;

8) ограничење приступа подацима и средствима за обраду података;

9) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;

10) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;

11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности ~~ОДНОСНО~~ И интегритета података;

12) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;

13) заштиту 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) заштиту података и средства за обраду података од злонамерног софтвера;

16) заштиту 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) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

20) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;

21) заштиту 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~~ ИСПУЊЕЊЕ ЗАХТЕВА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

24) заштиту података који се користе за потребе тестирања ИКТ система односно делова система;

25) заштиту 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) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;

28) мере које обезбеђују континуитет обављања посла у ванредним околностима.

Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система, уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

Обавештавање ~~НАДЛЕЖНОГ ОРГАНА~~ о инцидентима

Члан 11.

Оператори ИКТ система од посебног значаја ~~ОБАВЕЗНИ СУ ДА ОБАВЕСТЕ НАДЛЕЖНИ ОРГАН~~ ОБАВЕШТАВАЊЕ о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности ВРШЕ ПРЕКО ПОРТАЛА НАДЛЕЖНОГ ОРГАНА ИЛИ НАЦИОНАЛНОГ ЦЕРТ-А У ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА ОДРЖАВА НАДЛЕЖНИ ОРГАН.

Изузетно од става 1. овог члана, ~~ФИНАНСИЈСКЕ ИНСТИТУЦИЈЕ ОБАВЕШТЕЊА УПУЋУЈУ~~ ОБАВЕШТЕЊЕ О ИНЦИДЕНТИМА СЕ УПУЋУЈЕ:

1) Народној банци Србије, ~~ТЕЛЕКОМУНИКАЦИОНИ ОПЕРАТОРИ~~ У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (4) ОВОГ ЗАКОНА;

2) регулаторном телу за електронске комуникације ~~А ОПЕРАТОРИ~~ У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА 8) АЛИНЕЈА ПРВА ОВОГ ЗАКОНА:

3) Центру за безбедност ИКТ система У ОРГАНИМА ВЛАСТИ, У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА КОЈИ СУ ПОВЕЗАНИ НА ЈЕДИНСТВЕНУ ИНФОРМАЦИОНО-КОМУНИКАЦИОНУ МРЕЖУ ЕЛЕКТРОНСКЕ УПРАВЕ.

НАРОДНА БАНКА СРБИЈЕ, РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ЦЕНТАР ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА У ОРГАНИМА ВЛАСТИ ОБАВЕШТЕЊА ИЗ СТАВА 2. ОВОГ ЧЛАНА ДОСТАВЉАЈУ У ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА НА НАЧИН ИЗ СТАВА 1. ОВОГ ЧЛАНА.

У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА за рад са тајним подацима ОПЕРАТОРИ ТИХ ИКТ СИСТЕМА поступају у складу са прописима којима се уређује област заштите тајних података.

Одредбе ст. 1 и 2. овог члана не односе се на самосталне операторе ИКТ система.

~~ПОСТУПАК ДОСТАВЉАЊА ПОДАТАКА~~ ВЛАДА, НА ПРЕДЛОГ НАДЛЕЖНОГ ОРГАНА, УРЕЂУЈЕ ПОСТУПАК ОБАВЕШТАВАЊА О ИНЦИДЕНТИМА, листу, врсте и значај инцидената ~~И ПОСТУПАК ОБАВЕШТАВАЊА~~ ПРЕМА НИВОУ ОПАСНОСТИ, ПОСТУПАЊЕ И РАЗМЕНУ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА ИЗМЕЂУ ОРГАНА из ~~СТАВА 1~~ ЧЛАНА 5. овог ~~ЧЛАНА УРЕЂУЈЕ ВЛАДА~~ ЗАКОНА.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 2. овог члана коме се упућују обавештења о инцидентима, може ~~НАЛОЖИТИ ЊЕГОВО ОБЈАВЉИВАЊЕ~~ ОБЈАВИТИ ИНФОРМАЦИЈУ О ИНЦИДЕНТУ, НАКОН САВЕТОВАЊА СА ОПЕРАТОРОМ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИ ЈЕ ДОСТАВИО ОБАВЕШТЕЊЕ О ИНЦИДЕНТУ.

Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, ~~НАДЛЕЖНИ ОРГАН, ОДНОСНО ОРГАН ИЗ СТАВА 2. ОВОГ ЧЛАНА~~ ОРГАН коме ~~СЕ УПУЋУЈУ ОБАВЕШТЕЊА~~ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ о ~~ИНЦИДЕНТИМА~~ ИНЦИДЕНТУ, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

АКО ЈЕ ИНЦИДЕНТ ПОВЕЗАН СА ЗНАЧАЈНИМ НАРУШАВАЊЕМ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ, КОЈЕ ИМА ИЛИ МОЖЕ ИМАТИ ЗА ПОСЛЕДИЦУ УГРОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ, ОРГАН КОМЕ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ О ИНЦИДЕНТУ ОБАВЕШТАВА БЕЗБЕДНОСНО-ИНФОРМАТИВНУ АГЕНЦИЈУ.

Ако је инцидент повезан са нарушавањем права на заштиту података о личности, ~~НАДЛЕЖНИ~~ орган~~, ОДНОСНО ОРГАН ИЗ СТАВА 2. ОВОГ ЧЛАНА~~ коме ~~СЕ УПУЋУЈУ ОБАВЕШТЕЊА~~ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ о ~~ИНЦИДЕНТИМА~~ ИНЦИДЕНТУ и самостални оператор ИКТ система, о томе обавештавају и Повереника за информације од јавног значаја и заштиту података о личности.

У СЛУЧАЈУ НАСТУПАЊА ОКОЛНОСТИ УГРОЖАВАЊА, ОМЕТАЊА РАДА ИЛИ УНИШТЕЊА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА РУКОВОЂЕЊЕ И КООРДИНАЦИЈУ СПРОВОЂЕЊА МЕРА И ЗАДАТАКА У НАВЕДЕНИМ ОКОЛНОСТИМА ПРЕДУЗИМА РЕПУБЛИЧКИ ШТАБ ЗА ВАНРЕДНЕ СИТУАЦИЈЕ, У СКЛАДУ СА ЗАКОНОМ.

ИНЦИДЕНТИ У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

ЧЛАН 11А

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ПРИЈАВИ СЛЕДЕЋЕ ИНЦИДЕНТЕ КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ:

1) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА ВРШЕЊА ПОСЛОВА И ПРУЖАЊА УСЛУГА, ОДНОСНО ЗНАТНИХ ТЕШКОЋА У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊУ УСЛУГА;

2) ИНЦИДЕНТЕ КОЈИ УТИЧУ НА ВЕЛИКИ БРОЈ КОРИСНИКА УСЛУГА, ИЛИ ТРАЈУ ДУЖИ ВРЕМЕНСКИ ПЕРИОД;

3) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА, ОДНОСНО ТЕШКОЋА У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊА УСЛУГА, КОЈИ УТИЧУ НА ОБАВЉАЊЕ ПОСЛОВА И ВРШЕЊЕ УСЛУГА ДРУГИХ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ИЛИ УТИЧУ НА ЈАВНУ БЕЗБЕДНОСТ;

4) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА, ОДНОСНО ТЕШКОЋЕ У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊУ УСЛУГА И ИМАЈУ УТИЦАЈ НА ВЕЋИ ДЕО ТЕРИТОРИЈЕ РЕПУБЛИКЕ СРБИЈЕ;

5) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО НЕОВЛАШЋЕНОГ ПРИСТУПА ЗАШТИЋЕНИМ ПОДАЦИМА ЧИЈЕ ОТКРИВАЊЕ МОЖЕ УГРОЗИТИ ПРАВА И ИНТЕРЕСЕ ОНИХ НА КОЈЕ СЕ ПОДАЦИ ОДНОСЕ;

6) ИНЦИДЕНТЕ КОЈИ СУ НАСТАЛИ КАО ПОСЛЕДИЦА ИНЦИДЕНТА У ИКТ СИСТЕМУ ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (7) ОВОГ ЗАКОНА, КАДА ИКТ СИСТЕМ ОД ПОСЕБНОГ ЗНАЧАЈА У СВОМ ПОСЛОВАЊУ КОРИСТИ ИНФОРМАЦИОНЕ УСЛУГЕ ИКТ СИСТЕМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (7) ОВОГ ЗАКОНА.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ПРИЈАВИ И ИНЦИДЕНТЕ КОЈИ СУ ДОВЕЛИ ДО ЗНАЧАЈНОГ ПОВЕЋАЊА РИЗИКА ОД НАСТУПАЊА ПОСЛЕДИЦА ИЗ СТАВА 1. ОВОГ ЧЛАНА.

ДОСТАВЉАЊЕ СТАТИСТИЧКИХ ПОДАТАКА О ИНЦИДЕНТИМА

ЧЛАН 11Б

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА, ПОРЕД ОБАВЕШТАВАЊА О ИНЦИДЕНТИМА ИЗ ЧЛАНА 11. ОВОГ ЗАКОНА, ДОСТАВИ НАЦИОНАЛНОМ ЦЕРТ-У СТАТИСТИЧКЕ ПОДАТКЕ О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМУ У ПРЕТХОДНОЈ ГОДИНИ НАЈКАСНИЈЕ ДО 28. ФЕБРУАРА ТЕКУЋЕ ГОДИНЕ.

НАЦИОНАЛНИ ЦЕРТ ОБЈЕДИЊЕНЕ СТАТИСТИЧКЕ ПОДАТКЕ ИЗ СТАВА 1. ОВОГ ЧЛАНА ДОСТАВЉА НАДЛЕЖНОМ ОРГАНУ И ОБЈАВЉУЈЕ ИХ НА ПОРТАЛУ НАЦИОНАЛНОГ ЦЕРТ-А.

ВРСТУ СТАТИСТИЧКИХ ПОДАТАКА ИЗ СТАВА 1. ОВОГ ЧЛАНА УРЕЂУЈЕ НАЦИОНАЛНИ ЦЕРТ.

Међународна сарадња и рана упозорења о ризицима и инцидентима

Члан 12.

Надлежни орган остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

1) брзо расту или имају тенденцију да постану ~~ВИСОКИ РИЗИЦИ~~ ВИСОКО РИЗИЧНИ;

2) превазилазе или могу да превазиђу националне капацитете;

3) могу да имају негативан утицај на више од једне државе.

Уколико је инцидент у вези са извршењем кривичног дела, по добијању обавештења од Надлежног органа, министарство надлежно за унутрашње послове ће у званичној процедури проследити пријаву у складу са потврђеним међународним уговорима.

САМОСТАЛНИ ОПЕРАТОРИ ИКТ СИСТЕМА

Члан 13.

Самостални оператори ИКТ система одредиће посебна лица, односно организационе јединице за интерну контролу сопствених ИКТ система.

Лица за интерну контролу самосталних оператора ИКТ система извештај о извршеној интерној контроли подносе руководиоцу самосталног оператора ИКТ система.

~~НАЦИОНАЛНИ ЦЕНТАР ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (~~Национални ЦЕРТ~~)~~

Члан 14.

~~НАЦИОНАЛНИ ЦЕНТАР ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (У ДАЉЕМ ТЕКСТУ:~~ Национални ЦЕРТ~~)~~ обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.

За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.

НАДЛЕЖНОСТИ НАЦИОНАЛНОГ ЦЕРТА

Члан 15.

Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, ПРУЖА ПОДРШКУ, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно:

1) прати стање о инцидентима на националном нивоу,

2) пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима,

3) реагује по пријављеним или на други начин откривеним инцидентима У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА, КАО И ДРУГИМ ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ, тако што пружа савете И ПРЕПОРУКЕ на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања,

4) континуирано израђује анализе ризика и инцидената,

5) подиже свест код грађана, привредних субјеката и органа ~~ЈАВНЕ~~ власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести,

6) води евиденцију Посебних ЦЕРТ-ова;

~~ЕВИДЕНЦИЈА ИЗ СТАВА 1. ТАЧКА 6) ОВОГ ЧЛАНА ОД ПОДАТАКА О ЛИЧНОСТИ САДРЖИ ПОДАТКЕ О ОДГОВОРНИМ ЛИЦИМА, И ТО: ИМЕ, ПРЕЗИМЕ, ФУНКЦИЈУ И КОНТАКТ ПОДАТКЕ КАО ШТО СУ АДРЕСА, БРОЈ ТЕЛЕФОНА И АДРЕСА ЕЛЕКТРОНСКЕ ПОШТЕ.~~

7) ИЗВЕШТАВА НАДЛЕЖНИ ОРГАН НА КВАРТАЛНОМ НИВОУ О ПРЕДУЗЕТИМ АКТИВНОСТИМА.

НАЦИОНАЛНИ ЦЕРТ ОБЕЗБЕЂУЈЕ НЕПРЕКИДНУ ДОСТУПНОСТ СВОЈИХ УСЛУГА ПУТЕМ РАЗЛИЧИТИХ СРЕДСТАВА КОМУНИКАЦИЈЕ.

ПРОСТОРИЈЕ И ИНФОРМАЦИОНИ СИСТЕМИ НАЦИОНАЛНОГ ЦЕРТ-А МОРАЈУ ДА СЕ НАЛАЗЕ НА БЕЗБЕДНИМ ЛОКАЦИЈАМА.

У ЦИЉУ ОБЕЗБЕЂИВАЊА КОНТИНУИТЕТА РАДА, НАЦИОНАЛНИ ЦЕРТ ТРЕБА ДА:

1) БУДЕ ОПРЕМЉЕН СА ОДГОВАРАЈУЋИМ СИСТЕМИМА ЗА УПРАВЉАЊЕ ИНЦИДЕНТИМА;

2) ИМА ДОВОЉНО ЗАПОСЛЕНИХ КАКО БИ СЕ ОСИГУРАЛА ДОСТУПНОСТ У СВАКО ДОБА;

3) ОБЕЗБЕДИ ИНФРАСТРУКТУРУ ЧИЈИ ЈЕ КОНТИНУИТЕТ ОСИГУРАН, ОДНОСНО ДА ОБЕЗБЕДИ РЕДУНДАНТНЕ СИСТЕМЕ И РЕЗЕРВНИ РАДНИ ПРОСТОР.

Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ.

Национални ЦЕРТ промовише усвајање и коришћење прописаних и стандардизованих ~~ПРАВИЛА~~ ПРОЦЕДУРА за:

1) управљање и санирање ризика и инцидената;

2) класификацију информација о ризицима и инцидентима, ОДНОСНО КЛАСИФИКАЦИЈУ ПРЕМА НИВОУ ИНЦИДЕНАТА И РИЗИКА.

~~3) КЛАСИФИКАЦИЈУ ОЗБИЉНОСТИ ИНЦИДЕНАТА И РИЗИКА;~~

~~4) ДЕФИНИЦИЈУ ФОРМАТА И МОДЕЛА ПОДАТАКА ЗА РАЗМЕНУ ИНФОРМАЦИЈА О РИЗИЦИМА И ИНЦИДЕНТИМА И ДЕФИНИЦИЈУ ПРАВИЛА ПО КОЈИМА ЋЕ СЕ ИМЕНОВАТИ ЗНАЧАЈНИ СИСТЕМИ.~~

САРАДЊА ЦЕРТ-ОВА У РЕПУБЛИЦИ СРБИЈИ

ЧЛАН 15А

НАЦИОНАЛНИ ЦЕРТ, ЦЕРТ ОРГАНА ВЛАСТИ И ЦЕРТ-ОВИ САМОСТАЛНИХ ОПЕРАТОРА ИКТ СИСТЕМА ОДРЖАВАЈУ КОНТИНУИРАНУ САРАДЊУ.

ЦЕРТ-ОВИ ИЗ СТАВА 1. ОВОГ ЧЛАНА ОДРЖАВАЈУ МЕЂУСОБНЕ САСТАНКЕ У ОРГАНИЗАЦИЈИ НАЦИОНАЛНОГ ЦЕРТ-А НАЈМАЊЕ ТРИ ПУТА ГОДИШЊЕ, КАО И ПО ПОТРЕБИ У СЛУЧАЈУ ИНЦИДЕНАТА КОЈИ ЗНАЧАЈНО УГРОЖАВАЈУ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ У РЕПУБЛИЦИ СРБИЈИ.

САСТАНЦИМА ЦЕРТ-ОВА ИЗ СТАВА 1. ОВОГ ЧЛАНА ПРИСУСТВУЈУ И ПРЕДСТАВНИЦИ НАДЛЕЖНОГ ОРГАНА.

САСТАНЦИМА ЦЕРТ-ОВА ИЗ СТАВА 1. ОВОГ ЧЛАНА МОГУ, ПО ПОЗИВУ, ДА ПРИСУСТВУЈУ И ПРЕДСТАВНИЦИ ПОСЕБНИХ ЦЕРТ-ОВА.

НАДЗОР НАД РАДОМ НАЦИОНАЛНОГ ЦЕРТ-А

Члан 16.

Надзор над радом Националног ЦЕРТ-а у вршењу послова поверених овим законом врши Надлежни орган, који периодично, а најмање једном годишње, проверава да ли Национални ЦЕРТ располаже одговарајућим ресурсима, врши послове у складу са чланом 15. овог закона и контролише учинак успостављених процеса за управљање сигурносним инцидентима.

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 17.

Посебан центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Посебан ЦЕРТ) обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

Посебан ЦЕРТ је правно лице или организациона јединица у оквиру правног лица, које је уписано у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ.

Упис у евиденцију посебних ЦЕРТ-ова врши се на основу пријаве правног лица у оквиру кога се налази посебан ЦЕРТ.

Евиденција посебних ЦЕРТ-ова од података о личности садржи податке о одговорним лицима, и то: име, презиме, функцију и контакт податке као што су адреса, број телефона и адреса електронске поште.

Ближе услове за упис у евиденцију из става 3. овог члана доноси ~~НАДЛЕЖНИ ОРГАН~~ НАЦИОНАЛНИ ЦЕРТ.

Центар за безбедност ИКТ система у ~~РЕПУБЛИЧКИМ~~ органима ВЛАСТИ (ЦЕРТ ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ)

Члан 18.

~~ЦЕНТАР ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА У РЕПУБЛИЧКИМ ОРГАНИМА (У ДАЉЕМ ТЕКСТУ:~~ ЦЕРТ ~~РЕПУБЛИЧКИХ~~ органа~~)~~ ВЛАСТИ обавља послове који се односе на заштиту од инцидената у ИКТ системима ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ, изузев ИКТ система самосталних оператора.

Послове ЦЕРТ-а ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ обавља орган надлежан за пројектовање, развој, изградњу, одржавање и унапређење рачунарске мреже републичких органа.

Послови ЦЕРТ-а ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ обухватају:

1) заштиту ИКТ система Рачунарске мреже републичких органа (у даљем тексту: РМРО);

2) координацију и сарадњу са операторима ИКТ система које повезује РМРО у превенцији инцидената, откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;

3) издавање стручних препорука за заштиту ИКТ система ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ, осим ИКТ система за рад са тајним подацима.

ЦЕРТ САМОСТАЛНОГ ОПЕРАТОРА ИКТ СИСТЕМА

Члан 19.

Самостални оператори ИКТ система су у обавези да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима.

Центри из става 1. овог члана међусобно размењују информације о инцидентима, као и са националним ЦЕРТ-ом и са ЦЕРТ-ом ~~РЕПУБЛИЧКИХ~~ органа ВЛАСТИ, а по потреби и са другим организацијама.

Делокруг центра за безбедност ИКТ система, као организационе јединице самосталног оператора ИКТ система, поред послова из ст. 1. и 2. овог члана, може обухватати:

1) израду интерних аката у области информационе безбедности;

2) избор, тестирање и имплементацију техничких, физичких и организационих мера заштите, опреме и програма;

3) избор, тестирање и имплементацију мера заштите од КЕМЗ;

4) надзор имплементације и примене безбедносних процедура;

5) управљање и коришћење криптографских производа;

6) анализу безбедности ИКТ система у циљу процене ризика;

7) обуку запослених у области информационе безбедности.

ЗАШТИТА ДЕЦЕ ПРИ КОРИШЋЕЊУ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

ЧЛАН 19А

НАДЛЕЖНИ ОРГАН ПРЕДУЗИМА ПРЕВЕНТИВНЕ МЕРЕ ЗА БЕЗБЕДНОСТ И ЗАШТИТУ ДЕЦЕ НА ИНТЕРНЕТУ, КАО АКТИВНОСТИ ОД ЈАВНОГ ИНТЕРЕСА, ПУТЕМ ЕДУКАЦИЈЕ И ИНФОРМИСАЊА ДЕЦЕ, РОДИТЕЉА И НАСТАВНИКА О ПРЕДНОСТИМА, РИЗИЦИМА И НАЧИНИМА БЕЗБЕДНОГ КОРИШЋЕЊА ИНТЕРНЕТА, КАО И ПУТЕМ ЈЕДИНСТВЕНОГ МЕСТА ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ, И УПУЋУЈЕ ПРИЈАВЕ НАДЛЕЖНИМ ОРГАНИМА РАДИ ДАЉЕГ ПОСТУПАЊА.

ОПЕРАТОР ЕЛЕКТРОНСКИХ КОМУНИКАЦИЈА КОЈИ ПРУЖА ЈАВНО ДОСТУПНЕ ТЕЛЕФОНСКЕ УСЛУГЕ ДУЖАН ЈЕ ДА ОМОГУЋИ СВИМ ПРЕТПЛАТНИЦИМА УСЛУГУ БЕСПЛАТНОГ ПОЗИВА ПРЕМА ЈЕДИНСТВЕНОМ МЕСТУ ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ.

У СЛУЧАЈУ ДА НАВОДИ ИЗ ПРИЈАВЕ УПУЋУЈУ НА ПОСТОЈАЊЕ КРИВИЧНОГ ДЕЛА, НА ПОВРЕДУ ПРАВА, ЗДРАВСТВЕНОГ СТАТУСА, ДОБРОБИТИ И/ИЛИ ОПШТЕГ ИНТЕГРИТЕТА ДЕТЕТА, НА РИЗИК СТВАРАЊА ЗАВИСНОСТИ ОД КОРИШЋЕЊА ИНТЕРНЕТА, ПРИЈАВА СЕ ПРОСЛЕЂУЈЕ НАДЛЕЖНОМ ОРГАНУ ВЛАСТИ РАДИ ПОСТУПАЊА У СКЛАДУ СА УТВРЂЕНИМ НАДЛЕЖНОСТИМА.

НАДЛЕЖНИ ОРГАН ЈЕ ОВЛАШЋЕН ДА ВРШИ ОБРАДУ ПОДАТАКА О ЛИЦУ КОЈЕ СЕ ОБРАТИ НАДЛЕЖНОМ ОРГАНУ РАДИ ИНФОРМИСАЊА И

САВЕТОВАЊА У ВЕЗИ СА БЕЗБЕДНОШЋУ И ЗАШТИТОМ ДЕЦЕ НА ИНТЕРНЕТУ И ПОДНОШЕЊА ПРИЈАВЕ У СЛУЧАЈУ НАРУШАВАЊА ИЛИ УГРОЖАВАЊА БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ, У СКЛАДУ СА ЗАКОНОМ И ДРУГИМ ПРОПИСИМА.

ОБРАДА ПОДАТАКА О ЛИЦУ ИЗ СТАВА 4. ОВОГ ЧЛАНА ОБУХВАТА ИМЕ, ПРЕЗИМЕ И БРОЈ ТЕЛЕФОНА И/ИЛИ АДРЕСУ ЕЛЕКТРОНСКЕ ПОШТЕ И ВРШИ СЕ У СКЛАДУ СА ЗАКОНОМ КОЈИ УРЕЂУЈЕ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ, У СВРХУ УПУЋИВАЊА ПРИЈАВЕ НАДЛЕЖНИМ ОРГАНИМА РАДИ ДАЉЕГ ПОСТУПАЊА, У СКЛАДУ СА ЗАКОНОМ.

У ЦИЉУ ОБЕЗБЕЂИВАЊА КОНТИНУИТЕТА РАДА ЈЕДИНСТВЕНОГ МЕСТА ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ, НАДЛЕЖНИ ОРГАН ТРЕБА ДА:

1) БУДЕ ОПРЕМЉЕН СА ОДГОВАРАЈУЋИМ СИСТЕМИМА ЗА ПРИЈЕМ ПРИЈАВА;

2) ИМА ДОВОЉНО ЗАПОСЛЕНИХ КАКО БИ СЕ ОСИГУРАЛА ДОСТУПНОСТ У РАДУ;

3) ОБЕЗБЕДИ ИНФРАСТРУКТУРУ ЧИЈИ ЈЕ КОНТИНУИТЕТ ОСИГУРАН.

ВЛАДА БЛИЖЕ УРЕЂУЈЕ НАЧИН СПРОВОЂЕЊА МЕРА ЗА БЕЗБЕДНОСТ И ЗАШТИТУ ДЕЦЕ НА ИНТЕРНЕТУ ИЗ СТ. 1. И 3. ОВОГ ЧЛАНА.

Члан 30.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај ~~ПРАВНО ЛИЦЕ~~ ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ако:

1) НЕ ИЗВРШИ УПИС У ЕВИДЕНЦИЈУ У РОКУ ИЗ ЧЛАНА 6А ОВОГ ЗАКОНА;

~~1~~2) не донесе Акт о безбедности ИКТ система из члана 8. став 1. овог закона;

~~2~~3) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 8. став 2. овог закона;

~~3~~4) не изврши проверу усклађености примењених мера из члана 8. став 4. овог закона;

~~4~~5) НЕ ДОСТАВИ СТАТИСТИЧКЕ ПОДАТКЕ ИЗ ЧЛАНА 11Б ОВОГ ЗАКОНА;

6) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 29. став 1. тачка 1. овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице у ~~ПРАВНОМ ЛИЦУ~~ ОПЕРАТОРУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 31.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај ~~ПРАВНО ЛИЦЕ~~ ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ако о инцидентима у ИКТ систему не обавести ~~НАДЛЕЖНИ ОРГАН, ОДНОСНО ОРГАН НАДЛЕЖАН ЗА ОБЕЗБЕЂЕЊЕ ПРИМЕНЕ СТАНДАРДА У ОБЛАСТИ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА, НАРОДНУ БАНКУ СРБИЈЕ ИЛИ РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ (ЧЛАН~~ ОРГАНЕ ИЗ ЧЛАНА 11. ст. 1, 2. и ~~2.).~~ 4.ОВОГ ЗАКОНА.

За прекршај из става 1. овог члана казниће се и одговорно лице у ~~ПРАВНОМ ЛИЦУ~~ ОПЕРАТОРУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА новчаном казном у износу од 5.000,00 до 50.000,00 динара.