НАЦРТ

НАЦРТ

ЗАКОН

о информационој безбедности

I. ОСНОВНЕ ОДРЕДБЕ

Предмет уређивања

Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности субјеката приликом управљања и коришћења информационо-комуникационих система, поступци и мере за постизање високог општег нивоа информационе безбедности и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите, праћење правилне примене прописаних мера заштите, као и надлежности субјеката за надзор над спровођењем овог закона.

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 и услуге* 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 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;

(5) све типове системског и апликативног софтвера и софтверске развојне алате.

2) *оператор ИКТ система* је физичко лице у својству регистрованог субјекта, правно лице, орган или организациона јединица органа који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) *информациона безбедност* представља способност информационо-комуникационих система и мрежа да се одупру и/или ублаже, уз одређени степен поузданости, сваки догађај који би могао да угрози расположивост, интегритет,

аутентичност, непорецивост и поверљивост података који се обрађују, односно услуга које се пружају или су доступне путем тог ИКТ система;

4) *интегритет* је својство које осигурава да подаци или информације нису промењени или уништени на неовлашћени начин од када су креирани, пренети или ускладиштени;

5) *расположивост* је својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан;

6) *аутентичност* је својство којим се осигурава могућност да се провери и потврди да је информацију створио или послао онај за кога се тврди да је ту радњу извршио;

7) *поверљивост* је својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима;

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* представља представља постојање услова за нарушавање нивоа информационе безбедности, односно исправног функционисања ИКТ система, чији се ниво одређује проценом вероватноће да се деси одређена последица по ниво информационе безбедности и проценом обима те последице;

10) *рањивост* представља слабост или недостатак у ИКТ производима или услугама који се могу искористити за реализацију једне или више претњи;

11) *управљање ризиком* је скуп систематичних активности процене и контроле ризика који омогућава планирање, организовање и усмеравање мера заштите како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

12) *избегнути инцидент* представља сваки ризичан догађај који је могао угрозити расположивост, аутентичност, интегритет или поверљивост података који се чувају, преносе или обрађују у ИКТ систему или услуга које се пружају путем ИКТ система или којима се омогућава приступ ИКТ систему, али је успешно спречен или се није остварио;

13) *претња* представља сваку околност, догађај или радњу која може да угрози, поремети или на други начин штетно утиче на ИКТ систем, кориснике система и друга лица;

14) *озбиљна претња* представља претњу по информациону безбедност за коју се, с обзиром на њена техничка својства, може претпоставити да има потенцијал да изазове значајне негативне последице по ИКТ систем, његовог оператора или кориснике услуга тог оператора узрокујући значајну материјалну или нематеријалну штету;

15) *инцидент* је сваки догађај који угрожава расположивост, аутентичност, интегритет, непорецивост или поверљивост података који се чувају, преносе или обрађују или услуге које се пружају, односно које су доступне путем ИКТ система;

16) *јединствени систем за пријем обавештења о инцидентима* је информациони систем у који се уносе подаци о инцидентима и избегнутим инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

17) *управљање одговором на инцидент~~ом~~* подразумева предузимање свих радњи и поступака чији је циљ спречавање, откривање, анализа и прекид инцидента, као и предузимање других мера ради одговора на инцидент и отклањања његових последица;

18) *криза информационе безбедности* је догађај или стање које угрожава, омета рад или онемогућује рад ИКТ система од посебног значаја и при том изазива ризике, претње или последице по становништво, материјална добра или животну средину изузетно великог обима и интензитета које није могуће спречити или отклонити редовним деловањем

надлежних органа и служби, а одговор на такав догађај или стање захтева учешће више надлежних органа, као и примену одговарајућих мера;

19) *мере заштите ИКТ система* су техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система;

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

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

22) *орган* је државни орган, орган аутономне покрајине, јединица локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења;

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

24) *самостални оператори ИКТ система* су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове, службе безбедности и Народна банка Србије;

25) Центар за превезнцију безбедносних ризика у ИКТ системима (у даљем тексту: ЦЕРТ) је организациона јединица у оквиру органа или правног лица задужена за превенцију и заштиту од инцидената.

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

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

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

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

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

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

32) *информациона добра* обухватају информације које се обрађују у складу са функцијом и наменом ИКТ система; електронске записе о конфигурацији уређаја и електронске комуникационе мреже; електронске записе о интеракцијама у ИКТ системима, приступу и употреби ИКТ система (тзв. log записе); програмски кôд; техничку и корисничку документацију; електронске записе о интеракцијама у електронској комуникационој мрежи (тзв. мрежни саобраћај); информације којима се регулишу намена и коришћење ИКТ система, процеси, мере заштите и сл.

33) *услуга информационог друштва* је услуга у смислу закона којим се уређује електронска трговина;

34) *пружалац услуге информационог друштва* је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина;

35) *тачка за размену интернет саобраћаја (енгл. internet exchange point)* је мрежна структура која пружа могућност повезивања две или више независних мрежа (аутономних

система) првенствено у сврху олакшавања размене интернет саобраћаја, и која омогућује међуповезивање аутономних система, у ком случају није потребно да интернет саобраћај између аутономих система прође кроз трећи аутономни систем, те која такав саобраћај не мења и не утиче на њега на други начин;

36) *систем назива домена (ДНС)* је је дистрибуирани, хијерархијски организован систем који повезује називе домена са одговарајућим ИП адресама које се користе за усмеравање и повезивање корисничких уређаја са услугама и ресурсима на интернету;

37) *пружалац услуге ДНС-а* је субјекат који пружа услуге разрешавања ДНС упита корисницима интернета или пружа услугу ауторитативних сервера имена за називе домена које користе трећа лица, са изузетком коренских (енгл. root) сервера имена;

38) *услуга од поверења* је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

39) *пружалац услуге од поверења* је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

40) *квалификована услуга од поверења* је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

41) *пружалац квалификоване услуге од поверења* је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

42*) услуге рачунарства у клауду (енгл. „cloud computing service”)* су дигиталне услуге које омогућавају управљање на захтев и широки даљински приступ надоградивом и еластичном скупу дељивих рачунарских ресурса, укључујући и ситуације када су такви ресурси распоређени на неколико локација;

43) *услуга центра за управљање и чување података* је услуга која се пружа у оквиру инфраструктуре намењене за централизовано смештање, међуповезивање и функционисање рачунарске и мрежне опреме ради чувања, обраде и преноса података (дата центар), укључујући све објекте и инфраструктуру за дистрибуцију електричне енергије и контролу утицаја на животну средину;

44) *научноистраживачка организација* је организација у смислу закона којим се уређују наука и истраживање;

45) *јавна електронска комуникациона мрежа* је електронска комуникациона мрежа у смислу закона којим се уређују електронске комуникације;

46) *електронска комуникациона услуга* је услуга у смислу закона којим се уређују електронске комуникације;

47) *пружалац управљаних услуга* је субјект који пружа услуге у вези са постављањем, управљањем, радом и одржавањем ИКТ производа, мрежа, инфраструктуре, апликација или друге мреже и информационог система путем пружања помоћи или активног управљања које се спроводи у просторијама корисника услуге или на даљину;

48) *пружалац управљаних безбедносних услуга* је пружалац управљаних услуга који спроводи или пружа помоћ у спровођењу активности у вези са управљањем ризиком у области безбедности;

49) *регистар назива домена највишег нивоа (енгл. TLD name registry)* је субјект који је одговоран за управљање називом домена највишег нивоа (ТЛД) који му је додељен и који

доноси политике и правила за домен, управља базом регистра, генерише датотеку зоне и одржава техничку инфраструктуру сервера имена за додељени домен највишег нивоа.;

50) *пружалац услуге регистрације назива домена* је регистратор назива домена или други субјект који делује у име регистратора;

51) *ИКТ производ* је елемент или група елемената у оквиру информационо-комуникационог система;

52) *ИКТ услуга* је услуга која се у потпуности или у већој мери састоји из преноса, чувања, преузимања или обраде података коришћењем ИКТ система;

53) *ИКТ процес* је скуп активности који се обавља у циљу израде, развоја, коришћења и одржавања ИКТ производа или ИКТ услуге.

Термини који се користе у овом закону и прописима који се доносе на основу њега, а који имају родно значење, изражени у граматичком мушком роду, подразумевају природни женски и мушки пол лица на која се односе.

Начела информационе безбедности

Члан 3.

Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима:

1) начело управљања ризиком – избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;

2) начело свеобухватне заштите – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;

3) начело стручности и добре праксе – мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;

4) начело свести и оспособљености – сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине.

Обрада података о личности

Члан 4.

У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог закона поступа се у складу са начелима заштите података о личности који су дефинисани прописима који уређују заштиту података о личности.

II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Оператори приоритетних ИКТ система од посебног значаја

Члан 5.

Оператори приоритетних ИКТ система од посебног значаја су оператори ИКТ система од кључног значаја за одржавање критичних друштвених и економских активности чији би прекид или поремећај у пружању услуга имао значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио значајан системски ризик.

Оператори приоритетних ИКТ система од посебног значаја су:

1) правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:

(1) Енергетика

- производња електричне енергије;
- комбинована производња електричне и топлотне енергије;
- снабдевање електричном енергијом;
- пренос и управљање преносним системом електричне енергије;
- дистрибуција, управљање дистрибутивним системом и управљање затвореним дистрибутивним системом електричне енергије;
- складиштење електричне енергије;
- управљање организованим тржиштем електричне енергије;
- производња, дистрибуција и снабдевање топлотном енергијом;
- транспорт нафте нафтоводима, транспорт деривата нафте продуктоводима и транспорт нафте и деривата нафте другим облицима транспорта;
- истраживање, производња и прерада нафте и нафтних деривата;
- складиштење нафте и деривата нафте;
- транспорт и управљање транспортним системом за природни гас и течни нафтни гас;
- складиштење и управљање складиштем природног гаса и течног нафтног гаса;
- дистрибуција и управљање дистрибутивним системом за природни гас и течни нафтни гас;
- снабдевање и јавно снабдевање природним гасом и течним нафтним гасом;
- истраживање и прерада гаса и течног нафтног гаса;
- управљање системом течног нафтног гаса;
- производња, складиштење и пренос водоника.

(2) Саобраћај

- обављање јавног авио- превоза уз важећу оперативну дозволу;
- управљање аеродромом;
- услуге контроле летења;
- управљање јавном железничком инфраструктуром;
- послови железничких предузећа;
- обављање превоза путника и терета унутрашњим водама;
- управљање лукама;
- управљање бродским саобраћајем (ВТС);
- управљање путном инфраструктуром;
- управљање интелигентним транспортним системима (ИТС).

(3) Банкарство и финансијска тржишта

- послови финансијских институција, које су под надзором Народне банке Србије или Комисије за хартије од вредности;

- послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;
- послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;
- послови клиринга финансијских инструмената, у смислу закона којим се уређује тржиште капитала;
- послови пружалаца услуга повезаних с дигиталном имовином, у смислу закона којима се уређује дигитална имовина.

(4) Здравство

- пружање здравствене заштите;
- рад националних референтних лабораторија;
- истраживање и развој лекова;
- производња основних фармацеутских производа и препарата;
- производња медицинских производа који се сматрају критичним током ванредног стања у области јавног здравља.

(5) Вода за пиће

- снабдевање и дистрибуција воде намењене за људску потрошњу. изузев дистрибутера којима наведени послови нису претежни део њихове делатности.

(6) Отпадне воде

- сакупљање, одвођење или пречишћавање комуналних отпадних вода, отпадних вода насеља и привреде, изузев привредних субјеката којима наведени послови нису претежни део њихове делатности.

(7) Дигитална инфраструктура

- пружање услуга рачунарства у клауду;
- пружање услуге центра за чување и складиштење података.

(8) Управљање ИКТ услугама које се пружају операторима приоритетних ИКТ система од посебног значаја

- пружање управљаних услуга;
- пружање управљаних безбедносних услуга;

(9) Остале области

- управљање нуклеарним објектима;
- пружање квалификованих услуга од поверења, пружање услуга ДНС-а, и управљање регистром домена највишег нивоа, са изузетком оператора коренских сервера имена;
- обављање делатности електронских комуникација;
- тачка за размену интернет саобраћаја;
- издавање Службеног гласника Републике Србије и вођење Правно-информационог система Републике Србије;
- области у којој у Републици Србији постоји само један пружалац услуге и која је неопходна за обављање критичних друштвених и привредних делатности.

2) органи;

3) субјекти који су одређени као оператори критичне инфраструктуре у складу са прописима којима се уређује критична инфраструктура.

Оператори важних ИКТ система од посебног значаја

Члан 6.

Оператори важних ИКТ система од посебног значаја су оператори ИКТ системи чији би прекид или поремећај у пружању услуга могао да има значајан утицај на јавни интерес, функционисање других сектора или би створио значајан системски ризик.

Оператори важних ИКТ система од посебног значаја су:

1) правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:

- поштанске услуге у смислу закона којим се уређује област поштанских услуга;
- управљање отпадом, у смислу закона којим се уређује управљање отпадом, изузев привредних субјеката којима наведени посао није претежни део њихове делатности;
- производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије;
- производња, обрада и дистрибуција хране у сегменту велепродаје и индустријске производње и прераде;
- производња рачунара, електронских и оптичких производа;
- производња електричне опреме;
- производња машина и уређаја;
- производња моторних возила, приколица и полуприколица и производња остале опреме за превоз;
- производња медицинских уређаја и производња in vitro дијагностичких медицинских средстава;
- услуге информационог друштва у смислу закона о електронској трговини;
-
- производња, промет и превоз наоружања и војне опреме.

2) научноистраживачке институције;

3) правна и физичка лица у својству регистрованог субјекта и органи из члана 5. овог закона, а који не спадају у операторе приоритетних ИКТ система од посебног значаја према критеријумима за одређивање оператора.

Подзаконски акт којим се ближе уређују услови, општи и секторски критеријуми за одређивање оператора приоритетних и важних ИКТ система од посебног значаја доноси Влада, на предлог министарства надлежног за послеве информационе безбедности.

Министарства у чијим надлежностима су области у којима оператори приоритених и важаних ИКТ система од посебног значаја обављају делстности, дужни су да у поступку израде подзаконског акта из става 3. овог члана, доставе министарству надлежном за послове информационе безбедности предлоге секторских критеријума ради одређивања оператора ИКТ система од посебног значаја.

Обавезе оператора ИКТ система од посебног значаја

Члан 7.

Оператор ИКТ система од посебног значаја, сходно овом закону, у обавези је да:

1) се упише у евиденцију ИКТ система од посебног значаја;

2) предузме одговарајуће техничке, оперативне,организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената;

3) изврши процену ризика и донесе акт о процени ризика;

4) донесе акт о безбедности ИКТ система од посебног значаја;

5) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање:

(1) два пута годишње ако је оператор приоритетног ИКТ система од посебног значаја

(2) једном годишње ако је оператор важног ИКТ система од посебног значаја;

6) 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 са трећим лицима;

7) доставља обавештења, без одлагања, о сваком инциденту који је значајно угрозио безбедност ИКТ систем од посебног значаја;

8) доставља обавештења о озбиљним претњама за ИКТ систем од посебног значаја;

9) достави статистичке податке о инцидентима и избегнутим инцидентима у ИКТ системима.

Обавезе самосталних оператора

Члан 8.

Самостални оператор дужан је да:

1) се упише у евиденцију ИКТ система од посебног значаја;

2) предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање два пута 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 са трећим лицима.

Самостални оператори могу да међусобно размењују информације о инцидентима са Канцеларијом за информациону безбедност, а по потреби и са другим организацијама.

На самосталне операторе не примењују се одредбе овог закона о пријављивању инцидената који значајно угрожавају информациону безбедност и одредбе о достављању статистичких података о инцидентима.

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.

НАЦРТ

Евиденција оператора ИКТ система од посебног значаја

Члан 9.

Министарство надлежно за послове информационе безбедности (у даљем тексту: Министарство) успоставља и води евиденцију приоритетних и важних ИКТ система од посебног значаја (у даљем тексту: Евиденција) која садржи:

1) назив, матични број и седиште оператора ИКТ система од посебног значаја;

2) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора задуженог за одржавање и управљање ИКТ системом 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, односно да ли ИКТ систем од посебног значаја потпада под приоритетан или важан;

5) податак о делатности оператора ИКТ система од посебног значаја;

6) адресни опсег интернет протокола (енгл. „IP address range“) који припадају ИКТ систему од посебног значаја, а који обухвата податке о јавним статичким ИП адресама;

7) веб странице оператора ИКТ система од посебног значаја;

8) број локација на којима се ИКТ систем од посебног значаја налази.

Поред података из става 1. овог члана, евиденција може да садржи и друге допунске податке о ИКТ систему од посебног значаја..

Самостални оператори ИКТ система изузети су од обавезе достављања података из тач. 4), 5), 6) и 8) став 1. овог члана.

Подзаконски акт којим се ближе уређује садржај и структура евиденције, као и начин подношења захтева за унос и промену података у Евиденцији доноси Министарство.

Оператор ИКТ система од посебног значаја дужан је да Министарству достави податке из стс 1. и 2. овог члана најкасније 90 дана од дана усвајања прописа из става 4. овог члана, односно 90 дана од дана успостављања ИКТ система од посебног значаја.

Оператор ИКТ система од посебног значаја дужан је да у случају промене података из става 1. овог члана о томе обавести Министарство у року од 15 дана од дана настанка промене.

Подаци из става 1. тач. 2) и 3) обрађују се у сврху извршења одредби овог закона у погледу достављања обавештења и упозорења значајних за безбедност ИКТ система од посебног значаја, као и ради успостављања комуникације и остваривања сарадње у циљу отклањања штетних последица инцидената и превентивног деловања.

Подаци из става 1. тач. 2) и 3) обрађују се у складу са начелима обраде података о личности и сходним одредбама закона којим се уређује заштита података о личности, а чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 5. овог члана.

Министарство ставља на располагање Евиденцију Националном ЦЕРТ-у.

Евиденција представља тајни податак у смислу закона којим се уређује тајност података.

Мере заштите ИКТ система од посебног значаја

Члан 10.

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 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) прикупљање података о претњама по информациону безбедност ИКТ система;

3) постизање безбедности рада на даљину и употребе мобилних уређаја;

4) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност, односно да обезбеди одржавање основних и по потреби напредних информатичких обука за све запослене и ангажована лица која имају приступ ИКТ системима

5) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;

6) идентификовање информационих добара и одређивање одговорности за њихову заштиту;

7) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;

8) заштиту носача података;

9) ограничење приступа подацима и средствима за обраду података;

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

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

12) предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података;

13) примена мера заштите ради спречавања отицања података;

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

15) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;

16) обезбеђивање исправног и безбедног функционисања средстава за обраду података;

17) примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду;

18) праћење ИКТ система у циљу откривања рањивости и претњи

19) ограничење приступа интернет страницама које могу потенцијално да наруше безбедност ИКТ система;

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

21) заштиту од губитка података;

22) чување података о догађајима који могу бити од значаја за безбедност ИКТ система;

23) обезбеђивање интегритета софтвера и оперативних система;

24) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

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

26) заштиту података у комуникационим мрежама укључујући уређаје и водове;

27) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;

28) испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

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

30) процедуре за чување и брисање информација у ИКТ системима, у складу са прописима;

31) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;

32) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;

33) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама, као и примену мера санације последица инцидента;

34) мере које обезбеђују континуитет обављања посла у ванредним околностима које су дефинишу Планом континуитета обављања посла.

Подзаконски акт којим се ближе уређују мере заштите ИКТ система уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада доноси Влада, на предлог Министарства.

Акт о процени ризика ИКТ система од посебног значаја

Члан 11.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о процени ризика за ИКТ системе (у даљем тексту: акт о процени ризика) којима управља.

Актом о процени ризика врши се процена ризика за ИКТ систем од посебног значаја с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај.

Акт о процени ризика ревидира се најмање једном годишње.

Акт о процени ризика израђује се у складу са општом методологијом за процену ризика у ИКТ системима од посебног значаја коју доноси Канцеларија за информациону безбедност. Оператор ИКТ система од посебног значаја није у обавези да донесе акт из става 1. овог члана у случају када има дефинисану процену ризика, у другим постојећим интерним актима, која обухвата захтеве из опште методологије из става 4. овог члана.

Акт о безбедности ИКТ система од посебног значаја

Члан 12.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система (у даљем тексту: акт о безбедности).

Актом о безбедности одређују се мере заштите, а нарочито 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 мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

Оператор приоритетног ИКТ система од посебног значаја дужан је да, самостално или уз ангажовање спољних експерата, врши проверу усклађености примењених мера ИКТ система са актом о безбедности и то најмање два пута годишње и да о томе сачини извештај.

Оператор важног ИКТ система од посебног значаја дужан је да, самостално или уз ангажовање спољних експерата, врши проверу из претходног става најмање једном годишње и да о томе сачини извештај.

Подзаконски акт којим се уређује ближи садржај акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери доноси Влада на предлог Министарства.

Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност

Члан 13.

Оператори ИКТ система од посебног значаја дужани су да доставе обевештење о инциденту који може да има значајан утицај на нарушавање информационе безбедности, без одлагања, а најкасније у року од 24 сата од када су сазнали за инцидент.

Инциденти који могу да имају значајан утицај на нарушавање информационе безбедности су:

1) инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) инциденти који утичу на велики број корисника услуга, или трају дужи временски период;

3) инциденти 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) инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденти који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;

6) инциденти који су настали као последица инцидента у ИКТ систему оператора приоритетних ИКТ система од посебног значаја који обављају делатности у области дигиталне инфраструктуре, из члана 5. став 2. тачка 1) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге у области дигиталне инфраструктуре;

7) инциденти који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима.

Оператори ИКТ система од посебног значаја дужни су да пријаве и избегнуте инциденте који представљају озбиљну претњу и који би довели до значајног повећања ризика од наступања последица из става 2. 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.

Достављање обавештења о инцидентима

Члан 14.

Оператори ИКТ система од посебног значаја дужни су да обавештења о инцидентима доставе у јединствени систем за пријем обавештења о инцидентима који одржава Канцеларија за информациону безбедност.

Оператори приоритетних ИКТ система од посебног значаја који обављају делатности у области банкарства и финансијских тржишта из члана 5. став 2. тачка 1) подтачка (3) алинеја прва, друга и пета овог закона, дужни су да обавештење о инциденту доставе Народној банци Србије.

Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа, дужни су да обавештење о инциденту доставе регулаторном телу за електронске комуникације и поштанске услуге.

Народна банка Србије и регулаторно тело за електронске комуникације и поштанске услуге дужни су да добијена обавештења из ст. 2 и 3. овог члана проследе у јединствени систем за пријем обавештења о инцидентима.

Оператори ИКТ система од посебног значаја, осим оператора приоритетних ИКТ система из става 2. и 3. овог члана, дужни су да обавесте о инциденту кориснике којима пружају услуге, без одлагања, у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга, као и о мерама које корисници могу да предузму и употребе у циљу умањења или елиминације штетних последица инцидента.

Оператори приоритетних ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентма у складу са посебним прописима.

Орган коме је у складу са овим законом упућено обавештење о инциденту, уколико је реч о ИКТ систему од посебног значаја који је одређен као критична инфраструктура у складу са законом којим се уређује критична инфраструктура, информацију о томе прослеђује Министарству унутрашњих послова и министарствима надлежним за секторе критичне инфраструктуре.

Садржај обавештења о инциденту

Члан 15.

Обавештење о инциденту мора да садржи следеће податке:

1) податке о подносиоцу пријаве,
2) врсту и опис инцидента и процену да ли је инцидент последица кривичног дела,
3) датум и време почетка инцидента и трајање инцидента,
4) последице које је инцидент изазвао,
5) предузете активности ради ублажавања последица инцидента,
6) иницијалну процену нивоа опасности и утицаја инцидента на ИКТ систем од посебног значаја, као и индикаторе компромитације,
7) информацију о евентуалном прекограничном дејству инцидента,
8) друге релевантне информације, по потреби.

Значај инцидената према нивоу опасности

Члан 16.

Инциденти у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности сврставају се према нивоу опасности, имајући у виду последице инцидента у следеће нивое опасности:
1) низак;
2) средњи;
3) висок;
4) веома висок.
Подзаконски акт којим се уређује поступак обавештавања о инцидентима, обрасци за обавештавање, листа инцидената према врстама и класификација инцидената према нивоу опасности доноси Влада, на предлог Министарства.

Оперативни тим за реаговање на инциденте

Члан 17.

У циљу координисане реакције на инциденте високог и веома високог нивоа Канцеларија за информациону безбедност образује стални оперативни тим од представника Канцеларије за информацону безбедност, Министарства и ЦЕРТ-ова самосталних оператора.
По потреби, састанцима оперативног тима могу присуствовати и представници посебних ЦЕРТ-ова, као и друга лица.

План за реаговање у случају инцидента високог нивоа и криза информационе безбедности

Члан 18.

Влада доноси План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности, а на предлог Канцеларије за информациону безбедност.
План из става 1. овог члана обухвата:
1) циљеве мера и активности за реаговање у случају инцидената високог нивоа и криза информационе безбедности;
2) деловање надлежних органа у циљу спровођења плана;

3) опис процедура у случају инцидената високог нивоа и криза информационе безбедности;

4) активности за унапређење способности реаговања на инциденте, а пре свега планови одговарајућих вежби и обука;

5) моделе сарадње са приватним, невладиним и академским сектором;

6) међусобну сарадњу надлежних органа.

Приликом израде плана из става 1. овог члана Канцеларија за информациону безбедност сарађује са другим органима и правним лицима.

План из става 1. овог члана се периодично мења и допуњује у складу са потребама и новим околностима, а у целини се поново израђује и доноси сваке треће године, а уколико су се околности у значајној мери промениле и раније.

Поступање по пријему обавештења о инциденту

Члан 19.

По пријему обавештења о инциденту у ИКТ систему од посебног значаја, Канцеларија за информациону безбедност поступа у складу са надлежностима утврђеним законом, односно прикупља, анализира и размењује информације о ризицима за безбедност ИКТ система, као и инциденту, и у вези тога обавештава, пружа подршку, упозорава и саветује оператора ИКТ система од посебног значаја и врши друге послове из своје надлежности.

Канцеларија за информациону безбедност, након извршене анализе, утврђује ниво опасности инцидента.

Када је неопходно да јавност буде упозната са инцидентом или када је инцидент такав да је од интереса за јавност, Канцеларија за информациону безбедност може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио.

Канцеларија за информациону безбедност, Народна банка Србије и регулаторно тело за електронске комуникације и поштанске услуге дужни су да обевештења о инцидентима проследе:

1) надлежном јавном тужилаштву, односно министарству надлежном за унутрашње послове, у случају да је инцидент везан за извршење кривичних дела која се гоне по службеној дужности,

2) органу надлежном за послове одбране и националне безбедности у случају да је инцидент повезан са значајним нарушавањем информационе безбедности које има или може имати за последицу угрожавање одбране или националне безбедности.

Приликом управљања инцидентом Канцеларија за информациону безбедност, Народна банка Србије и регулаторно тело за електорнске комуникације и поштанске услуге означавају обавештење о инциденту, односно информације о инциденту у складу са прописима и TLP (енг.„traffic light protocol”) протоколом.

Поступање у случају инцидента нивоа опасности „низак”

Члан 20.

У случају инцидената којима је у складу са класификацијом утврђен ниво опасности „низак” Канцеларија за информациону безбедност по потреби даје препоруке за поступање оператору ИКТ система од посебног значаја.

Поступање у случају инцидента нивоа опасности „средњи”

Члан 21.

У случају инцидената којима је у складу са класификацијом утврђен ниво опасности „средњи” Канцеларија за информациону безбедност, даје препоруке за поступање оператору ИКТ система од посебног значаја.

Поступање у случају инцидента нивоа опасности „висок”

Члан 22.

У случају инцидената којима је у складу са класификацијом утврђен ниво опасности „висок” Канцеларија за информациону безбедност дужна је о томе обавестити Министарство.

Канцеларија за информациону безбедност сазива састанак оперативног тима из члана 17. овог закона ради међусобне координације током реаговања по пријављеном инциденту и припреме препорука и мера за решавање инцидента.

Министарство након састанка из става 2. овог члана, сазива седницу Тела за координацију послова информационе безбедности.

Након завршетка инцидента Канцеларија за информациону безбедност сачињава завршни извештај који доставља Министарству у року од 30 дана након завршеног инцидента.

Поступање у случају инцидента нивоа опасности „веома висок”

Члан 23.

У случају инцидена којем је у складу са класификацијом утврђен ниво опасности „веома висок“ и који представаља кризу информационе безбедности, руковођење и координацију спровођења мера и задатака предузима Влада.

Канцеларија за информациону безбедност сазива састанак оперативног тима из члана 17. овог закона ради давања предлога за проглашавање кризе информационе безбедности, у складу са Планом за реаговање у случају инцидента високог нивоа и кризе информационе безбедности, који садржи:

1) податке о инциденту;
2) информације о предузетим мерама;
3) разлоге за проглашење кризе инфорамционе безбедности;
4) задужење органа за поступање у складу са својим надлежностима;
5) мере за решавање кризе.

Предлог за проглашење кризе информацоине безбедности упућује се Министарству.

Влада, на предлог Министарства доноси одлуку о проглашењу кризе информационе безбедности и задужује органе да поступају према предложеним мерама у складу са својим надлежностима.

Министарство након састанка из става 2. овог члана, сазива седницу Тела за координацију послова информационе безбедности.

Канцеларија за информациону безбедност координира оперативним радом органа из става 2. овог члана у решавању кризе информационе безбедности и најмање једном недељно извештава Министарство и Владу о свим активностима.

Предлог за проглашење завршетка кризе информацоине безбедности упућује се Министарству.

Одлуку о проглашењу завршетка кризе информационе безбедности доноси Влада на предлог Министарства.

Након завршетка кризе информационе безбедности Канцеларија за информациону безбедност сачињава завршни извештај који доставља Министарству и Влади у року од 30 дана након завршетка кризе.

Извештавање током и након инцидента

Члан 24.

Оператори ИКТ система од посебног значаја дужни су да:

1) достављају извештај о инциденту, током трајања инцидента, са описом мера које су предузете за решавање инцидента, у јединствени систем за пријем обавештења о инцидентима и то:

(1) на свака три дана у случају инцидента средњег нивоа;

(2) на свака 24 сата у случају инцидената високог и веома високог нивоа;

2) достављају обавештења и додатне извештаје о битним догађајима у вези са инцидентом и активностима које предузимају, на захтев Националног ЦЕРТ-а;

3) достављају завршни извештај о инциденту у року од 15 дана од дана престанка инцидента, који садржи следеће податке:

(1) врсту и опис инцидента,

(2) време и трајање инцидента,

(3) последице које је инцидент изазвао,

(4) информацију о евентуалном прекограничном дејству инцидента,

(5) предузете активности ради отклањања последица инцидента и, по потреби, друге информације од значаја за евидентирање инцидента и статистичку обраду.

Након завршеног инцидента Канцлеарија за информациону безбедност припрема препоруке и савете за заштиту од потенцијалних ризика, на основу анализе извршеног инцидента.

Достављање статистичких података о инцидентима

Члан 25.

Оператор ИКТ система од посебног значаја дужан је да, поред обавештавања о инцидентима из члана 13. овог закона, достави Националном ЦЕРТ-у статистичке податке

о свим инцидентима у ИКТ систему, укључујући и избегнуте инциденте, у претходној години најкасније до 28. фебруара текуће године.

Национални ЦЕРТ извештаје о статистичким подацима доставља Министарству.

Врсту, форму и начин достављања статистичких података из става 1. овог члана утврђује Национални ЦЕРТ.

III. ОРГАНИ НАДЛЕЖНИ ЗА ПРЕВЕНЦИЈУ И ЗАШТИТУ ОД БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ

Надлежни орган

Члан 26.

Орган државне управе надлежан за информациону безбедност је министарство надлежно за послове информационе безбедности

У оквиру својих надлежности Министарство:

1) припрема и предлаже прописе и планска докумената из области информационе безбедности у складу са овим законом;

2) води евиденцију оператора ИКТ система од посебног значаја;

3) врши надзор над радом Канцеларије за информациону безбедност;

4) врши инспекцијски надзор над радом оператора ИКТ система од посебног значаја;

5) остварује међународну сарадњу у оквиру својих надлежности.

Тело за координацију послова информационе безбедности

Члан 27.

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 за информациону безбедност, Канцеларије Савета за националну безбедност и заштиту тајних података, органа надлежног за пројектовање, усклађивање, развој и функционисање система електронске управе, Генералног секретаријата Владе, Народне банке Србије и регулаторног тела за електронске комуникације и поштанске услуге.

У функцији унапређења појединих области информационе безбедности формирају се стручне радне групе Тела за координацију у које се укључују и представници других органа, 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.

Канцеларија за информациону безбедност

Члан 28.

Ради обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији оснива се Канцеларија за информациону безбедност (у даљем тексту: Канцеларија), као посебна организација у смислу закона којим се уређује положај државне управе.

Канцеларија има својство правног лица.

Радом Канцеларије руководи директор кога именује Влада, а који мора бити лице одговарајуће стручности које има најмање 5 година искуства на пословима руковођења.

Канцеларија има заменика директора, који мора бити лице одговарајуће стручности, који се именује и има овлашћења у складу са прописима о државној управи.

Запослена лица у Канцеларији која су распоређена на радна места на којима се обављају сложени послови под сталним или привременим отежаним околностима, имају право на увећање коефицијента основне плате у износу до 30%, у складу са актом Владе.

Надзор над радом Канцеларије

Члан 29.

Надзор над радом Канцеларије у вршењу послова спроводи Министарство, које периодично, а најмање једном годишње, проверава да ли Канцеларија располаже одговарајућим ресурсима и врши послове у складу са овим законом.

Надлежности Канцеларије

Члан 30.

Канцеларија у оквиру своје надлежности обавља следеће послове и то:

1) обавља послове Националног ЦЕРТ-а;
2) обавља послове ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе
3) сарадњу на националном нивоу у области информационе безбедности
4) послове јединствене тачке контакта;
5) послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга;
6) прописује минималне мере заштите ИКТ система органа, уважавајући начела из члана 3. овог закона, мере заштите из члана 10. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада
7) у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиногсектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима;
8) извештава Министарство на кварталном нивоу о предузетим активностима
9) друге послове у складу са овим законом.

Послови Националног ЦЕРТ-а

Члан 31.

У оквиру послова превенције и заштите од безбедносних ризика и инцидената Канцеларија врши послове Националног ЦЕРТ-а и то:

1) прикупља и размењује информације о претњама, рањивостима и инцидентима и пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији као и јавност.

2) прати стање о инцидентима у Републици Србији;

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

4) реагује без одлагања по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања;

5) на захтев оператора ИКТ система од посебног значаја, пружа помоћ у праћењу стања безбедности ИКТ система у реалном времену или приближно реалном времену;

6) на захтев оператора ИКТ система од посебног значаја, врши проактивно скенирање ИКТ система у циљу утврђивања рањивости које могу да потенцијално знатно наруше безбедност ИКТ система, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;

7) поступа као координатор за потребе координираног откривања рањивости, у складу са овим законом;

8) учествује у развоју и коришћењу технолошких алата за размену информација са операторима ИКТ система од посебног значаја и других субјеката са којима сарађује;

9) континуирано израђује анализе ризика и инцидената, на основу прикупљених информација;

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

11) води Евиденцију посебних ЦЕРТ-ова

12) води базу рањивости

13) припрема извештаје на кварталном нивоу о предузетим активностима.

Национални ЦЕРТ промовише усвајање и коришћење прописаних и стандардизованих процедура за:

1) управљање инцидената;

2) класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената;

3) управљање кризним ситуацијама;

4) координирано откривање рањивости.

Национални ЦЕРТ је овлашћен да врши обраду података о лицу које пријави инцидент, при чему обрада података о лицу обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Национални ЦЕРТ обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације.

Послови ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе

Члан 32.

У оквиру послова ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе (у даљем тексту: мрежа еУправе) Канцеларија обавља следеће послове:

1) врши заштиту мреже еУправе;

2) обавља координацију и сарадњу са операторима ИКТ система које повезује мрежа еУправе у превенцији инцидената;

3) активно учествује у откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;

4) врши проактивно скенирање мреже оператора ИКТ система од посебног значаја који су корисници мреже, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;

5) у случају откривене рањивости:

(1) обавести операторе ИКТ система који су корисници мреже еУправе о томе,

(2) налаже операторима ИКТ система од посебног значаја који су корисници мреже да предузму адекватне мере заштите у циљу спречавања, смањења и отклањања последица индицента;

6) издаје стручне препоруке за заштиту ИКТ система органа, осим ИКТ система за рад са тајним подацима;

7) прописује процедуре за поступање оператора ИКТ система од посебног значаја који користе мреже у случају инцидента;

8) у сарадњи са надлежним органима врши процену потребе за стручним усавршавањем запослених у операторима ИКТ система од посебног значаја који користе мрежу;

9) планира и организује процедуралне и практичне вежбе у области информационе безбедности за запослене у операторима ИКТ система од посебног значаја који користе мрежу;

10) израђује предлоге за унапређење безбедносних карактеристика мреже еУправе;

11) израђује анализе ризика и инцидената у оквиру мреже еУправе;

12) обавља друге послове у складу са законом у циљу унапређења информационе безбедности мреже еУправе.

Сарадња на националном нивоу

Члан 33.

Национални ЦЕРТ непосредно сарађује са Министарством, ЦЕРТ-ом мреже еУправе, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система.

Национални ЦЕРТ/, ЦЕРТ мреже еУправе и ЦЕРТ-ови самосталних оператора ИКТ система одржавају међусобне састанке у организацији Канцеларије најмање три пута годишње, као и по потреби у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Састанцима из става 2. овог члана присуствују и представници Министарства, а по позиву могу да присуствују и представници посебних ЦЕРТ-ова, као и друга лица.

Приликом сарадње са субјектима из става 1. овог члана Национални ЦЕРТ је дужан да обезбеди ефективну, ефикасну и безбедну размену информација уз примену адекватних процедура, укључујући „traffic light protocol" (TLP), и поштујући прописе о заштити података о личности.

Међународна сарадња и послови јединствене тачке контакта

Члан 34.

Национални ЦЕРТ 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 високоризични;

2) превазилазе или могу да превазиђу националне капацитете;

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

Приликом размене података из става 2. овог члана, Национални ЦЕРТ је дужан да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система.

Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Национлни ЦЕРТ ће о томе обавестити надлежно јавно тужилаштво, које ће самостално или преко министарства надлежног за унутрашње послове у званичној процедури проследити пријаву у складу са потврђеним међународним уговорима.

Национални ЦЕРТ обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 35.

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 са седиштем на територији Републике Србије, које је уписано у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ.

Упис у евиденцију посебних ЦЕРТ-ова, коју води Национални ЦЕРТ, 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, а у сврху ангажовања посебних ЦЕРТ-ова у случају безбедносних ризика и инцидената у ИКТ системима.

Национални ЦЕРТ прописује садржај, начин уписа и вођења евиденције из става 3. овог члана.

База рањивости

Члан 36.

Национални ЦЕРТ успоставља и одржава базу рањивости ИКТ производа и ИКТ услуга у Републици Србији и омогућава физичким и правним лицима, као и произвођачима, добављачима и пружаоцима услуге у ИКТ систему, да на добровољној бази пријаве рањивости у ИКТ производима или ИКТ услугама, а које се могу пријавити анонимно.

База рањивости ИКТ производа и ИКТ услуга садржи:

1) податке о рањивости;

2) податке о рањивостима ИКТ производа или ИКТ услуга.

Национални ЦЕРТ прописује садржај, процедуре верификације рањивости, начин уписа и вођења регистра.

Заштита деце при коришћењу информационо-комуникационих технологија

Члан 37.

Министарство 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 ради поступања у складу са утврђеним надлежностима.

Министарство је овлашћено да врши обраду података о лицу које се обрати Надлежном органу у складу са законом који уређује заштиту података о личности 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 сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Подаци о личности из става 5. овог члана чувају се у роковима предвиђеним прописима који уређују канцеларијско пословање.

У циљу обезбеђивања континуитета рада јединственог места за пружање савета и пријем пријава у вези безбедности деце на интернету, Министарство 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.

Подзаконски акт којим се ближе уређује начин спровођења мера за безбедност и заштиту деце на интернету из ст. 1. и 3. овог члана доноси Влада на предлог Министарств.

IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Надлежност

Члан 38.

Министарство надлежно за послове одбране је надлежно за послове информационе безбедности који се односе на одобравање криптографских производа који се користе за заштиту преноса и чувања података који су одређени као тајни, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења и послове и задатке у складу са законом и прописима донетим на основу закона.

Послови и задаци

Члан 39.

У складу са овим законом, министарство надлежно за послове одбране:

1) организује и реализује научноистраживачки рад у области криптографске безбедности и заштите од КЕМЗ;

2) развија, имплементира, верификује и класификује криптографске алгоритме;

3) истражује, развија, верификује и класификује сопствене криптографске производе и решења заштите од КЕМЗ;

4) верификује и класификује домаће и стране криптографске производе и решења заштите од КЕМЗ;

5) дефинише процедуре и критеријуме за евалуацију криптографских безбедносних решења;

6) врши функцију националног органа за одобрења криптографских производа и обезбеђује да ти производи буду одобрени у складу са одговарајућим прописима;

7) врши функцију националног органа за заштиту од КЕМЗ;

8) врши проверу ИКТ система са аспекта криптобезбедности и заштите од КЕМЗ;

9) врши функцију националног органа за дистрибуцију криптоматеријала и дефинише управљање, руковање, чување, дистрибуцију и евиденцију криптоматеријала у складу са прописима;

10) планира и координира израду криптопараметара (параметара криптографског алгоритма), дистрибуцију криптоматеријала и заштите од компромитујућег електромагнетног зрачења у сарадњи са самосталним операторима ИКТ система;

11) формира и води централни регистар верификованог и дистрибуираног криптоматеријала;

12) формира и води регистар издатих одобрења за криптографске производе;

13) израђује електронске сертификате за криптографске системе засноване на инфраструктури јавних кључева (Public Key Infrastructure – PKI);

14) предлаже доношење прописа из области криптобезбедности и заштите од КЕМЗ на основу овог закона;

15) врши послове стручног надзора у вези криптобезбедности и заштите од КЕМЗ;

16) пружа стручну помоћ носиоцу инспекцијског надзора информационе безбедности у области криптобезбедности и заштите од КЕМЗ;

17) пружа услуге уз накнаду правним и физичким лицима, изван система јавне власти, у области криптобезбедности и заштите од КЕМЗ према пропису Владе на предлог министра одбране;

18) сарађује са домаћим и међународним органима и организацијама у оквиру надлежности уређених овим законом.

Средства остварена од накнаде за пружање услуга из става 1. тачка 17) овог члана су приход буџета Републике Србије.

Компромитујуће електромагнетно зрачење

Члан 40.

Мере заштите од КЕМЗ у ИКТ системима за руковање са тајним подацима примењују се у складу са прописима којима се уређује заштита тајних података.

Мере заштите од КЕМЗ могу примењивати на сопствену иницијативу и оператори ИКТ система којима то није законска обавеза.

За све техничке компоненте система (уређаје, комуникационе канале и просторе) код којих постоји ризик од КЕМЗ, а што би могло довести до нарушавања информационе безбедности из става 1. овог члана, врши се провера заштићености од КЕМЗ и процена ризика од неовлашћеног приступа тајним подацима путем КЕМЗ.

Проверу заштићености од КЕМЗ врши министарство надлежно за послове одбране.

Самостални оператори ИКТ система могу вршити проверу КЕМЗ за сопствене потребе.

Подзаконски акт којим се ближе уређују услови за проверу КЕМЗ и начин процене ризика од отицања података путем КЕМЗ доноси Влада, на предлог министарства надлежног за послове одбране.

Мере криптозаштите

Члан 41.

Мере криптозаштите за руковање са тајним подацима у ИКТ системима примењују се у складу са прописима којима се уређује заштита тајних података.

Мере криптозаштите се могу применити и приликом преноса и чувања података који нису означени као тајни у складу са законом који уређује тајност података, када је на основу закона или другог правног акта потребно применити техничке мере ограничења приступа подацима и ради заштите интегритета, аутентичности и непорецивости података.

Подзаконски акт којим се уређују техничкие услови за криптографске алгоритме, параметре, протоколе и информациона добра у области криптозаштите који се у Републици Србији користе у криптографским производима ради заштите тајности, интегритета, аутентичности, односно непорецивости података доноси Влада, на предлог министарства надлежног за послове одбране.

Одобрење за криптографски производ

Члан 42.

Криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни, у складу са законом, морају бити верификовани и одобрени за коришћење.

Подзаконски акт којим се ближе уређују услови које морају да испуњавају криптографски производи из става 1. овог члана доноси Влада, на предлог министарства надлежног за послове одбране.

Издавање одобрења за криптографски производ

Члан 43.

Одобрење за криптографски производ издаје министарство надлежно за послове одбране, на захтев оператора ИКТ система, произвођача криптографског производа или другог заинтересованог лица.

Одобрење за криптографски производ се може односити на појединачни примерак криптографског производа или на одређени модел криптографског производа који се серијски производи.

Одобрење за криптографски производ може имати рок важења.

Министарство надлежно за послове одбране решава по захтеву за издавање одобрења за криптографски производ у року од 45 дана од дана подношења уредног захтева, који се може продужити у случају посебне сложености провере највише за још 60 дана.

Против решења из става 4. овог члана жалба није допуштена, али може да се покрене управни спор.

Министарство надлежно за послове одбране води регистар издатих одобрења за криптографски производ.

Регистар из става 6. овог члана од података о личности садржи податке о одговорним лицима, и то: име, презиме, функција и контакт податке као што су адреса, број телефона и адреса електронске поште.

Министарство надлежно за послове одбране објављује јавну листу одобрених модела криптографских производа за све моделе криптографских производа за које је у захтеву за издавање одобрења наглашено да модел криптографског производа треба да буде

на јавној листи и ако је захтев поднео произвођач или лице овлашћено од стране произвођача предметног криптографског производа.

Министарство надлежно за послове одбране претходно издато одобрење за криптографски производ може повући или променити услове из ст. 2. и 3. овог члана из разлога нових сазнања везаних за техничка решења примењена у производу, а која утичу на оцену степена заштите који пружа производ.

Подзаконски акт којим се ближе уређује садржај захтева за издавање одобрења за криптографски производ, услове за издавање одобрења за криптографски производ, начин издавања одобрења и садржај регистра издатих одобрења за криптографски производ доноси Влада, на предлог министарства надлежног за послове одбране.

Опште одобрење за коришћење криптографских производа

Члан 44.

Самостални оператори ИКТ система имају опште одобрење за коришћење криптографских производа.

Оператор ИКТ система из става 1. овог члана самостално оцењује степен заштите који пружа сваки појединачни криптографски производ који користи, а у складу са прописаним условима.

Ставови 1. и 2. не односе се на Народну банку Србије.

Регистри у криптозаштити

Члан 45.

Самостални оператори ИКТ система који имају опште одобрење за коришћење криптографских производа устројавају и воде регистре криптографских производа, криптоматеријала, правила и прописа и лица која обављају послове криптозаштите.

Регистар лица која обављају послове криптозаштите од података о личности садржи следеће податке о лицима која обављају послове криптозаштите: презиме, име оца и име, датум и место рођења, матични број, телефон, адресу електронске поште, школску спрему, податке о завршеном стручном оспособљавању за послове криптозаштите, назив радног места, датум почетка и завршетка рада на пословима криптозаштите.

Регистар криптоматеријала за руковање са страним тајним подацима води Канцеларија Савета за националну безбедност и заштиту тајних података, у складу са ратификованим међународним споразумима.

Подзаконски акт којим се ближе уређује вођење регистара из става 1. овог члана дониси Влада, на предлог министарства надлежног за послове одбране.

VI. НАДЛЕЖНОСТИ И ОДГОВОРНОСТИ СУБЈЕКАТА ЗА НАДЗОР НАД СПРОВОЂЕЊЕМ ОВОГ ЗАКОНА

Инспекција за информациону безбедност

Члан 46.

Инспекција за информациону безбедност врши инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима, а у складу са законом којим се уређује инспекцијски надзор.

Послове инспекције за информациону безбедност обавља министарство надлежно за послове информационе безбедности преко инспектора за информациону безбедност.

У оквиру инспекцијског надзора рада оператора ИКТ система, инспектор за информациону безбедност утврђује да ли су испуњени услови прописани овим законом и прописима донетим на основу овог закона.

Члан 47.

Овлашћења инспектора за информациону безбедност

Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом:

1) наложи отклањање утврђених неправилности и за то утврди разуман рок;

2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок;

3) захтева од оператора ИКТ система од посебног значаја да изврши скенирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;

4) наложи да надзирани субјект учини доступним јавности информације које се тичу непоштовања одредби овог закона, а за које постоји оправдан интерес јавности на утврђени начин;

5) наложи да надзирани субјект одреди лице са тачно утврђеним овлашћењима које ће у утврђеном временском периоду надзирати и пратити усаглашеност са одредбама овог закона и наложеним мерама.

VII. КАЗНЕНЕ ОДРЕДБЕ

Члан 48.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај приоритетни оператор ИКТ система од посебног значаја ако:

1) не изврши упис у евиденцију из члана 9. став 1. овог закона;

2) не донесе Акт о процени ризика из члана 11. став 1. овог закона;

3) не донесе Акт о безбедности ИКТ система из члана 12. став 1. овог закона;

4) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 12. став 2. овог закона;

5) не изврши проверу усклађености примењених мера из члана 12. став 4. овог закона;

6) не достави статистичке податке из члана 25. став 1. овог закона;

7) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 47. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице у оператору приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 49.

Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај важни оператор ИКТ система од посебног значаја ако:

1) не изврши упис у евиденцију из члана 9. став 1. овог закона;

2) не донесе Акт о процени ризика из члана 11. став 1. овог закона;

3) не донесе Акт о безбедности ИКТ система из члана 12. став 1. овог закона;

4) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 12. став 2. овог закона

5) не изврши проверу усклађености примењених мера из члана 12. став 4. овог закона;

6) не достави статистичке податке из члана 25. став 1. овог закона;

7) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 47. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице у оператору важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 50.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај приоритетни оператор ИКТ система од посебног значаја ако:

1) о инцидентима у ИКТ систему из члана 13. став 2. овог закона не обавести органе из члана 14. ст. 1. до 3. овог закона;

2) не обавести кориснике којима пружају услуге у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга у складу са чланом 14. став 5. овог закона;

3) не доставља обавештења и извештаје о току и након завршетка инцидента из члана 24 овог закона.

За прекршаје из става 1. овог члана казниће се и одговорно лице у оператору приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Изузетно од ст. 1. и 2. овог члана, ако финансијска институција не обавести Народну банку Србије о инцидентима у ИКТ систему од посебног значаја, Народна банка Србије изриче тој финансијској институцији мере и казне у складу са законом којим се уређује њено пословање.

Члан 51.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај важни оператор ИКТ система од посебног значаја ако:

1) о инцидентима у ИКТ систему из члана 13. став 2. овог закона не обавести органе из члана 14. ст. 1. до 3. овог закона;

2) не обавести кориснике којима пружају услуге у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга у складу са чланом 14. став 5. овог закона;

3) не доставља обавештења и извештаје током и након завршетка инцидентаиз члана 24 овог закона.

За прекршаје из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

VIII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Члан 52.
Рокови за доношење подзаконских аката

Подзаконска акта предвиђена овим законом донеће се у року од шест месеци од дана ступања на снагу овог закона

Члан 53.

До доношења подзаконског акта из члана 6. овог закона оператори ИКТ система од посебног значаја који су одређени Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) настављају да поступају у складу са обавезама утврђеним тим законом.

Оператори ИКТ система од посебног значаја који су били уписани у Евиденцију оператора ИКТ система од посебног значаја која се водила у складу са Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) додатне податке који су предвиђени овим законом достављају у року од 90 дана од дана доношења подзаконског акта из члана 9. овог закона.

Оператори ИКТ система од посебног значаја дужни су да донесу акт из члана 11. овог закона у року од 12 месеци од дана ступања на снагу овог закона.

Оператор ИКТ система од посебног значаја дужан је да донесе акт из члана 12. овог закона у року од 3 месеца од дана ступања на снагу овог подзаконског акта из члана 12. овог закона.

Члан 54.

Канцеларија за информациону безбедност послове из своје надлежности прописане овим законом почиње да обавља почев од 90 дана од дана ступања на снагу овог закона.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 6 месеци од дана ступања на снагу овог закона.

Канцеларија преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Регулаторног тела за електронске комуникације и поштанске услуге насталу у обављању послова Националног ЦЕРТ-а даном истека периода од 6 месеци од дана ступања на снагу овог закона, потребне за вршење стручних послова утврђених овим законом.

Канцеларија преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву насталу у раду Канцеларије за информационе технологије и електронску управу у делокругу послова ЦЕРТ-а органа власти у складу са Законом о информационој безбедности („Службени гласник РС“, бр. 6/16, 94/17 и 77/19), потребне за вршење стручних послова утврђених овим законом.

Члан 55.

Престанак важења Закона о информационој безбедности

Даном ступања на снагу овог закона престаје да важи Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19), изузев одредби које се односе на обавезе оператора ИКТ система од посебног значаја које важе до доношења подзаконског акта из члана 6. овог закона.

Подзаконски акти донети на основу Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) примењиваће се до доношења подзаконских аката у складу са овим законом.

Члан 56.

Ступање на снагу

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.