ПРЕДЛОГ

З А К О Н
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 могућност настанка догађаја или услова који могу угрозити ниво информационе безбедности или исправно функционисање ИКТ система, што се утврђује на основу процене вероватноће догађаја и величине његовог потенцијалног утицаја на ниво информационе безбедности;

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 идентификације, процене и успостављање система 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 идентификовани догађај у ИКТ систему који је могао довести до значајног угрожавања расположивости, аутентичности, интегритета или поверљивости података, услуга или система, али је правовременом интервенцијом или заштитним мерама спречено остваривање штетних последица;

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 са јасном вероватноћом настајања штете у случају да изостане реакција;

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) *злонамерни софтвер* је софтвер намерно креиран са циљем да оштети, поремети, онемогући или неовлашћено приступи информационо-комуникационим системима и обухвата различите типове штетних програма, укључујући вирусе, тројанске коње, црве, рансомвер и шпијунски софтвер;

17) *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;

18) *управљање инцидентом* 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;

19) *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*;*

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

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

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

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

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

25) *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;

26) Центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: ЦЕРТ*)* је функционална целина у оквиру органа или правног лица која обухвата скуп послова који се односе на превенцију и заштиту од инцидената;

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

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

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

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

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

32) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци, као и простор или просторија која је од кључног значаја за очување информационе безбедности ИКТ система;

33) *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;

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

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

36) *мрежа за испоруку садржаја (Content Delivery Network – CDN)* означава мрежу географски распоређених сервера која је осмишљена да обезбеди високу доступност, приступачност и брзу испоруку дигиталног садржаја и услуга корисницима интернета, у име пружалаца садржаја и услуга;

37) *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 аутономних система прође кроз трећи аутономни систем, те која такав саобраћај не мења и не утиче на њега на други начин;

38) *систем назива домена (ДНС)* 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;

39) *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;

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

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

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

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

44) *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;

45) *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;

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

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

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

49) *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;

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

51) *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;

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

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

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

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

56) *TLP (Traffic Light Protocol)* представља стандард за дељење информација у области информационе безбедности, који је успостављен у циљу обезбеђивања ефективне сарадње и дељења информација од извора информације до једног или више прималаца. Протокол пружа једноставну и интуитивну шему од четири ознаке за упућивање на то са ким се потенцијално осетљиве информације могу поделити;

57) *податак о личности* је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета;

58) *администратор* је лице које је овлашћено и одговорно за одржавање, управљање и обезбеђивање функционалности и безбедности ИКТ система од посебног значаја, у складу са одредбама овог закона и другим важећим прописима.

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;

5) начело континуираног побољшања – мере заштите и управљања информационом безбедношћу треба редовно процењивати и унапређивати како би се осигурала њихова ефикасност и прилагодљивост новим претњама и технолошким променама;

6) начело равноправности и недискриминације – мере заштите ИКТ система морају се спроводити на начин који осигурава једнак третман свих корисника, без дискриминације по било ком основу, у складу са законом.

Обрада података о личности

Члан 4.

На обраду података о личности која је неопходна за вршење надлежности и испуњење обавеза из овог закона примењују се одредбе овог закона, одредбе посебних закона којима се уређују одређене области, као и одредбе закона којим се уређује заштита података о личности.

II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ИКТ системи од посебног значаја

Члан 5.

ИКТ системи од посебног значаја су ИКТ системи који су од кључног значаја за одржавање критичних друштвених и економских активности чији би прекид или поремећај у пружању услуга имао или могао да има значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио односно могао да створи значајан системски ризик.

ИКТ системи од посебног значаја су:

1) приоритетни ИКТ системи;
2) важни ИКТ системи.

Оператори приоритетних ИКТ система су:

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

(1) Енергетика и рударство

- производња електричне енергије, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика;
- комбинована производња електричне и топлотне енергије;
- снабдевање електричном енергијом;
- пренос електричне енергије и управљање преносним системом;
- дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом;
- складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика;
- 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 и производња нафте и природног гаса;
- производња деривата нафте;
- складиштење нафте и деривата нафте;
- транспорт и управљање транспортним системом за природни гас;
- складиштење и управљање складиштем природног гаса;
- дистрибуција и управљање дистрибутивним системом за природни гас;
- снабдевање и јавно снабдевање природним гасом;
- производња и прерада угља;
- производња и прерада бакра, злата, олова, цинка, литијума и бора;
- 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;
- сервис за управљање бродским саобраћајем (VTS);

- речни информациони сервиси (RIS);
- управљање путном инфраструктуром;
- управљање интелигентним транспортним системима (ИТС);

(3) Банкарство и финансијска тржишта

- послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно 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 односно салдирања 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 фармацеутских лекова и препарата намењених за здравствену употребу;

  производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја 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

- 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;
- пружање услуга мреже за испоруку садржаја;
- 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

Члан 6.

Оператори важних ИКТ система 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;
- управљање амбалажним отпадом, у смислу закона којим се уређује управљање амбалажним отпадом;
- производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије;
- производња, прерада 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 према критеријумима за одређивање оператора.

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

Министарства у чијим надлежностима су области у којима оператори приоритетних и важних ИКТ система обављају делатности, дужни су да у поступку израде подзаконског акта из става 2. 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) поднесе пријаву за упис 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 једном годишње;

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 трећим лицима;

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

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

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

Обавезе самосталних оператора

Члан 8.

Самостални оператор дужан је да:

1) поднесе пријаву за упис 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 у складу са сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима;

6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима.

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, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ система од посебног значаја.

Самостални оператори, у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе.

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.

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 (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 става 1. тач. 4), 5), 6) и 8) 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 ст. 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) овог члана 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) овог члана обрађују се у складу са законом којим се уређује заштита података о личности и чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 6. овог члана.

Министарство ставља на располагање ажурну Евиденцију Канцеларији за информациону безбедност ради извршења одредби овог закона у погледу прикупљања и размене информација о претњама, рањивостима и инцидентима и пружања подршке, упозоравања и саветовања лица која управљају ИКТ системима.

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 примењују се у свим ИКТ системима оператора из става 1. овог члана.

Мере заштите ИКТ система се односе на:

1) успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством 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, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедношћу, ради обезбеђивања континуиране едукације;

5) обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу;

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

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

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

9) заштиту носача података;

10) ограничење приступа подацима и средствима за обраду података;

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

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

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

14) примена мера заштите ради спречавања отицања података;

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

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

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

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

19) праћење ИКТ система у циљу откривања рањивости и претњи;

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

21) заштиту података и средстава за обраду података од злонамерног софтвера;

22) заштиту од губитка података редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за размену података;

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

24) обезбеђивање интегритета софтвера и оперативних система;

25) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

26) обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања;

27) заштиту података у комуникационим мрежама, укључујући уређаје и водове;

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

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

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

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

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

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

34) 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;

35) мере које обезбеђују континуитет обављања посла у ванредним околностима које се дефинишу Планом континуитета обављања посла;

36) усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите;

37) употребу мултифакторске аутентикације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система

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 орган, односно организација у којој се обављају послови Националног ЦЕРТ-а.

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 ИКТ система од посебног значаја заснива се на Акту о процени ризика из члана 11. овог закона. Примена мера заштите ИКТ система мора бити у складу са процењеним ризицима, како би се обезбедила адекватна заштита система и минимизирао утицај потенцијалних инцидената.

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

Оператор 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 ближе уређује садржај акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери, као и достављање извештаја надлежном органу, доноси Влада на предлог Министарства.

Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност

Члан 13.

Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденти који доводе до неовлашћеног приступа 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 који обављају делатности у области дигиталне инфраструктуре, из члана 5. став 3. 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије за информациону безбедност.

Оператори приоритетних ИКТ система од посебног значаја који обављају делатности у области банкарства и финансијских тржишта из члана 5. став 3. тачка 1) подтачка (3) овог закона дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности.

Оператори приоритетних ИКТ система који обављају делатности електронских комуникација из члана 5. став 3. тачка 1) подтачка (9) алинеја четврта овог закона и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва овог закона, дужни су да обавештење о инциденту доставе Регулаторном телу за електронске комуникације и поштанске услуге.

Народна банка Србије, Регулаторно тело за електронске комуникације и поштанске услуге и Комисија за хартије од вредности 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 ИКТ система из ст. 2. и 3. овог члана, дужни су да путем одговарајућих канала комуникације 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 ИКТ система од посебног значаја из ст. 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре.

Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података.

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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете;

9) 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.

Канцеларија за информациону безбедност утврђује критеријуме за именовање чланова оперативног тима.

Канцеларија за информациону безбедност може да, зависно од природе и последица инцидента, затражи укључивање других органа у рад оперативног тима у оквиру њихових надлежности.

По потреби, састанцима оперативног тима могу присуствовати и представници посебних ЦЕРТ-ова, као и друга лица.

Лица која учествују у раду сталног оперативног тима дужна су да се сертификују за рад са тајним подацима.

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, 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 планове 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 успоставља се сарадња са органима и правним лицима чије су надлежности, односно послови и делатности повезани са планираним активностима.

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 са тим 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 објављује информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио.

Изузетно од става 3. овог члана, Канцеларија за информациону безбедност може објавити информацију о инциденту који се догодио у оператору приоритетног ИКТ система од посебног значаја који обавља делатност у области банкарства и финансијских тржишта из члана 5. став 3. тачка 1) подтачка (3) овог закона, уз претходно прибављену сагласност Народне банке Србије односно Комисије за хартије од вредности.

Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске комуникације и поштанске услуге дужни су да обавештења 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 безбедносне и контраобавештајне послове од значаја за одбрану Републике Србије или органу надлежном за послове националне безбедности, у случају да је инцидент повезан са значајним нарушавањем информационе безбедности које има или може имати за последицу угрожавање одбране Републике Србије или националне безбедности.

Приликом управљања инцидентом Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске 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 је дужна да о томе обавести Министарство.

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, припрема препоруке и мере за решавање инцидента.

Министарство након пријема обавештења из става 1. овог члана сазива седницу Тела за координацију послова информационе безбедности.

Након завршетка инцидента Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, 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 инцидента којем је у складу са класификацијом утврђен ниво опасности „веома висок“ и који представља кризу информационе безбедности, руковођење и координацију спровођења мера и задатака предузима Влада.

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, израђује предлог 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 информационе безбедности;

4) задужење органа за поступање у складу са својим надлежностима;

5) мере за решавање кризе.

Предлог за проглашење кризе информационе безбедности упућује се Министарству, које по пријему предлога без одлагања сазива седницу Тела за координацију послова информационе безбедности.

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

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, координира решавањем кризе информационе безбедности и најмање једном недељно извештава Министарство и Владу о свим активностима.

Предлог за проглашење завршетка кризе информационе 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 Канцеларије;

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

(1) врсту и детаљан опис инцидента;

(2) врсту претње и узрок који је довео до инцидента;

(3) време и трајање инцидента;

(4) озбиљност и утицај инцидента, односно последице које је инцидент изазвао;

(5) информацију о евентуалном прекограничном дејству инцидента;

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

Након завршеног инцидента Канцеларија 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 органу, односно организацији надлежној за послове Националног ЦЕРТ-а статистичке податке о свим инцидентима у ИКТ систему, укључујући и избегнуте инциденте, у претходној години најкасније до 28. фебруара текуће године.

Орган, односно организација из става 1. овог члана извештаје о статистичким подацима доставља Министарству и објављује на својој интернет страници.

Врсту, форму и начин достављања статистичких података из става 1. овог члана утврђује орган, односно организација из става 1. овог члана.

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 документа 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 у вршењу послова за које је надлежна у складу са овим законом;

4) 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;

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, послове правосуђа, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, 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 који мора да буде лице одговарајуће стручности са најмање пет година радног искуства у области информационе безбедности и кога именује Влада, у складу са законом којим се уређује положај државних службеника.

Канцеларија има заменика директора, који мора бити лице одговарајуће стручности са најмање пет година радног искуства у области информационе безбедности, који се поставља у складу са прописима којим се уређује положај државних службеника и има овлашћења у складу са прописима о државној управи.

Надзор над радом Канцеларије

Члан 29.

Надзор над радом Канцеларије у вршењу послова спроводи Министарство, у складу са законом којим се уређује државна управа.

Надлежности Канцеларије

Члан 30.

Канцеларија у оквиру своје надлежности обавља следеће послове и то:

1) врши превенцију и заштиту од безбедносних ризика на националном нивоу у складу са овим законом (послови Националног ЦЕРТ-а);

2) предузима превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе у складу са овим законом (послови ЦЕРТ-а органа власти);

3) обавља сарадњу на националном нивоу у области информационе безбедности;

4) врши послове јединствене тачке контакта;

5) врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима;

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 невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности;

8) обавља сарадњу и размену информација на међународном нивоу у области информационе безбедности у циљу праћења и усаглашавања са међународним прописима и стандардима;

9) врши стручни надзор над радом оператора ИКТ система од посебног значаја;

10) води базу рањивости ИКТ производа и ИКТ услуга;

11) извештава Министарство на кварталном нивоу о предузетим активностима;

12) обавља друге послове у складу са овим законом.

Подзаконски акт којим се ближе уређује начин вршења сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга из става 1. тачка 5) овог члана доноси Влада, на предлог Министарства.

Послови превенције и заштите од безбедносних ризика на националном нивоу (Национални ЦЕРТ)

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 претњама, рањивостима 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) припрема извештаје на кварталном нивоу о предузетим активностима;

13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима

Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за:

1) управљање инцидентима;

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

3) управљање кризним ситуацијама;

4) координирано откривање рањивости.

Канцеларија је овлашћена 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.

Канцеларија обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације.

У оквиру обављања послова Националног ЦЕРТ-а потребно је обезбедити следеће захтеве:

1) висок ниво доступности комуникационих канала избегавањем јединствених тачака прекида и коришћење више средстава за двосмерно контактирање;

2) просторије Националног ЦЕРТ-а и информациони системи за подршку треба да буду смештени на сигурним локацијама;

3) употребу одговарајућег система за управљање захтевима и њихово усмеравање, посебно како би се олакшала ефикасна и ефективна размена информација;

4) обезбеђивање поверљивости и поузданости својих активности;

5) постојање адекватних кадровских капацитета;

6) опремљеност редундантним системима и резервним радним простором како би се осигурао континуитет услуга.

Подзаконски акт којим се ближе уређује поступак проактивног скенирања ИКТ система из става 1. тачка 6) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјекат који непосредно врши скенирање, као и процедура којом се утврђују услови у циљу заштите безбедности система, мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

Превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе (ЦЕРТ органа власти)

Члан 32.

У оквиру предузимања превентивних и реактивних мера у циљу заштите 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) обавештава 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 инцидента;

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

7) доноси акт којим се уређује 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.

Подзаконски акт којим се ближе уређује поступак проактивног скенирања ИКТ система из става 1. тачка 4) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјекат који непосредно врши скенирање, као и процедура којом се утврђују услови у циљу заштите безбедности система, мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

Сарадња на националном нивоу

Члан 33.

Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система.

Канцеларија 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 Канцеларија је дужна 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.

Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система.

Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације.

Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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.

Канцеларија 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 орган, односно организација надлежна за послове Националног ЦЕРТ-а и објављује је јавно.

Упис у евиденцију посебних ЦЕРТ-ова, коју води Канцеларија, 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.

Орган, односно организација из става 2. овог члана прописује садржај, начин уписа и вођења евиденције из става 3. овог члана.

База рањивости

Члан 36.

Орган, односно организација надлежна за послове Националног ЦЕРТ-а 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.

Орган, односно организација из става 1. овог члана прописује садржај, процедуре верификације рањивости, процедуре за управљање техничким рањивостима ИКТ производа и ИКТ услуга, начин уписа и вођења регистра.

База података о регистрацији домена

Члан 37.

Организације које су овлашћене за управљање регистром домена највишег нивоа и пружање услуга ДНС-а обавезне су да прикупљају, чувају и одржавају тачне и потпуне податке о регистрацији домена у посебној бази података, уз дужну пажњу и у складу са прописима о заштити података о личности.

База података из става 1 овог члана мора да садржи најмање следеће податке:

1) назив домена;
2) датум регистрације домена;
3) име, контакт адресу електронске поште и број телефона регистранта;
4) контакт адресу електронске поште и број телефона лица задуженог за администрацију домена, уколико се разликују од података регистранта.

Организације из става 1. овог члана дужне су да усвоје и примене акте и процедуре за верификацију тачности и потпуности података у бази података. Ове процедуре морају бити јавно доступне.

Организације из става 1. овог члана дужне су да обезбеде јавну доступност података који нису лични одмах по регистрацији домена, а у складу са правилима и условима регистрације назива националних интернет домена.

Организације из става 1. овог члана обавезне су да омогуће приступ специфичним подацима о регистрацији домена на основу законитих и образложених захтева овлашћених лица или органа, у складу са овлашћењима додељеним прописима који уређују делокруг њиховог рада.

Одговор на захтев из става 5. овог члана мора бити достављен без одлагања, а најкасније у року од 72 сата од пријема захтева.

Акти и процедуре за откривање података на основу ових захтева морају бити јавно доступни.

У складу са овим чланом, прикупљање података о регистрацији домена не сме довести до дуплирања података. Организације из става 1. овог члана

дужне су да сарађују ради избегавања дуплирања и осигурања усклађености са законом.

Министар надлежан за информациону безбедност прописује ближе услове за прикупљање, чување, верификацију и објављивање података из овог члана, а у складу са најбољом праксом регистара националних интернет домена из Европске Уније, као и Интернет корпорације за додељене називе и бројеве (ICANN).

Заштита деце при коришћењу информационо-комуникационих технологија

Члан 38.

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 Министарству 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.

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 Министарства.

IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Надлежност

Члан 39.

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 40.

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 41.

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 42.

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 технички 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 43.

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 44.

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 вођења регистра издатих одобрења за криптографски производ доноси Влада, на предлог министарства надлежног за послове одбране.

Опште одобрење за коришћење криптографских производа

Члан 45.

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.

Регистри у криптозаштити

Члан 46.

Самостални оператори ИКТ система који имају опште одобрење за коришћење криптографских производа успостављају 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 доноси Влада, на предлог министарства надлежног за послове одбране.

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

Инспекција за информациону безбедност

Члан 47.

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 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.

Овлашћења инспектора за информациону безбедност

Члан 48.

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, конфигурацију и пенетрационо тестирање 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.

Подзаконски акт којим се ближе уређује поступак скенирања, конфигурација и пенетрационо тестирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости из става 1. тачка 3) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјекат који непосредно врши активности из става 1. тачка 3) овог члана, као и процедура којом се утврђују услови у циљу заштите безбедности система, мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

Стручни надзор

Члан 49.

Стручни 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, врши Канцеларија, а у складу са законом којим се уређује инспекцијски надзор.

Послове стручног надзора обавља овлашћено лице запослено у Канцеларији (у даљем тексту: овлашћено лице).

У поступку стручног надзора овлашћено лице има право и обавезу да контролише:

1) адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај;

2) ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите;

3) одговарајуће спровођење процеса провере усклађености примењених мера ИКТ система са актом о безбедности;

4) примену препорука и мера у случају инцидената који значајно угрожавају информациону безбедност.

Ако у вршењу стручног надзора Канцеларија утврди неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, о томе обавештава надзираног субјекта и одређује му рок у коме је дужан да их отклони.

Рок из става 4. овог члана не може бити краћи од осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање.

Ако Канцеларија утврди да надзирани субјекат није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, подноси пријаву инспекцији.

Канцеларија је дужна да по захтеву инспектора за информациону безбедност обави стручни надзор и достави информацију о утврђеном чињеничном стању.

Образац легитимације и начин издавања легитимације овлашћеног лица утврђује Канцеларија.

Легитимација овлашћеног лица обавезно садржи: грб Републике Србије и назив Канцеларије, име и презиме овлашћеног лица, фотографију овлашћеног лица, службени број легитимације, датум издавања легитимације, печат Канцеларије, потпис директора Канцеларије, као и одштампани текст

следеће садржине: „Ималац ове легитимације има овлашћења у складу са одредбама члана 49. ст. 3. и 4. Закона о информационој безбедности.”

VI. КАЗНЕНЕ ОДРЕДБЕ

Члан 50.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система ако:

1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 500.000,00 динара.

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 51.

Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система ако:

1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система новчаном казном у износу од 10.000,00 до 250.000,00 динара.

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 52.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система 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 инцидента из члана 24. овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 500.000,00 динара.

За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Изузетно од ст. 1–3. овог члана, ако финансијска институција не обавести Народну банку Србије о инцидентима у ИКТ систему, Народна банка Србије изриче тој финансијској институцији мере и казне у складу са законом којим се уређује њено пословање.

Члан 53.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система 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 инцидента из члана 24 овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 250.000,00 динара.

За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

VII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рокови за доношење подзаконских аката

Члан 54.

Подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона.

План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности из члана 18. овог закона доноси се у року од 18 месеци од дана ступања на снагу овог закона.

Члан 55.

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 чл. 6а-11б тог закона до 31. децембра 2025. године.

На операторе ИКТ система од посебног значаја који су одређени Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) до датума из става 1. овог члана примењују се казнене одредбе из чл. 30. и 31. тог закона.

Оператори ИКТ система од посебног значаја дужни су да донесу акт из члана 11. став 1. овог закона у року од 18 месеци од дана ступања на снагу овог закона.

Орган, односно организација у којој се обављају послови Националног ЦЕРТ-а дужна је да, у року од девет месеци од дана ступања на снагу овог закона, донесе општу методологију за процену ризика у ИКТ системима од посебног значаја из члана 11. став 4. овог закона.

Оператор ИКТ система од посебног значаја дужан је да донесе акт из члана 12. овог закона у року од 18 месеци од дана ступања на снагу овог закона.

Члан 56.

Канцеларија за информациону безбедност успоставља се и послове из своје надлежности прописане овим законом почиње да обавља 1. јануара 2027. године. Послове Канцеларије за информациону безбедност прописане овим законом, изузев послова Националног ЦЕРТ-а, обављаће Канцеларија за информационе технологије и електронску управу у периоду који почиње даном наступања 12 месеци од дана ступања на снагу овог закона и који траје до 1. јануара 2027. године.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до успостављања Канцеларије за информациону безбедност односно до 1. јануара 2027. године.

Канцеларија за информациону безбедност 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 потребне за вршење стручних послова утврђених овим законом.

Канцеларија за информациону безбедност почев од датума из става 1. овог члана преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Канцеларије за информационе технологије и електронску управу насталу у обављању послова прописаних овим законом из надлежности Канцеларије за информациону безбедност.

Престанак важења Закона о информационој безбедности

Члан 57.

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 чл. 6а-11б и чл. 30. и 31. које важе до 31. децембра 2025. године.

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

Ступање на снагу

Члан 58.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”, изузев члана 29. овог закона који почиње да се примењује 1. јануара 2027. године.

ОБРАЗЛОЖЕЊЕ

I. УСТАВНИ ОСНОВ

Уставни основ за доношење Закона о информационој безбедности садржан је у члану 97. тачка 12. Устава Републике Србије, којим је предвиђено да Република Србија уређује и обезбеђује развој Републике Србије, политику и мере за подстицање равномерног развоја појединих делова Републике Србије, укључујући и развој недовољно развијених подручја; организацију и коришћење простора; научно-технолошки развој.

II. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА

Како би се Република Србија успешно укључила у јединствено европско дигитално тржиште неопходно је обезбедити регулаторне и институционалне услове за убрзан развој дигиталног тржишта у Републици Србији, као и обезбедити да се тај развој одвија у сигурним условима како за сваког појединца, тако и за друштво у целини.

У дигиталном окружењу које се мења, императив је да Влада, пословни субјекти и организације раде заједно на развоју регулаторног оквира који унапређује ИКТ системе и мреже на начин да је омогућено безбедно и неометано чување података и пружање услуга, као и одвијање других процеса. Са константним порастом употребе ИКТ у свакодневном животу, као и са порастом броја услуга које се нуде грађанима електронским путем, неопходно је благовремено одговорити на бројне изазове и пратити динамичан развој сектора уз обавезу сталног усклађивања и праћења прописа Европске уније из ове области.

Област информационе безбедности уређена је Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19, у даљем тексту: ЗИБ) и подзаконским актима донетим на основу тог закона.

ЗИБ се ослања на Директиву ЕУ 2016/1148 Европског парламента и Савета од 6. јула 2016. године која се тиче мера за високи заједнички ниво безбедности мрежа и информационих система (у даљем тексту: НИС1). У процесу испуњавања услова за пуноправно чланство у Европској унији, Република Србија је дужна да своје законодавство усклади са правним тековинама Европске уније у области информационе безбедности. У међувремену, ЕУ је свој регулаторни оквир употпунила и ревидирала усвајањем нове Директиве (ЕУ) 2022/2055 Европског парламента и Савета од дана 14. децембра 2022. године о мерама за висок заједнички ниво сајбер безбедности (у даљем тексту НИС2). У том смислу, први разлог доношења новог закона лежи у потреби да се регулаторни оквир усагласи са оквиром који је на снази у ЕУ како би се благовремено испратили развојни трендови у овој области и омогућило да се употреба ИКТ у Републици Србији одвија у складу са најсавременијим регулаторним тенденцијама.

Директива НИС2 са собом доноси редефинисан приступ информационој безбедности, превасходно у смислу идентификације оператора ИКТ система од посебног значаја и разликовања истих на приоритетне и важне, уз пропратне обавезе и појачани инспекцијски надзор и ревизију, као и строжу казнену политику. Директива јача улогу Националног ЦЕРТ-а у смислу надлежности и реаговања на инцидент или претњу да може доћи до инцидента, омогућава бољу координацију надлежних органа и детаљније уређује питање међународне сарадње и размене информација.

Такође, имајући у виду опсег ових прописа и додатне обавезе на страни државних органа да омогуће безбедну употребу ИКТ, створила се и потреба за ревизијом досадашњег институционалног оквира са циљем да се надлежни органи припреме за неопходан развој капацитета за одговор на ризике и претње приликом употребе ИКТ система и мрежа.

Имајући у виду наведено, најзначајнији циљеви који се доношењем новог закона у области информационе безбедности имају постићи јесу усклађивање са НИС2 Директивом са сврхом да се утврди регулаторни оквир који одговара савременим развојним тенденцијама на тлу Европе и испуни обавеза из Споразума о стабилизацији и придруживању и поступка приступања Републике Европској унији, као и да се унапреди институционални оквир са циљем да се он оспособи да правилно примењује новоуспостављене обавезе и надлежности. Поред тога, овом изменом законског оквира потребно је и унапредити постојећа решења на основу искуства из досадашње примене, као и организационо и структурално унапредити законски текст.

Предлогом закона уређују се следеће области:

1) основне одредбе, којима се уређује предмет закона као и значење појединих појмова који се користе у закону;
2) безбедност ИКТ система од посебног значаја;
3) правни положај и надлежности органа надлежних за превенцију и заштиту од безбедносних ризика у ИКТ системима у Републици Србији;
4) криптобезбедност и заштита од компромитујућег електромагнетног зрачења;
5) надлежности и одговорности субјеката за надзор над спровођењем закона;
6) казнене одредбе;
7) прелазне и завршне одредбе.

Основни разлози због којих се предлаже доношење закона су:

- унапређење законских решења и отклањање недостатака важећег закона који су уочени кроз његову досадашњу примену;
- спровођење активности које су усмерене на даље јачање капацитета и развојних могућности органа надлежних за област информационе безбедности;
- унапређење безбедне употребе ИКТ система и мрежа у Републици Србији;
- промовисање додатног јачања конкуренције на тржишту даљим развојем начина пружања услуга електронским путем;
- унапређење заштите неометаног пружања услуга електронским путем, као и безбедности чувања података;
- стимулисање домаћих и страних инвестиција;
- успостављање правног основа и надлежности за развој оквира и шема сертификације ИКТ производа, процеса и услуга;
- стварање оптималних услова за безбедно коришћење ИКТ од стране појединаца, организација, привредних субјеката и државних органа и организација.

Овом регулаторном изменом постижу се циљеви који се тичу усклађености са важећим регулаторним оквиром ЕУ, остварује се креирање регулаторног оквира који је у стању да омогући унапређени и координисани заједнички одговор на информационо - безбедносне ризике и претње и унапређују се институционални капацитети на начин који ће омогућити њихов

даљи развој и стварање способности да преузму проширене надлежности и задатке.

Имајући у виду да је у поступку придруживања Европској унији Република Србија преузела обавезу да усклади своје законодавство са прописима Европске уније, потребно је извршити усклађивање законодавства доношењем овог закона и тиме испунити преузете обавезе. Како је приступ информационој безбедности новим оквиром фундаментално измењен и уводе се поједине нове тематске области у вези са којима постоји правна празнина, као и да значајније унапређење институционалног оквира може само законом да се успостави, ни једна друга могућност осим законодавна измена није адекватна за остварење ових циљева. Закони, а посебно системски, представљају основ за развој области.

Сви наведени ефекти новог закона треба да омогуће адекватан одговор на ризике и претње у вези са употребом ИКТ у одвијању свакодневних активности, пружању услуга и циркулисању података.

Такође, изражена је потреба да и законска решења буду флексибилна и отворена за нова технолошка достигнућа, да се заснивају на решењима садржаним у међународним документима, прописима и стандардима Европске уније, а посебно на решењима технолошки развијених земаља.

Доношење овог закона није само најбољи, већ је, у постојећем нормативном оквиру и једини начин за решавање проблема и достизање циљева, али и за потпуно транспоновање европског регулаторног оквира.

Најважнија законска решења односе се на:

- Дефинисање приоритетних и важних ИКТ система од посебног значаја;
- Оснивање Канцеларије за информациону безбедност;
- Одређивање активности које ИКТ системи од посебног значаја треба да предузму ради заштите безбедности ИКТ система (мере заштите, процена ризика, акт о безбедности);
- Процедуре у случају инцидента који значајно угрожавају информациону безбедност оператора ИКТ система;
- Активну улогу Националног ЦЕРТ-а и ЦЕРТ-а органа у отклањању инцидената у ИКТ системима;
- Проширена инспекцијска овлашћења.

Сходно одредбама НИС2 директиве, овим законом се дефинишу оператори ИКТ система од посебног значаја који се деле на приоритетне и важне. Приоритетни ИКТ системи од посебног значаја 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. Реч је о ИКТ системима у областима које су виталне за функционисање друштва (енергетика, здравство, банкарство и друге области) и који због свог значаја морају да буду безбедни како би се делатности обављале неометано.

Поред ових система, закон прописује и важне ИКТ системе од посебног значаја, и то из области чије би угрожавање потенцијално могло да има неповољан ефекат на јавни интерес, функционисање других сектора или би створио значајан системски ризик.

Услед неопходности да функционишу несметано и сачувају интегритет података и услуга које пружају, ИКТ системи од посебног значаја треба да буду заштићени применом различитих мера (примена мера заштите у складу са законом, националним и међународним стандардима, одговарајућа процена ризика, доношење акта о безбедности, редовне периодичне провере ИКТ система).

Посебна новина у односу на постојећи законски режим је обавезно обављање процене ризика ИКТ система и доношење Акта о процени ризика

ИКТ система, имајући у виду да организације морају да буду свесне опасности које могу да угрозе информациону безбедност и на основу тога предузму мере заштите одговарајућег нивоа у односу на потенцијални ризик.

Закон предвиђа процедуре у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији. Предложена је класификација инцидената према нивоу опасности, као и поступање надлежних органа зависно од нивоа опасности. Дефинисано је и поступање у случају кризе информационе безбедности, која 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.

У складу са све чешћом праксом других развијених земаља, које оснивају органе посебно задужене за информациону безбедност, тако и наша земља планира да овим законом оснује Канцеларију за информациону безбедност.

Канцеларија за информациону безбедност, која би имала статус посебне организације у смислу закона којим се уређује државна управа и која би почела са својим радом 1. јануара 2027. године, треба да удружи постојеће ресурсе у области информационе безбедности и тиме побољша одговор Републике Србије на изазове у области информационе безбедности. Планирано је да Канцеларија за информациону безбедност врши послове координације и управљања одговором на инциденте у ИКТ системима од посебног значаја који значајно угрожавају информациону безбедност, како би се благовремено и адекватно реаговало на инциденте у овим системима. Канцеларија за информациону безбедност биће дужна да реагује хитно и без одлагања и да активно учествује у отклањању инцидента који могу да наруше безбедност ИКТ система од посебног значаја, као и да угрозе функционисање државе, привреде и грађана. Такође, Канцеларија за информациону безбедност обавља послове Националног ЦЕРТ-а, ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, врши послове јединствене тачке контакта у међународној сарадњи, прописује минималне мере заштите ИКТ система органа, у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиног и приватног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности у органима и друге послове у складу са законом. Законом је предвиђено да до образовања Канцеларије за информациону безбедност, а у периоду који почиње даном наступања 12 месеци од дана ступања на снагу овог закона, ове послове врши Канцеларија за информационе технологију и електронску управу.

Законом се уређују и послови криптобезбедности и заштите од компромитујућег електромагнетног зрачења (КЕМЗ). Министарство одбране, као и у досадашњем законском режиму, 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.

Поред овога, предложене су и одредбе које се односе на надзор над применом овог закона и санкције у случају непоштовања одредби.

III. ОБЈАШЊЕЊЕ ПОЈЕДИНИХ РЕШЕЊА

Члан 1. Предлога закона – 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.

Члан 2. Предлога закона – овим чланом утврђује се значење појединих термина у смислу овог закона.

Члан 3. Предлога закона – овим чланом утврђују се начела информационе безбедности приликом планирања и примене мера заштите ИКТ система.

Члан 4. Предлога закона – прописује се опште правило у вези са обрадом података о личности.

Члан 5. Предлога закона – овим чланом утврђују се приоритетни оператори ИКТ система од посебног значаја, односно они 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 су идентификовани према делатностима у следећим областима: енергетика, саобраћај, банкарство и финансијска тржишта, здравство, вода за пиће, отпадне воде, дигитална инфраструктура, пружање услуга ИКТ операторима ИКТ система од посебног значаја, управљање нуклеарним објектима, пружање квалификованих услуга од поверења, пружање услуга мреже за испоруку садржаја, пружање услуга ДНС, делатност електронских комуникација, тачка за размену интернет саобраћаја, издавање Службеног гласника Републике Србије и вођење Правно-информационог система Републике Србије и она делатност где постоји само један пружалац услуге. Поред ових субјеката, приоритетним операторима ИКТ система сматрају се органи јавне власти, сви субјекти који су препознати као оператори критичне инфраструктуре и оператори који су по постојећем закону препознати као оператори ИКТ система у наведеним делатностима.

Члан 6. Предлога закона – овим чланом уређују се важни оператори ИКТ система од посебног значаја чији би прекид или поремећај у пружању услуга могао да има значајан утицај на јавни интерес, функционисање других сектора или би се створио значајан системски ризик. Они су препознати као оператори у следећим делатностима: поштанске услуге, управљање отпадом, управљање амбалажним отпадом, производња и снабдевање хемикалијама, производња, прерада и дистрибуција хране, рачунара и електронских и оптичких производа, производња електричне опреме, машина и уређаја, моторних возила, приколица и полуприколица, медицинских уређаја, услуге информационог друштва, наоружање и војна опрема, научноистраживачки рад, као и оператори у делатностима из члана 5. који не прођу секторски праг за приоритетне операторе ИКТ система. Предвиђено је и доношење подзаконског акта којим се ближе уређују услови, општи и секторски критеријуми за одређивање оператора приоритетних и важних ИКТ система од посебног значаја које доноси Влада, на предлог министарства надлежног за послове информационе безбедности.

Члан 7. Предлога закона – овим чланом уређују се обавезе оператора ИКТ система у смислу овог закона.

Члан 8. Предлога закона – овим чланом уређују се обавезе самосталних оператора ИКТ система у смислу овог закона.

Члан 9. Предлога закона – овим чланом уређују се питања вођења евиденције оператора ИКТ система од посебног значаја, изузеци од обавезе

уписа у евиденцију, садржина и подаци који се уносе у евиденцији, сврха обраде података о личности.

Члан 10. Предлога закона – овим чланом прописују се мере заштите ИКТ система које је сваки оператор ИКТ система од посебног значаја дужан да предузима.

Члан 11. Предлога закона – овим чланом прописује обавеза доношења Акта о процени ризика ИКТ система од посебног значаја.

Члан 12. Предлога закона – овим чланом прописује се обавеза доношења Акта о безбедности ИКТ система од посебног значаја.

Члан 13. Предлога закона – овим чланом уређује се обавеза обавештавања оператора ИКТ система од посебног значаја о инцидентима који значајно нарушавају информациону безбедност.

Члан 14. Предлога закона – овим чланом уређује се достављање обавештења о инцидентима, док се изузеци односе на Народну банку Србије, Комисију за хартије од вредности, Регулаторно тело за електронске комуникације и поштанске услуге, као и начин поступања по пријави 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.

Члан 15. Предлога закона – овим чланом уређује се садржај обавештења о инциденту, које садржи податке који се односе на подносиоца пријаве, врсту и опис инцидента, датум и време почетка и трајања инцидента, последице које је инцидент изазвао, предузете активности, процену нивоа опасности и утицаја инцидента на ИКТ систем и друге релевантне информације.

Члан 16. Предлога закона – овим чланом врши се идентификација инцидената према њиховом значају и домету, као и нивоу опасности.

Члан 17. Предлога закона – овим чланом успоставља се стални оперативни тим за реаговање на инциденте „високог” и „веома високог” нивоа, који образује Канцеларија за информациону безбедност.

Члан 18. Предлога закона – овим чланом уређује се план за реаговање у случају инцидента „високог” нивоа и кризе информационе безбедности, који доноси Влада на предлог Канцеларије за информациону безбедност.

Члан 19. Предлога закона – овим чланом уређује се поступање по пријему обавештења о инциденту.

Члан 20 - 23. Предлога закона – овим чланом уређује се поступање у случају инцидента према следећем нивоима опасности: „низак”, „средњи”, „висок” и „веома висок”.

Члан 24. Предлога закона – овим чланом уређује се начин извештавања оператора ИКТ система од посебног о инциденту, током инцидента и након инцидента у зависности од нивоа опасности.

Члан 25. Предлога закона – овим чланом уређује се обавеза и начин достављања статистичких података о инцидентима.

Члан 26 - 27. Предлога закона – овим члановима уређује се надлежност Министарства информисања и телекомуникација и успоставља се Тело за координацију послова информационе безбедности.

Члан 28. Предлога закона – овим чланом предвиђа се оснивање Канцеларије за информациону безбедност (у даљем тексту: Канцеларија), као посебне организација у смислу закона којим се уређује положај државне управе.

Члан 29. Предлога закона – овим чланом уређује се надзор над радом Канцеларије.

Члан 30. Предлога закона – овим чланом утврђују се надлежности Канцеларије.

Члан 31. Предлога закона – овим чланом уређују се послови Националног ЦЕРТ-а које Канцеларија обавља у оквиру превенције и заштите од безбедносних ризика и инцидената.

Члан 32. Предлога закона - утврђују се послови ЦЕРТ-а Јединствене информационо - комуникационе мреже електронске управе које Канцеларија обавља у оквиру предузимања превентивних и реактивних мера у циљу заштите ЦЕРТ-а органа власти.

Члан 33. - 34. Предлога закона – овим члановима уређује се сарадња надлежних органа на националном нивоу, као и међународна сарадња и послови јединствене тачке контакта за размену информација о инцидентима.

Члан 35. Предлога закона - овим чланом уређују се питања посебних центара за превенцију безбедносних ризика у ИКТ системима.

Члан 36. Предлога закона – овим уређује се обавеза успостављања и одржавање базе рањивости.

Члан 37. Предлога закона – овај члан се односи на Базу података о регистрацији домена.

Члан 38. Предлога закона – овим чланом уређује се питање заштите деце при коришћењу ИКТ технологија.

Члан 39. - 46. Предлога закона – овим члановима уређује се питање одобравања криптографских производа, дистрибуција криптоматеријала и заштита од компромитујућег електромагнетног зрачења.

Члан 47. – 48. Предлога закона – овим члановима регулише се рад инспекције за информациону безбедност и прописују овлашћења инспектора за информациону безбедност.

Члан 49. Предлога закона уређује стручни надзор.

Члан 50. - 53. Предлога закона – овим члановима прописују се износи новчане казне за прекршај који учине правно лице, одговорно лице у правном лицу, као и предузетник и оне су подељене у више распона зависно од утврђеног прекршаја.

Члан 54. - 58. Предлога закона – овим члановима уређују се прелазне и завршне одредбе и то: рокови за доношење подзаконских аката, примена одређених одредби Закона о информационој безбедности који је на снази, датум успостављања Канцеларије за информациону безбедност, вршење послова Националног ЦЕРТ-а до успостављања Канцеларије, престанак важења Закона о информационој безбедности и ступање на снагу.

IV. ПРОЦЕНА ФИНАНСИЈСКИХ СРЕДСТАВА ПОТРЕБНИХ ЗА СПРОВОЂЕЊЕ ЗАКОНА

За спровођење овог закона у 2025, 2026. и 2027. години нису потребна финансијска средства из буџета Републике Србије са раздела Министарства информисања и телекомуникација.

За спровођење овог закона у 2026. години потребна су додатна средства у Буџету Републике Србије на разделу Канцеларије за информационе технологије у укупном износу од 46.700.000 динара, и то на следећим позицијама:

- извор финансирања 01 – Општи приходи и примања буџета, Функција – 140 – Основно истраживање, Програм 0614 – Информационе технологије и електронска управа, Програмска активност 0002 - Развој ИТ и информационе безбедности, економска класификација 411 – Плате, додаци и накнаде запослених, у износу од 40.000.000 динара;
- извор финансирања 01 – Општи приходи и примања буџета, Функција – 140 – Основно истраживање, Програм 0614 – Информационе технологије и електронска управа, Програмска активност 0002 - Развој

ИТ и информационе безбедности, економска класификација 412 - Социјални доприноси на терет послодавца, у износу од 6.000.000 динара;

- извор финансирања 01 – Општи приходи и примања буџета, Функција – 140 – Основно истраживање, Програм 0614 – Информационе технологије и електронска управа, Програмска активност 0002 - Развој ИТ и информационе безбедности, економска класификација 415 – Накнаде трошкова за запослене, у износу од 700.000 динара.

За спровођење закона у 2025. и 2027. години нису потребна средства на разделу Канцеларије за информационе технологије и електронску управу.

Предвиђа се да ће за рад Канцеларије за информациону безбедност чији је почетак рада планиран 1. јануара 2027. године бити потребно да се у 2027. години у Буџету Републике Србије обезбеди 150.000.000 динара, од чега на:

- економској класификацији 411 – Плате додаци и накнаде запослених износ од 40.000.000 динара;
- економској класификацији 412 – Социјални доприноси на терет послодавца износ од 6.000.000 динара;
- економској класификацији 423 – Услуге по уговору износ од 45.000.000 динара;
- економској класификацији 512 – Машине и опрема износ од 50.000.000 динара;
- економској класификацији 515 - Нематеријална имовина износ од 9.000.000 динара.

АНАЛИЗА ЕФЕКАТА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

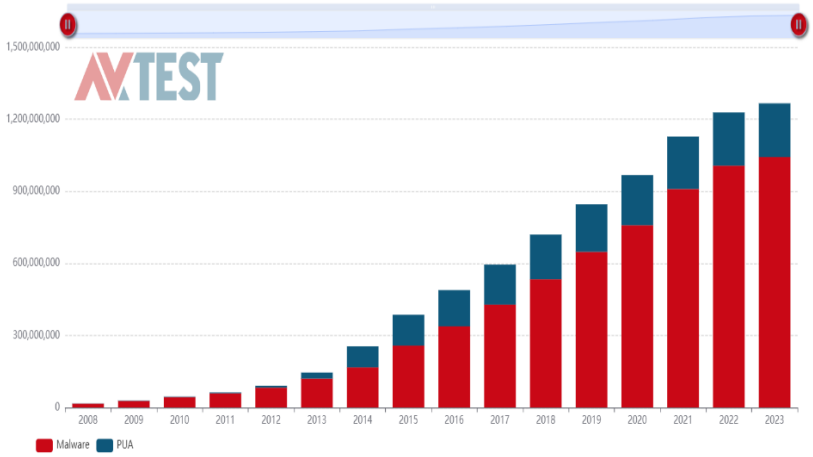
1) Који показатељи се прате у области, који су разлози због којих се ови показатељи прате и које су њихове вредности?

У области информационе безбедности показатељи који се прате односе се на:

- примену мера заштите од безбедносних ризика у информационо-комуникационим системима и
- инциденте који значајно угрожавају информациону безбедност, а којима су изложени ИКТ системи од посебног значаја.

У Стратегији за дигиталну декаду ЕУ наведено је да је процена глобалне штете од инцидената - сајбер напада у 2020. години била око 5.5 трилиона евра. Процењује се да је око 12% компанија у ЕУ било на неки начин погођено сајбер нападом, док је само 2019. године забележено 450 инцидената који су погодили критичну инфраструктуру ЕУ. Евидентан проблем је и недостатак радне снаге са проценом да око 291.000 понуда за посао у области информационе безбедности нису реализоване.

Број малвера и потенцијално нежељених апликација је у сталном порасту. Према подацима независног института AV-TEST GmbH из Магдебурга, сваког дана појави се преко 450.000 нових узорака.



Дијаграм 1 Број малициозних софтвера

Како би се ефикасније борила против изазова којих је свакодневно све више у сајбер простору, Европска унија је, по питању информационе безбедности, одредила пет стратешких приоритета:

- Постизање еластичности – системи се аутоматски опорављају након инцидента;
- Драстично смањење сајбер криминала;
- Развој политике сајбер одбране и капацитета сагласних Заједничкој безбедносној и одбрамбеној политици (CSDP);
- Развој индустријских и технолошких ресурса за информациону безбедност;
- Успостављање повезаних међународних политика информациону безбедности за ЕУ.

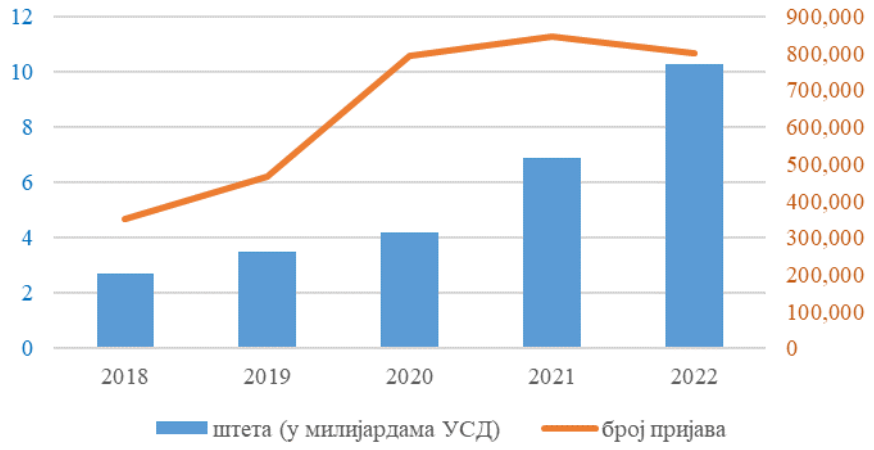
Наведени приоритети у претходним деценијама реализовали су се кроз следеће активности:

- 1992. године донета је Одлука Савета у вези безбедности информационих система
- 2004. године оснива се Европска агенција за мрежну и информациону безбедност (ЕНИСА)

- прва Стратегија безбедности информационог друштва доноси се 2006. године
- 2008. године доноси се Директива Савета за идентификацију и одређивање европске критичне инфраструктуре и процена потребе за побољшањем заштите
- 2009. године усваја се Акциони план за заштиту критичне информационе инфраструктуре
- 2012. године Европска унија формира ЦЕРТ_ЕУ
- 2013. године усваја се Стратегија информационе безбедности ЕУ
- 2016. године доноси се Директива о мерама за висок заједнички ниво безбедности мрежа и информационих система широм Уније (НИС Директива)
- 2019. године доноси се Акт о сајбер безбедности ЕУ којим су дата нова овлашћења агенцији ЕНИСА.

Сајбер криминал је свакако најзаступљенији облик злонамерног деловања у сајбер простору, уз друге облике у које спадају сајбер шпијунажа, сајбер тероризам, хактивизам и сајбер ратовање. У свом последњем извештају[1] Европски центар за сајбер криминал (енг. *European Cybercrime Centre*) наводи да је у околностима пандемије сајбер криминал еволуирао и да је то тренд који ће се наставити. Примери прилагођавања су: злоупотребе небезбедних РДП протокола (енг. *Remote Desktop Protocol*) и рањивих ВПН конекција (енг. *virtual private network*), злоупотребе повећане онлајн куповине и коришћење мобилног банкарства за имплементацију малвера или крађу креденцијала и личних података, али и све већа и напреднија употреба метода социјалног инжењеринга.

Центар за жалбе на интернет криминал америчког Федералног истражног бироа је у 2022. години примио 800.944 пријава са штетом процењеном на преко 10 милијарди долара.[2] Забрињавајући податак је да је број пријава у односу на претходну годину мањи за око 5%, али је укупна штета већа за око 49%, што указује да криминалци усавршавају своје вештине.



Дијаграм 2 Пријаве и штете на годишњем нивоу

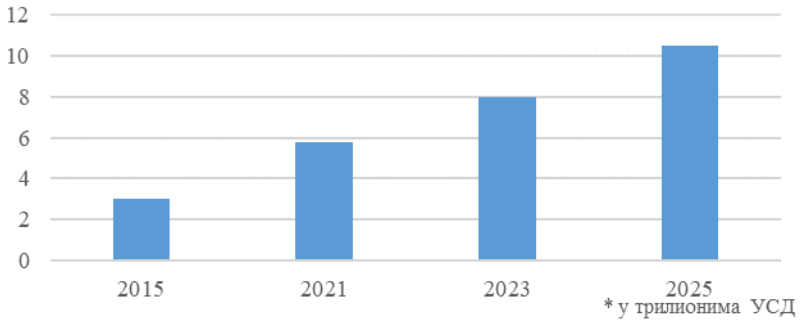
Компанија *Cybersecurity Ventures*, која израђује годишње извештаје о стању сајбер криминала[3], процењује да ће у 2024. години штете од сајбер криминала достићи осам трилиона америчких долара, што превазилази процењене приходе од трговине свих наркотика заједно. Према доступним подацима, штете од сајбер криминала расту по стопи од 15% годишње и процењује се да ће у 2025. години прећи суму од 10 трилиона долара.

---

1 https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

2 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

3 https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

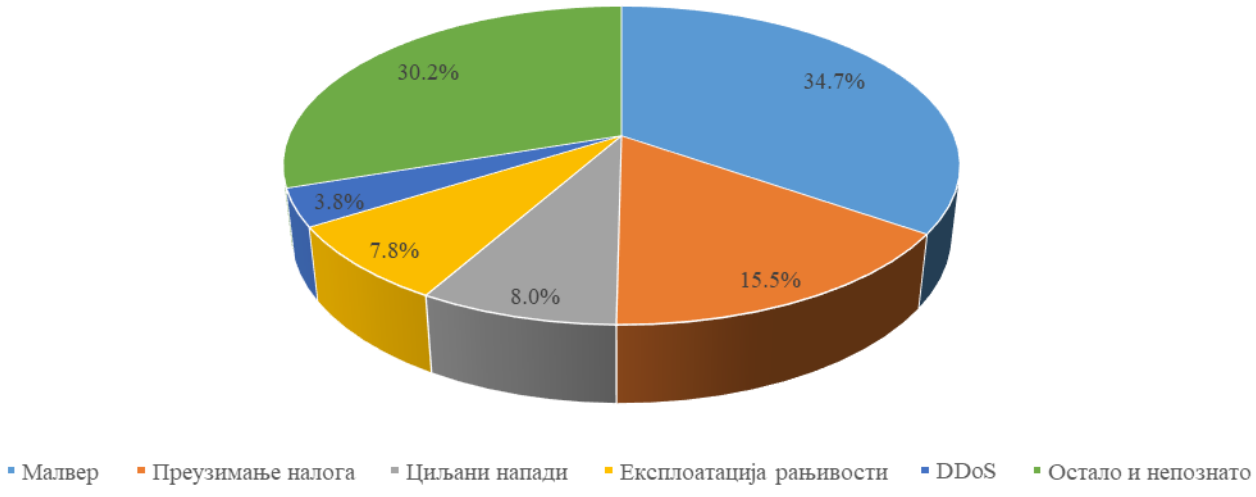


Дијаграм 3 Укупна штета од сајбер криминала

Иста компанија у свом извештају износи податке о недостатку радне снаге, са проценама да је у овом тренутку на светском нивоу непопуњено 3,5 милиона радних места у области информационе безбедности, од чега 700.000 само у САД. Илустративан је податак да је у тренутку писања тог извештаја у САД било 106.000 отворених понуда за посао за стручњаке са CISSP сертификатом (енг. *Certified Information Systems Security Professional*), док је укупан број таквих сертификата издатих у САД нешто преко 90.000. Такође је идентификован и проблем задржавања радне снаге, а посебно најквалитетније и најобученије, са податком да 24% главних службеника за информациону безбедност (CISO) у 500 највећих компанија промени посао након годину дана.

Како би се одговорило на претње у сајбер простору које се из дана у дан повећавају, неопходно је континуирано унапређивати стратешки, институционални и правни оквир у области информационе безбедности која, пре све, треба да обезбеди превентивно деловање на ове претње.

Према подацима са сајта *hackmageddon.com*, на глобалном нивоу 2022. године најзаступљенији тип напада био је коришћење малвера, док су мање заступљени (али са значајним процентом) били преузимање налога, циљани напади, искоришћавање рањивости и дистрибуирано ометање сервиса (DDoS).



Дијаграм 4 Заступљеност различитих типова инцидената у свету

Агенција ЕУ за сајбер безбедност - ЕНИСА (енг. *The European Union Agency for Cybersecurity*) објавила је у марту 2023. године студију ***Утврђивање претњи и изазова информационе безбедности за 2030. годину***, која садржи предвиђања будућих претњи и

могуће противмере. Примарни циљ студије је да идентификује и прикупи информације о будућим претњама које би могле да утичу на инфраструктуру и услуге Европске уније, као и на безбедност грађана и друштва у целини. У израду студије укључени су футуристи, социолози, пословни лидери, стручњаци за информациону безбедност и други, а циљна група су национални органи за информациону безбедност, доносиоци одлука у Европској унији и земљама чланицама, тимови за реаговање, стручњаци у овој области и све друге заинтересоване стране.

Студија је идентификовала 21 претњу, од којих је издвојено десет најзначајнијих:

- компромитација ланца снабдевања,
- напредне кампање дезинформисања,
- повећање дигиталног надзора/губитак приватности,
- људске грешке и експлоатација наслеђених система,
- циљани напади побољшани злоупотребом података са паметних уређаја,
- недостатак анализе и контроле инфраструктуре и објеката у свемиру,
- напредне хибридне претње,
- недостатак обучене радне снаге,
- прекогранични пружаоци ИКТ услуга као јединствена тачка прекида (енг. *single point of failure*),
- злоупотреба вештачке интелигенције.

Пратећи стање у овој области Република Србија је усвојила Закон о информационој безбедности 28. јануара 2016. године, који је делимично пренео Директиву 2016/1148 о мерама за висок заједнички ниво безбедности мрежних и информационих система у Европској унији[4] (енг. *Network and Information Security Directive - NIS Directive*, у даљем тексту: НИС директива), с обзиром да је усвојен пре доношења те директиве.

Закон појам информационе безбедности дефинише као 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. Предметни закон представља оквир за уређење безбедности информационо-комуникационих система у Републици Србији. Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

Сходно томе, оператори ИКТ система од посебног значаја дужни су да донесу акт о безбедности ИКТ система и дефинишу мере заштите, а нарочито принципе, 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.

Поред тога, овим законом се у оквиру Регулаторног тела за електронске комуникације и поштанске услуге (у даљем тексту РАТЕЛ) успоставља Национални центар за превенцију и заштиту од безбедносних ризика у ИКТ системима у Републици Србији (у даљем тексту: Национални ЦЕРТ), који прати стање о инцидентима о националном нивоу, обавештава релевантна лица о ризицима и инцидентима, реагује по пријављеним инцидентима, израђује анализе ризика и инцидената и подиже свест друштва о значају информационе безбедности. Једна од важних функција Националног ЦЕРТ-а је и сарадња са истим институцијама из других земаља. Имајући у виду да инциденти у ИКТ системима најчешће имају прекогранични

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, доступна на адреси: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016L1148

карактер, односно да се дешавају на територији више земаља, међусобна сарадња ЦЕРТ-ова је од изузетног значаја, како би се међусобном разменом информација успешно одговорило на инциденте. Од 1. новембра 2017. године Национални ЦЕРТ је уврштен у списак међународне организације за сарадњу и размену информација из области информационе безбедности *Trusted Introducer*, а налази се и на листи ЦЕРТ тимова Агенције ЕУ за сајбер безбедност - ЕНИСА.

У оквиру Канцеларије за информационе технологије и електронску управу формиран је Сектор за информациону безбедност који, у складу са Законом, спроводи активности ЦЕРТ-а републичких органа.

У циљу спровођења Закона и у Министарству унутрашњих послова формиран је Центар за реаговање на нападе на информациони систем МУП-а (ЦЕРТ МУП) који се од јула 2016. године налази на листи ЦЕРТ тимова Агенције ЕУ за сајбер безбедност - ЕНИСА, а у новембру 2018. године добио је и акредитацију од стране сервиса *Trusted Introducer*.

Иако се са применом Закона започело одмах по усвајању, утврђено је да је неопходно извршити додатне измене и допуне законске регулативе ради усклађивања са НИС директивом која је у међувремену усвојена, али и ради унапређења неких од постојећих решења у циљу ефикаснијег спровођења закона у пракси. Због тога су у октобру 2019. године усвојене измене и допуне Закона о информационој безбедности[5] који је у потпуности усклађен са наведеном Директивом.

Изменама и допунама Закона о информационој безбедности, који је усвојен у октобру 2019. године уређене су новине које се тичу:

- надлежности и потребних капацитета Националног ЦЕРТ-а;
- укључивања Народне банке Србије у рад Тела за координацију послова информационе безбедности;
- успостављања Евиденције оператора ИКТ система од посебног значаја;
- успостављања обавезе достављања статистичких података о инцидентима који се десе у ИКТ системима од посебног значаја на годишњем нивоу;
- сарадње ЦЕРТ-ова у Републици Србији;
- заштите деце при коришћењу информационо-комуникационих технологија;
- класификовања инцидената и поступања надлежних органа у зависности од нивоа опасности инцидента.

Инспекцијским надзором над радом оператора ИКТ система од посебног значаја утврђује се да ли су оператори донели акт о безбедности и применили мере заштите, односно да ли је успостављен адекватан ниво безбедности система. Инспекцијски надзор спроводи се од 2019. године и показује, поред поштовања законских одредби, недостатак капацитета за адекватно реаговање на инциденте.

Оператори ИКТ система од посебног значаја у складу са Законом обавезни су да обавесте Надлежни орган, односно Министарство информисања и телекомуникација (у даљем тексту Министарство) о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

У циљу бољег разумевања постојећег стања у области информационе безбедности, значајно је сагледати инциденте који су пријављени Националном ЦЕРТ-у у претходних неколико година. Ова статистика може бити значајан показатељ да ли су постојеће превентивне мере довољне и у ком правцу је потребно унапређивати правни и институционални оквир. Закон о информационој безбедности, обавезује операторе ИКТ система од посебног значаја да достављају обавештења о инцидентима који значајно нарушавају информациону безбедност

[5] "Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019., доступан на адреси: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg

ИКТ система. На основу добијених обавештења о инцидентима Национални ЦЕРТ израђује годишње статистичке извештаје који су јавно доступни путем веб презентације.

Инциденти су сврстани у 10 група:

- инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл.malware),
- неовлашћено прикупљање података,
- превара,
- покушај упада у ИКТ систем,
- упад у ИКТ систем,
- недоступност или ограничена доступност ИКТ система,
- угрожавање безбедности података,
- оперативни инциденти,
- инциденти физичко-техничке безбедности и
- остали инциденти.

У 2022. години статистички најзаступљенији били су инциденти из групе Неовлашћено прикупљање података са преко седам и по милиона пријављених случајева, док су следећи по бројности инциденти из групе Покушаји упада у ИКТ систем са готово три милиона пријава. Број пријава у осталим групама је знатно мањи па тако у групи Преваре има преко 58 хиљада, у групи Инсталирање злонамерног софтера у оквиру ИКТ система близу 55 хиљада, а у групи Оперативни инциденти преко 13 хиљада пријава. Укупан број пријава у осталих пет група је око шест хиљада.

Дијаграм 5 Број пријављених инцидената у Србији по групама у 2022. години

Посматрано појединачно према врсти инцидента, у 2022. години највише пријава односило се на скенирање портова које је уочено у преко 7 милиона случајева и које не наноси директну штету жртви, али представља индикативне активности нападача у фази извиђања. Пракса нападача је да овакве нападе покрећу према великом броју ИП адреса у покушају да нађу потенцијалне жртве које имају незаштићене портове, па се на тај начин и ИП адресе оператора критичне инфраструктуре нађу у том опсегу.

На другом месту по бројности налази се покушај откривања креденцијала који подразумева покушај приступа систему жртве узастопним испробавањем великог броја различитих комбинација слова, бројева и симбола са циљем идентификације корисничког имена и лозинке. Ова врста напада ослања се на недостатак свести корисника приликом креирања лозинки за приступ систему и веома је популарна међу нападачима јер злоупотребом легитимног налога може бити омогућен приступ читавом ИКТ систему.

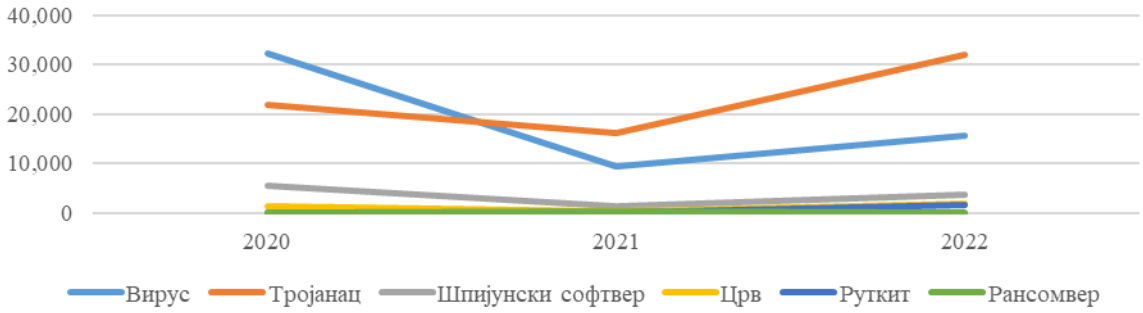
Покушај искоришћавања рањивости система је на трећем месту, а ова врста напада могућа је уколико у систему постоје рањивости.

На четвртом месту по бројности налазе се фишинг напади, који су током 2022. године често били усмерени на кориснике поштанских услуга и платформи за е-трговину преко неколико великих фишинг кампања.

На петом месту су тројанци, који по покретању могу да преузму друге претње са Интернета, убацују друге типове малвера на угрожене рачунаре, комуницирају са удаљеним нападачима, бележе све што се куца на тастатури и шаљу нападачима, као и да на друге начине буду део комплекснијих сајбер напада.

Дијаграм 6 Најчешће пријављени инциденти у Србији у 2022. години

Прегледом броја инцидената по врстама за једну годину може се стећи слика о тренутном стању, али за дубљу анализу потребно је посматрати трендове у неком временском периоду. Трендови за сваку групу инцидената представљени су на наредним дијаграмима.

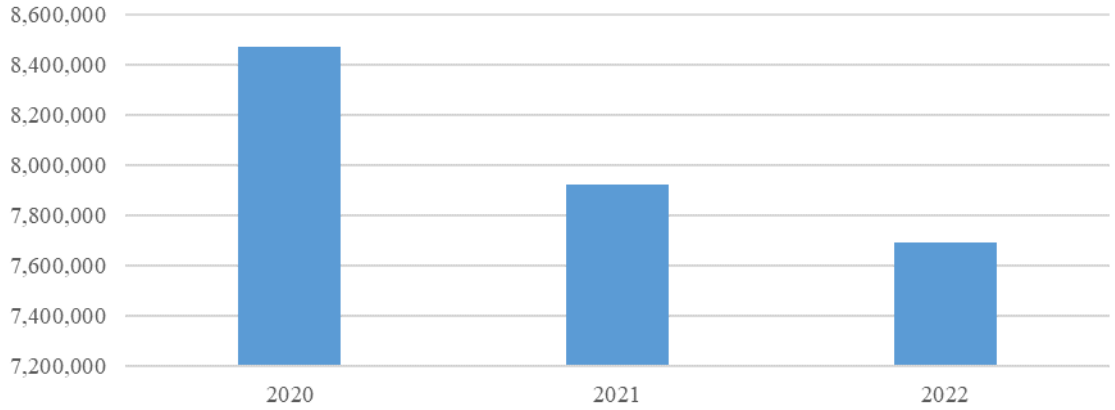


Дијаграм 7 Инциденти у групи Инсталирање злонамерног софтвера у оквиру ИКТ система

У групи Инсталирање злонамерног софтвера у оквиру ИКТ система прате се подаци за шест врста злонамерног софтвера (малвера): вирусе, тројанце, црве, руткит, рансомвер и шпијунски софтвер. Након драстичног пада броја пријава случајева инцидената код којих је коришћен злонамерни софтвер у 2021. години у односу на претходну годину, 2022. године је дошло до значајног пораста броја инцидента који спадају у ову групу, а укупан број инцидената у овој групи готово се изједначио са бројем забележеним 2020. године.

Тројанци су најчешћи тип малвера који је коришћен у последње две године са уделом од преко 50% од свих злонамерних софтвера. Карактеристика тројанаца је да покушавају да наведу кориснике да их покрену тако што се претварају да су корисни програми, па за њихову успешну дистрибуцију нападачи укључују и методе социјалног инжењеринга.

Дијаграм 8 Инциденти у групи Неовлашћено прикупљање података (осим скенирања портова)



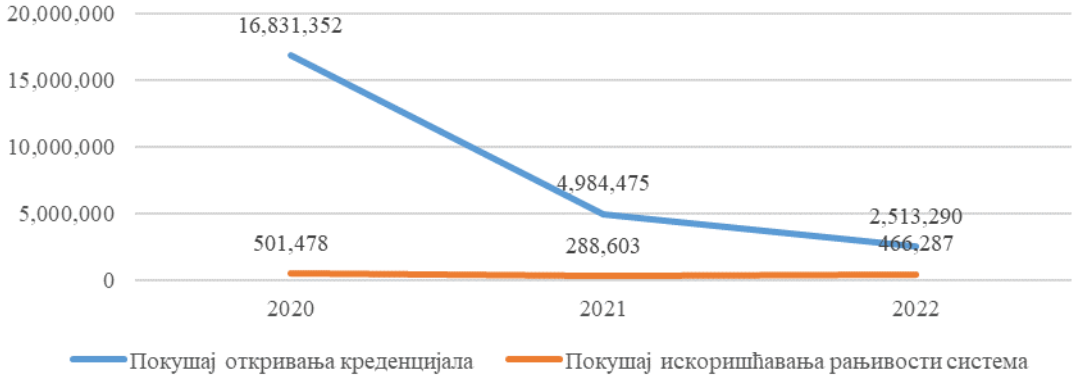
Дијаграм 9 Инциденти типа Скенирање портова из групе Неовлашћено прикупљање података

Неовлашћено прикупљање података обухвата социјални инжењеринг, компромитовање или цурење података, пресретање података између рачунара и сервера и скенирање портова. На дијаграмима се може приметити индикативни тренд повећања броја напада из ове групе, осим скенирања портова. Социјални инжењеринг је у 2020. и 2021. години био на релативно блиском нивоу, да би у 2022. години било регистровано преко четири пута више оваквих инцидената. Компромитовање или цурење података је имало велики скок у броју пријава 2021. у односу на 2020. годину и тај број се задржао и у 2022. години, док је број регистрованих случајева пресретања података између рачунара и сервера имао енорман раст са мање од 10 забележених случајева у 2020. и 2021. години, на преко 600 случајева у 2022. години.

Пријављени случајеви скенирања портова приказани су на посебном дијаграму због несразмерне разлике у броју у односу на друге врсте инцидената из ове групе, али ово је и једини пример у овој групи да постоји константан опадајући тренд. Овако велики број забележених случајева последица је аутоматизованих процеса за испитивање доступних сервиса на удаљеним рачунарима, што не мора нужно бити вођено малициозним намерама али се врши без експлицитне сагласности оператора ИКТ система.

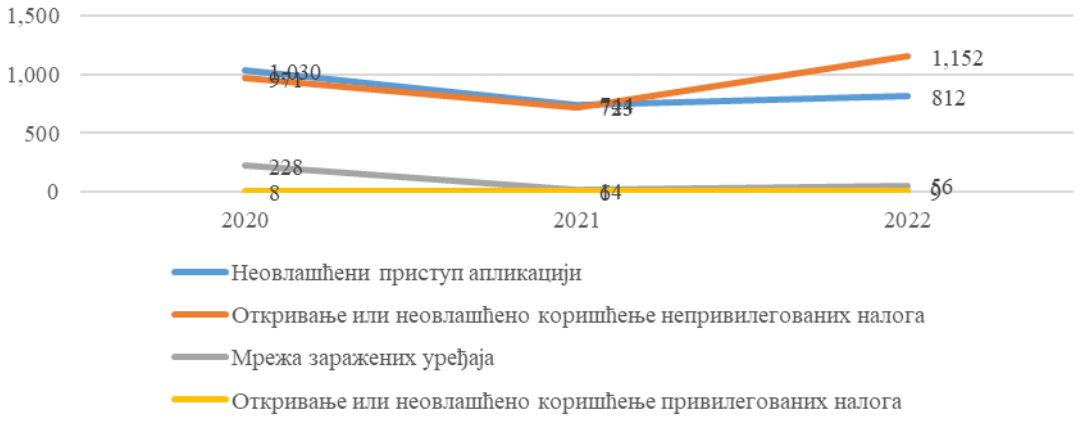
Дијаграм 10 Инциденти у групи Превара

У групи Превара налазе се фишинг и неовлашћено коришћење ресурса и други облици превара. Слично као код других типова инцидената који обухватају методе социјалног инжењеринга, и код фишинга је у 2021. години дошло до пада броја забележених случајева, да би у 2022. години број пријава драстично порастао. Сличан тренд може се видети и за друге случајеве неовлашћеног коришћења ресурса (као што је криптоџекинг) али у мањем броју и са процентуално мањим осцилацијама.



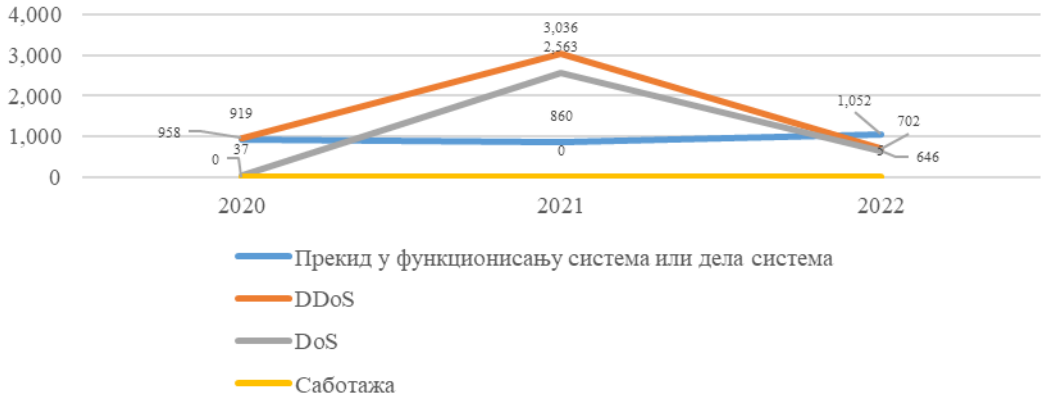
Дијаграм 11 Инциденти у групи Покушај упада у ИКТ систем

Да би упали у неки ИКТ систем нападачи покушавају да открију валидне креденцијале или да искористе рањивости система. За откривање креденцијала најчешће се примењују технике бруталне силе или речника које подразумевају да нападачи покушавају да се пријаве на систем са креденцијалима које уносе редом према одређеном шаблону све док не унесу исправан, што подразумева огроман број покушаја и зато су ови бројеви овако велики (мада се уочава тренд опадања броја покушаја). Други тип инцидента у овој групи, искоришћавање рањивости система, такође показује већ виђен трен да после смањења броја пријава у 2021. години долази до поновног повећања у 2022. години и враћања приближно на ниво из 2020. године.



Дијаграм 12 Инциденти у групи Упад у ИКТ систем

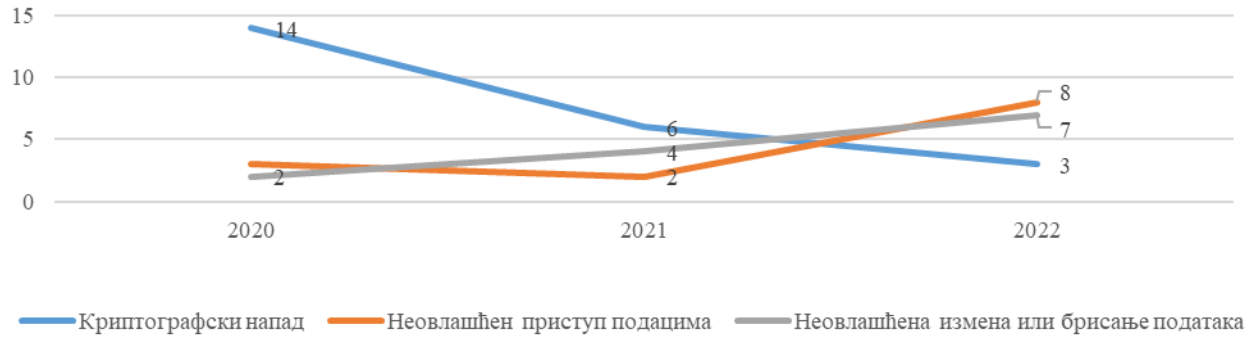
Неовлашћени приступ апликацији, откривање или неовлашћено коришћење непривилегованих налога, откривање или неовлашћено коришћење привилегованих налога и мрежа заражених уређаја су врсте инцидената које припадају групи Упад у ИКТ систем. У овој групи у 2022. години пријављено је највише откривања или неовлашћеног коришћења непривилегованих налога, са трендом да је забележен пад броја пријављених случајева 2021. године у односу на претходну годину и раст 2022. године.



Дијаграм 13 Инциденти у групи Недоступност или ограничена доступност ИКТ система

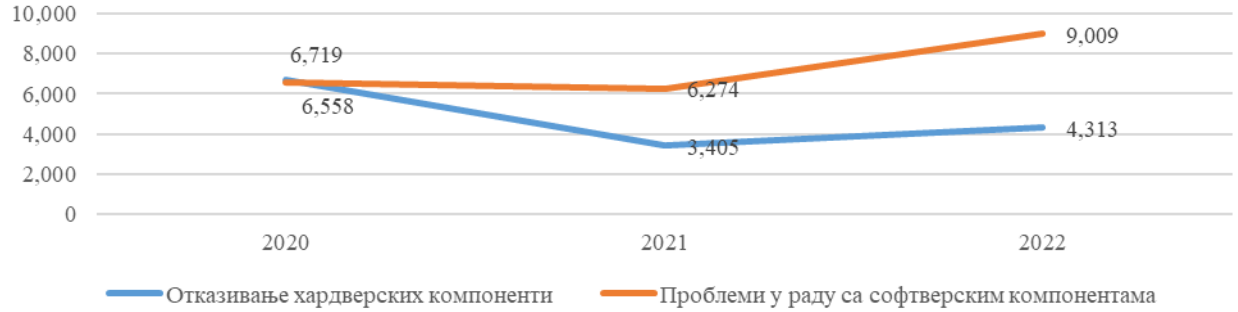
Неовлашћено откривање или коришћење привилегованих налога, које представља много озбиљнији инцидент јер у случају успешности нападачи имају могућност приступа осетљивим подацима, забележено је у приближно истом броју све три године.

Група Недоступност или ограничена доступност ИКТ система укључује четири типа инцидента: прекид у функционисању система или дела система (енг. *outage*), дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система (енг. *distributed denial-of-service - DDoS*), напад са циљем онемогућавања или ометања функционисања ИКТ система (енг. *Denial-of-Service - DoS*) и саботажу. За DoS и DDoS нападе приметан је обрнут тренд у односу на претежан тренд код других врста напада, у смислу да је у 2021. години уочен нагли скок броја пријављених напада, а у 2022. години нагли пад у односу на претходну годину. Такође се може уочити да у 2020. и 2021. години није забележен нити један случај саботаже, док је у 2022. години пријављено пет таквих случајева.



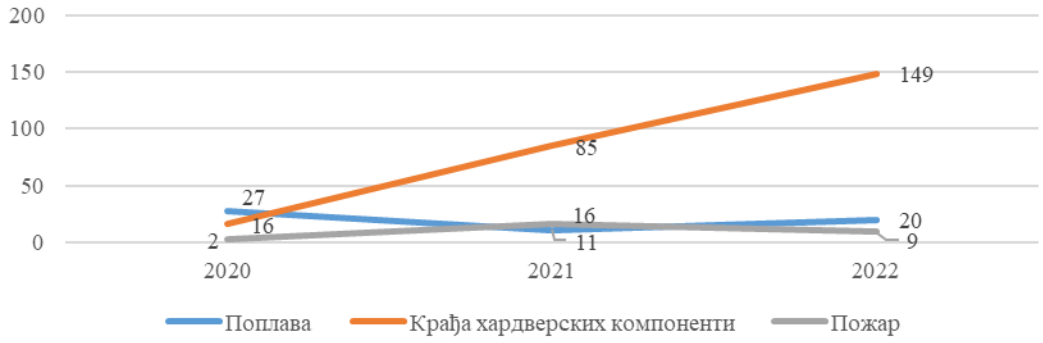
Дијаграм 14 Инциденти у групи Угрожавање безбедности података

Угрожавање безбедности података обухвата криптографски напад, неовлашћен приступ подацима и неовлашћене измене или брисање података. Укупан број ових напада није велики, а може се приметити благи тренд раста броја случајева неовлашћеног приступа подацима и неовлашћене измене или брисања података и тренд пада броја криптографских напада.



Дијаграм 15 Инциденти у групи Оперативни инциденти

Оперативни инциденти су они који доводе до застоја у пружању услуга, односно прекида који на било који начин угрожавају пословни процес изазваних отказивањем хардверских компоненти или проблема у раду са софтверским компонентама. У 2020. години број забележених проблема са хардверским и са софтверским компонентама био је приближно исти, док је у последње две године пријављен приближно двоструко већи број проблема са софтерским компонентама него са хардвером.



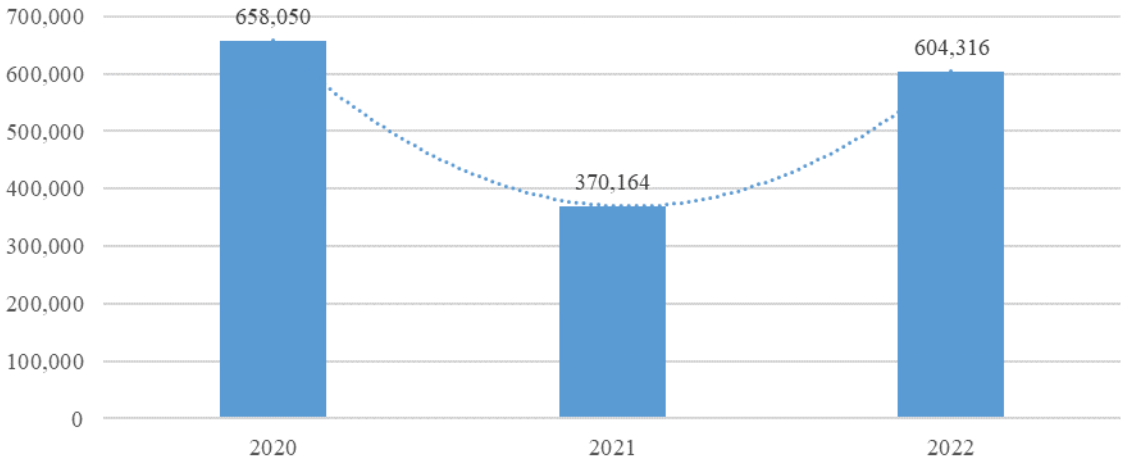
Дијаграм 16 Инциденти у групи Инциденти физичко-техничке безбедности

У групу Инцидената физичко-техничке безбедности спадају поплаве, пожари и крађе. Може се констатовати да је збир пожара и поплава у збиру прилично константан (по 29 у 2020.

и 2022. години и 27 у 2021. години), али је број пријављених крађа практично једини тип инцидента који бележи линеарни тренд раста у протекле три године.

У остале инциденте сврстани су сви они који не спадају у наведене категорије, као што су детекција потенцијално небезбедних апликација, неодобрене платне трансакције или лажни профили на друштвеним мрежама.

Укупан број пријављених инцидената у 2020. години био је 25.958.850, у 2021. години 13.279.007, а у 2022. години 10.808.838. Гледајући само ове бројеве могао би се стећи утисак да постоји генералан тренд смањења броја инцидената. Међутим, треба имати у виду да је у 2020. години број инцидената на глобалном нивоу еруптирао као последица пандемије и измењених околности пословања па ни Србија није била изузета од тог тренда (на жалост, статистика која би показала овај скок није вођена у Србији пре 2020. године). Следећа година донела је значајно смиривање, па поређење 2021. и 2022. године може боље показати прави тренд. Посматрајући тренд пријављених скенирања портова (8.469.448 у 2020. години, 7.924.368 у 2021. години и 7.691.232 у 2022. години) и број покушаја откривања креденцијала (16.831.352 у 2020. години, 4.984.475 у 2021. години и 2.513.290 у 2022. години) очигледно је да ове две врсте инцидената, које у свакој од ове три године заједно чине између 94,4% и 97,4% од укупног броја инцидената, бележе значајно смањење након прве године пандемије и требају бити третиране засебно због своје процентуалне заступљености. Ако се из укупног броја инцидената изузму ове две врсте, добија се следећи дијаграм броја инцидената по годинама:



Дијаграм 17 Укупан број инцидената по годинама без скенирања портова и покушаја откривања креденцијала

Ако се узме у обзир да је 2020. година била специфична и узме у обзир однос броја инцидената у 2021. и 2022. години, уочава се значајан и забрињавајући раст. На глобалном нивоу, прогнозе су да ће број инцидената значајно расти у наредном периоду (није нам позната нити једна анализа која закључује да ће број инцидената опадати), али такође и њихова софистицираност. Посебно су алармантна предвиђања да ће се наставити тренд раста просечне штете по инциденту, што значи да ће укупна сума штете нанете инцидентима расти у доста већем проценту од раста броја инцидената. Овакви трендови неће мимоићи ни Србију па се може очекивати да се и у наредним годинама настави раст броја пријављених инцидената, али и раст нанете штете.

2) Да ли се у предметној области спроводи или се спроводио документ јавне политике или пропис? Представити резултате спровођења тог документа јавне политике или прописа и образложити због чега добијени резултати нису у складу са планираним вредностима.

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године представља међусекторску стратегију којом се утврђују циљеви и мере за развој информационог друштва и информационе безбедности. У делу који се односи на информациону безбедност Стратегија је усклађена са Директивом о мрежној и информационој безбедности ЕУ (енг. *Network and Information Security Directive - NIS Directive*), која предвиђа обавезу доношења националне стратегије за информациону безбедност којом ће се дефинисати стратешки циљеви и приоритети који се односе на мрежну и информациону безбедност.

Стратегијом је дефинисан посебан циљ ***Унапређење информационе безбедности грађана, јавне управе и привреде***, који се остварује кроз реализацију следећих мера:

- подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде,
- подизање капацитета ИКТ система од посебног значаја за примену мера заштите,
- подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ,
- подизање капацитета инспекције за информациону безбедност,
- подстицање јавно-приватног партнерства у области информационе безбедности и
- унапређење регионалне и међународне сарадње.

Акциони план за реализацију Стратегије развоја информационог друштва и информационе безбедности за период од 2024. до 2026. године мери оствареност овог посебног циља кроз Глобални индекс информационе безбедности (енг. *Global Cyber Security Indeks*) који мери осам индикатора: позицију државе у глобалним оквирима у овој области, индекс безбедности у сајбер простору, законе, техничку развијеност, организацију, капацитете, сарадњу и позицију државе у регионалним оквирима у овој области. У последњем издању „Глобалног индекс аинформационе безбедности“, Република Србија нашла се у првој од пет група држава која обухвата земље са највишим нивоом развоја у области информационе безбедности. Међународна телекомуникациона унија вредновала је пет кључних компоненти развоја, и то правни оквир, техничке мере, организационе мере, јачање капацитета и међународну сарадњу. Република Србија препозната је као једна од водећих земаља у свим овим аспектима чиме је потврђен значајан допринос наше земље у осигуравању високог нивоа информационе безбедности.

У оквиру мере *Подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде* реализоване су следеће активности:

- У сарадњи са надлежним Министарством креиране су и спроведене две врсте обука намењене представницима министарстава. Теоријску обуку под називом „Примена Модела акта о безбедности” похађало је укупно 27 запослених лица из 9 министарстава, а дводневну техничку обуку „Детекција и одбрана ИКТ система од сајбер напада” похађало је укупно 28 запослених из 8 министарстава. Такође, у сарадњи са Институтом за стандардизацију и Министарством унутрашњих послова одржан је вебинар под називом „Од ЗИБ-а до стандарда” намењен представницима судства и правосудних органа, који је похађало укупно 78 учесника.
- У сарадњи са Радио телевизијом Србије организована је медијска кампања намењена подизању свести о значају информационе безбедности у оквиру које су емитовани едукативни спотови на тему безбедности деце на интернету. Такође је у 10 епизода реализована и емисија „Породична мрежа” у циљу подизања свести о значају информационе безбедности, о ризицима и мерама заштите, у којој су активно учешће имали родитељи са децом.
- У току 2022. године спроведен је Јавни позив за доделу средстава за организовање регионалних конференција на тему размене искуства у области подизања нивоа

дигиталне писмености, дигиталних компентенција и реализацију програма који за циљ имају подизање дигиталних компетенција жена из руралних области.

- Израђен је Водич за сајбер безбедност малих и средњих предузећа у сарадњи са Националним ЦЕРТ-ом Републике Србије. Водич је намењен малим и средњим предузећима и садржи упутства о томе како се заштитити од најчешћих претњи по информациону безбедност с којима мала и средња предузећа могу да се сусретну у свом раду, а заснован је на доказаним примерима добре праксе приватног и јавног сектора.
- Национални ЦЕРТ Републике Србије креирао је платформу за подизање свести и знања из области информационе безбедности, која је доступна на адреси: https://learn.cert.rs/Home/Home?mostrarTour=True.

У оквиру мере *Унапређење сарадње и подизање капацитета ИКТ система од посебног значаја за примену мера заштите*:

- одржане су обуке и вежбе за представнике правосудних органа и оператора ИКТ система од посебног значаја у области енергетике;
- припремљене су смернице за достизање неопходног нивоа испуњености захтева (енг. *common criteria*) за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;
- у октобру 2022. године од стране Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ), као Националног ЦЕРТ-а, организована је Национална конференција „Будимо сајбер свесни”, којом је обележен октобар као међународни месец информационе безбедности на којој су презентована актуелна дешавања у сајбер простору, начини унапређења сарадње и размене информација о сајбер претњама, представљени су начини заштите критичне инфраструктуре, као и значај јавно-приватног партнерства у овој области;
- током новембра 2022. године одржана је конфренција у организацији Регистра националног Интернет домена Србије на којој су настављени разговори поводом подизања свести и едукације о информационој безбедности и презентовани су резултати пројеката Сајбер херој и дигиталне кампање Заштити се;
- у оквиру базе Националног ЦЕРТ-а креиран је део за размену података између Националног ЦЕРТ-а и ИКТ система од посебног значаја и успостављена је платформа за размену података *MISP - Malware Information Sharing Platform*);
- у току је припрема образаца за самопроцену ИКТ система од посебног значаја као и за проверу степена развијености информационе безбедности у Републици Србији.

У оквиру мере *Подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ система*:

- израђене су смернице за поступање у случају инцидената који су високог и веома високог нивоа опасности;
- успостављена је сарадња између Министарства, Националног ЦЕРТ-а и Сектора за ванредне ситуације у оквиру Министарства унутрашњих послова ради препознавања механизама сарадње у случају инцидента веома високог нивоа опасности;
- успостављен је ЦЕРТ Министарства одбране и уписан у Евиденцију ИКТ система од посебног значаја;
- континуирано се врши похађање обука запослених у Националном ЦЕРТ-у у складу са планом стручног усавршавања РАТЕЛ-а

Подизање капацитета инспекције за информациону безбедност врши се кроз бројне обуке међу којима су најзначајније:

- Обука коју је организовало Акредитационо тело Србије уз учешће ЕУ експерата везано за eIDAS регулативу (енг. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*);
- Обуке за коришћење софтвера еИнспектор;
- Учествовање на Техничком колоквијуму за ЦЕРТ-ове Западног Балкана коју је организовао Женевски центар за управљање безбедносним сектором (енг. *Geneva Centre for Security Sector Governance - DCAF*) у сарадњи са Албанском националном агенцијом за електронску сертификацију и информациону безбедност (AKCESK) у оквиру регионалног пројекта;
- Обука Института за стандардизацију за чланове комисија за стандарде и сродне документе;
- NFC радионица коју је организовала Агенција Европске Уније за сајбер безбедност – ЕНИСА.

Мера *Подстицање јавно-приватног партнерства у области информационе безбедности* реализује се кроз следеће активности:

- У оквиру фондације „Мрежа за сајбер безбедност" (некадашња Петничка група), која повезује привреду и доносиоце одлука о политикама кроз платформу за дискусију и спровођење активности усмерених ка унапређењу информационе безбедности у Србији, реализује се програм „Сајбер херој" у оквиру кога се реализује такмичење у области информационе безбедности *Serbian Cybersecurity Challenge*. 2022. године национални тим Србије учествовао је на међународном такмичењу *European Cyber Security Challenge* (ЕЦСЦ 2022). Поред тога, на позив Агенције Европске Уније за сајбер безбедност – ЕНИСА, два представника из Србије били су кандидати за Тим Европе на такмичењу континената.
- Закључени су споразуми о сарадњи са Савезом слепих Београд и Савезом глувих Београд - постигнут је договор о одржавању презентација на тему безбедности деце на интернету.

Унапређење регионалне и међународне сарадње спроводи се кроз бројне активности прдвиђене акционим планом међу којима се издвајају:

- У оквиру иницијативе „Отворени Балкан" закључен је Споразум о повезивању шема електронске идентификације грађана Западног Балкана између Србије, Албаније и Северне Македоније, чиме су државе међусобно признале шеме електронске идентификације уписане у одговарајуће регистре. Закључивање овог споразума подразумева да стране технички повежу своје портале електронске управе тако да грађани могу да се електронски идентификују у складу са најнапреднијим стандардима информационе безбедности.
- У септембру 2022. године потписан је Меморандум о разумевању у области информационе безбедности између Министарства информисања и телекомуникација Републике Србије и Савета за сајбер безбедност Уједињених Арапских Емирата. Сарадња предвиђена овим меморандумом се спроводи кроз разне унапред договорене форме, укључујући обуку, техничке консултације и размену стручњака у неопходним областима. Области сарадње предвиђене меморандумом су: размена информација о ризицима по информациону безбедност, заједничко информисање и одговор на инциденте на пољу информационе безбедности, подела информација о ширењу злонамерних софтвера, размена података о индикаторима компромитације, пружање информација о могућим успешним решењима у области информационе безбедности, заједничка сарадња у организовању техничких радионица, конференција, едукативних

посета и обука, заједничка координација и сарадња у организацији и спровођењу обука у области информационе безбедности.

- У новембру 2022. године у Београду реализована је *TAIEX* експертска мисија које се односи на сертификацију у области информационе безбедности, као и на остала питања у вези са применом Акта о сајбер безбедности ЕУ (Уредба 2019/881). TAIEX је инструмент Европске комисије за техничку помоћ и размену информација и подржава јавну администрацију у вези са усклађивањем, применом и спровођењем законодавства ЕУ, као и олакшавањем размене најбољих пракси ЕУ. Експертској мисији присуствовали су представници Канцеларије за информационе технологије и електронску управу, Министарства одбране, Министарства информисања и телекомуникација, Безбедносно – информативне агенције, као и представници РАТЕЛ-а - Националног ЦЕРТ-а. Експертска мисија затражена је у циљу припреме за ревидирање прописа из области информационе безбедности у складу са најновијим законодавством ЕУ.
- У октобру 2022. године одржан је семинар о *Предлог*у НИС 2 директиве Европске уније, упоредној пракси у вези уређења и рада агенција за информациону безбедност, променама у стандарду ИСО 27001 и најбољим решењима у погледу управљања кризним ситуацијама у случају сајбер инцидената. У вези са наведеним темама учесници семинара представили су правни и стратешки оквир и праксу из свог делокруга рада.
- У октобру 2022. године Министарство је учествовало на међународној конференцији *INSAFE AND INHOPE*, одржаној у Бриселу.
- Надлежни органи РС сарађују са ЕУ институцијама надлежним за област информационе безбедности. Министарство остварује сарадњу са Међународном унијом за телекомуникације у погледу израде Глобалног индекса сајбер безбедности, као и са Агенцијом Европске Уније за сајбер безбедност ЕНИСА учешћем у радној групи за електронску идентификацију и квалификоване услуге од поверења. ЦЕРТ-ови из Републике из Србије налазе се на *Trusted Introducer* листи, а Национални ЦЕРТ и ЦЕРТ МУП чланови су *Forum of Incident Response and Security Teams* организације.

И поред успешног спровођења активности предвиђених Стратегијом развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године, због недовољних кадровских и техничких капацитета надлежних органа у области информационе безбедности, касни се у реализацији појединих активности, као што су: израда смерница за достизање неопходног нивоа испуњености захтева (енг. *common criteria*) за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система; развој, хармонизација и проширење специјализованих курсева и програма информационе безбедности на универзитетима и другим високошколским установама; обуке за мала и средња предузећа о потреби и начину примене мера заштите и важности континуираног подизања капацитета запослених, у складу са националним и међународним стандардима. Због измена европских директива у овој области неопходно је извршити хармонизацију прописа и ускладити одредбе Закона о информационој безбедности са НИС 2 Директивом (енг. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive)* Усклађивање прописа омогућиће наставак сарадње са међународним телима и испуњење обавеза Републике Србије у процесу придруживања Европској унији. Унапређење правног оквира требало би да побољша не само међународну сарадњу, већ и капацитете свих ентитета надлежних за обезбеђивање информационе безбедности.

3) Да ли су уочени проблеми у области и на кога се они односе? Представити узроке и последице проблема.

Анализирајући постојећи законски оквир и његову имплементацију, циљеве постављене Стратегијом развоја информационог друштва и информационе безбедности за период 2021.-2026. године и правце развоја на глобалном и нивоу Европске уније, могу се идентификовати следећи проблеми који се могу превазићи искључиво изменом институционалног и правног оквира:

- неусклађеност Закона о информационој безбедности са европским прописима,
- недостатак капацитета надлежних органа,
- потреба за подизањем оперативних капацитета за реаговање на инциденте, посебно на оне од националног значаја,
- недостатак системског прикупљања и размене информација,
- непостојање националне платформе за брзу детекцију инцидената,
- недостатак координације за откривање рањивости и
- недовољна координација међународних активности.

Неусклађеност Закона о информационој безбедности са европским прописима

Измене и допуне Закона о информационој безбедности 2019. године односиле су се на усклађивање са НИС Директивом која је у децембру 2022. године замењена НИС 2 Директивом.

Због тога је представљена упоредна анализа НИС и НИС 2 Директиве, како би се препознале разлике у правном оквиру које је неопходно превазићи. НИС Директива уводи 19 дефиниција, док је у НИС 2 Директиви овај број порастао на 41. Већина дефиниција из НИС Директиве задржана је и у НИС 2 Директиви у истом или практично истом облику, али је неколико дефиниција термина претрпело суштинске промене.

На пример, термин „инцидент” је у НИС Директиви дефинисан као било који догађај који има стварни нежељени ефекат на безбедност мрежних и информационих система, док је у НИС 2 Директиви овај термин дефинисан као догађај који компромитује доступност, аутентичност, интегритет или поверљивост складиштених, преношених или процесираних података, или услуга које се нуде или којима се приступа путем мрежних и информационих система. Дефиниција термина „руковање инцидентом” у НИС 2 Директиви проширена је превенцијом, реаговањем и опоравком, уз детекцију, анализу и ограничавање који су већ били укључени у дефиницију овог термина у НИС Директиви.

НИС Директива је у свом Члану 5 прописивала критеријуме за одређивање оператора есенцијалних сервиса:

- ентитет пружа сервис који је неопходан за одржавање критичних друштвених и/или економских активности;
- пружање тог сервиса зависи од мрежних и информационих система; и
- инцидент би имао значајне реметилачке ефекте на пружање тог сервиса.

Ови критеријуми нису задржани у НИС 2 Директиви, већ је ова Директива ентитете којима су прописане посебне обавезе поделила на есенцијалне и важне. У складу са овом поделом, одређени су и сектори високе критичности и остали критични сектори у којима се обављају делатности од посебног значаја. НИС 2 Директивом одређено је да у секторе високе критичности спадају:

- енергетика,
- саобраћај,
- банкарство,
- инфраструктуре финансијских тржишта,
- здравље,
- пијаћа вода,
- отпадне воде,
- дигитална инфраструктура,
- управљање ИКТ услугама,

- јавна администрација и
- свемир.

Уређено је да у остале критичне секторе спадају:

- поштанске и курирске услуге,
- управљање отпадом,
- производња и снабдевање хемикалијама,
- производња, обрада и дистрибуција хране,
- друге производне делатности (производња медицинских уређаја и in vitro дијагностичких медицинских средстава, рачунара, електронских и оптичких производа, електричне опреме, машина и уређаја, моторних возила, приколица и полуприколица и производња остале опреме за превоз),
- пружање дигиталних услуга и
- истраживање.

Одредбама НИС 2 Директиве прописано је да се есенцијалним ентитетима сматрају:

- ентитети који превазилазе величину средњих предузећа (имају више од 250 запослених и обрт од преко 50 милиона евра) и који своју делатност обављају у неком од високо критичних сектора;
- пружаоци квалификованих услуга од поверења, пружаоци услуге регистрације домена највишег нивоа и пружаоци услуга DNS без обзира на величину;
- пружаоци услуга јавних електронских комуникационих мрежа или јавно доступних електронских комуникационих услуга који спадају у предузећа средње величине;
- органи државне управе на централном нивоу;
- сви други ентитети који своје делатности обављају у високо критичним или критичним секторима, а које је држава чланица идентификовала као есенцијалне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу;
- ентитети идентификовани као критични у складу са Директивом 2022/2557;
- сви други ентитети идентификовани као есенцијални у складу са Директивом 2016/1148 (НИС Директива), ако држава чланица процени да је то потребно.

Важним ентитетима сматрају се ентитети који своје делатности обављају у високо критичним или критичним секторима, а који не испуњавају критеријуме да буду идентификовани као есенцијални. Такође, важним ентитетима се сматрају и они које је држава чланица идентификовала као важне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу.

НИС директивом прописано је да се одређивање шта представља значајан реметилачки ефекат препусти земљама чланицама, при чему је Директивом сугерисано да се у обзир узме:

- број корисника сервиса који пружа тај ентитет који су погођени прекидом;
- зависност других сектора којима припадају оператори есенцијалних сервиса од сервиса који пружа тај ентитет;
- утицај који би инциденти могли имати, у смислу обима и трајања, на економске и друштвене активности или јавну безбедност;
- тржишни удео тог ентитета;
- географско ширење у погледу подручја које би могло бити погођено инцидентом; и
- важност ентитета за одржавање довољног нивоа сервиса, узимајући у обзир доступност алтернативних могућности за пружање тог сервиса.

У НИС 2 Директиви није задржан појам значајног реметилачког ефекта, али су уведени појмови значајне сајбер претње и значајног инцидента. Значајна сајбер претња је као појам дефинисана у члану 3. НИС 2 Директиве као сајбер претња за коју се, на основу својих техничких карактеристика, може претпоставити да има потенцијал да озбиљно утиче на мрежне и информационе системе ентитета или кориснике његових услуга наношењем знатне материјалне или нематеријалне штете. Чланом 23, којим су прописане обавезе извештавања, дефинисано је да ће се инцидент сматрати значајним ако:

- је проузроковао или има капацитет да проузрокује озбиљне прекиде пружања услуга или озбиљне финансијске губитке угроженом ентитету, и
- је утицао или има капацитет да утиче на друга физичка или правна лица путем наношења значајне материјалне или нематеријалне штете.

НИС Директива обавезала је државе чланице да усвоје националну стратегију безбедности мрежних и информационих система која мора укључивати следеће:

- циљеве и приоритете националне стратегије безбедности мрежних и информационих система;
- оквир управљања за постизање циљева и приоритета ове стратегије, укључујући улоге и одговорности државних органа и других релевантних актера;
- утврђивање мера које се односе на припремљеност, реаговање и опоравак, укључујући сарадњу између јавног и приватног сектора;
- програме образовања, подизања свести и обуке;
- планове истраживања и развоја;
- план процене ризика ради њихове идентификације;
- списак актера укључених у спровођење националне стратегије безбедности мрежних и информационих система.

У НИС 2 Директиви такође постоји обавеза за државе чланице да усвоје националну стратегију (али се користи израз „национална стратегија информационе безбедности”), при чему је списак обавезних ставки остао сличан, а додате су и координација и сарадња. Такође, државама чланицама је дата обавеза да као део националне стратегије усвоје следеће политике:

- решавање информационе безбедности у ланцу снабдевања;
- укључивање и спецификацију захтева везаних за безбедност ИКТ производа и услуга у јавним набавкама;
- управљање рањивостима;
- одржавање опште доступности, интегритета и поверљивости јавног језгра отвореног интернета;
- промовисање развоја и интеграције релевантних напредних технологија са циљем имплементације најсавременијих мера за управљање ризиком у области информационе безбедности;
- промовисање и развој образовања и обука, вештина, подизања свести и иницијатива за истраживање и развој, као и смерница о добрим праксама и контролама сајбер хигијене;
- подршка академским и истраживачким институцијама у развоју, унапређењу и промоцији примене алата за информациону безбедност;
- подршка добровољној размени информација;
- јачање сајбер отпорности и основе сајбер хигијене малих и средњих предузећа;
- промовисање активне сајбер заштите.

Обе директиве прописују обавезе за државе чланице да одреде надлежне органе (један или више) и јединствену тачку контакта, као и да успоставе Тимове за хитно реаговање на инциденте - ЦСИРТ (енг. *Computer emergency response team*) са надлежностима које покривају секторе од посебног значаја.

НИС 2 Директивом задржане су одредбе о Групи за сарадњу и Мрежи ЦСИРТ-ова из НИС Директиве, уз нешто проширен скуп задатака за ова два тела.

НИС 2 Директивом детаљније су разрађене техничке, оперативне (додатна врста мера која није била поменута у НИС Директиви) и организационе мере за управљање ризицима по мрежне и информационе системе. У ове мере спадају:

- политике у вези анализе ризика и безбедности информационих система;
- руковање инцидентима;
- континуитет пословања и управљање кризама;
- безбедност ланца снабдевања;
- безбедност у набавци, развоју и одржавању мрежних и информационих система, укључујући откривање и руковање рањивостима;
- политике и процедуре за процену ефикасности мера за управљање ризиком;
- практиковање основних мера сајбер хигијене и обуке у циљу подизања безбедносне свести;
- политике и процедуре везане за коришћење криптографских метода;
- безбедност људских ресурса, политике контроле приступа и управљање асетима;
- коришћење мултифакторске аутентификације и других метода јаке аутентификације и коришћење безбедних комуникационих система, посебно у случају ванредних ситуација.

НИС 2 Директива задржала је одредбе о обавези извештавања о инцидентима, при чему се ова обавеза односи и на есенцијалне и на важне ентитете.

У односу на НИС Директиву, у новој Директиви уведена је обавеза за државе чланице да одреде или успоставе један или више надлежних органа одговорних за управљање великим инцидентима и кризама. Ако се одреди више органа, мора се недвосмислено одредити која институција координира њихов рад у случају великих инцидената и криза. Државе чланице такође морају усвојити национални план за одговор на велике инциденте и кризе који мора садржати:

- циљеве због којих се предузимају мере и активности,
- задатке и одговорности надлежних органа,
- процедуре за реаговање и њихово уклапање у општи оквир за реаговање у случају националне кризе, као и канале за размену информација,
- мере које је потребно предузети ради припреме, укључујући вежбе и обуке,
- организације из јавног и приватног сектора и инфраструктуру која се ангажује,
- процедуре и споразуме између националних надлежних органа.

НИС 2 Директивом прописани су слични захтеви и проширен скуп задатака за ЦСИРТ-ове (ЦЕРТ-ове) у односу на НИС Директиву. Додатни захтев у НИС 2 Директиви је да су ЦСИРТ-ови у обавези да обезбеде поверљивост и поузданост својих операција, а задаци за ЦСИРТ-ове су следећи:

- праћење и анализирање сајбер претњи, рањивости и инцидената на националном нивоу и, на захтев, пружање помоћи есенцијалним и важним ентитетима,
- пружање раних упозорења и других информација о ризицима и инцидентима есенцијалним и важним ентитетима, надлежним органима и другим субјектима од значаја,
- реаговање на инциденте и пружање помоћи есенцијалним и важним ентитетима (где је применљиво),
- пружање динамичке анализе ризика и инцидената и указивање на тренутну ситуацију,
- пружање есенцијалним и важним ентитетима услуге проактивног скенирања мрежних и информационих система ради откривања рањивости,
- учешће у Мрежи ЦСИРТ-ова,

- координација активности усмерених на координисано откривање рањивости (где је применљиво), и
- допринос примени безбедних алата за размену информација.

Одредбе о координисаном откривању рањивости су уведене у НИС 2 Директиву као нова тема (која није постојала у НИС Директиви). НИС 2 Директивом прописано је да државе чланице треба да одреде ЦСИРТ који ће бити координатор ових активности. Тај ЦСИРТ треба да делује као посредник од поверења и олакша комуникацију између оног ко пријављује рањивост (било да је у питању правно или физичко лице) и произвођача потенцијално рањивог производа или пружаоца потенцијално рањиве услуге. Задаци овог ЦСИРТ-а укључују:

- идентификацију и успостављање контакта са предметним странама,
- помоћ страни која пријављује рањивост и
- договарање о роковима за објављивање, као и управљање рањивостима које утичу на више ентитета.

Страни која пријављује рањивост мора бити загарантована анонимност ако то жели.

НИС 2 Директива даје задатак ЕНИСА-и да развије и одржава Европску базу рањивости, укључујући одговарајући информациони систем, политике и процедуре, као и да предузме неопходне техничке и организационе мере које ће гарантовати безбедност и интегритет ове базе података. База података ће бити доступна свим значајним ентитетима, а садржаће следеће податке:

- опис рањивости,
- обухваћене производе или услуге и озбиљност рањивости у смислу околности под којима она може бити експлоатисана и
- доступност одговарајуће закрпе или упутство за умањење ризика ако закрпа не постоји.

Новитет у НИС 2 Директиви је успостављање Европске мреже за организацију везе за сајбер кризе (EU-CyCLONe). Сврха успостављања ове мреже је подршка управљању великим инцидентима и кризама на оперативном нивоу и осигурање размене релевантних информација између држава чланица и институција ЕУ. Задаци ове мреже су:

- да повећа ниво припремљености за управљање великим инцидентима и кризама;
- да развије заједничку свест о ситуацији у вези са великим инцидентима и кризама;
- да процени последице и утицај релевантних великих инцидената и криза и предложи мере за ублажавање;
- да координира управљање великим инцидентима и кризама и подржи доношење одлука на политичком нивоу у вези са њима;
- да расправља, на захтев државе чланице, о националним плановима за реаговање на велике инциденте и кризе.

Нови задатак који је ЕНИСА добила НИС 2 Директивом је да, у сарадњи са Европском Комисијом и Групом за сарадњу, изради извештај о стању у ЕУ у области информационе безбедности и да га представи Европском Парламенту. Овај извештај се израђује сваке друге године и треба да обухвати:

- процену ризика на нивоу ЕУ;
- процену развоја капацитета у области информационе безбедности у јавном и приватном сектору;
- процену општег нивоа свести о информационој безбедности и сајбер хигијени међу грађанима и ентитетима, укључујући мала и средња предузећа;
- збирну процену нивоа зрелости капацитета и ресурса за информациону безбедност широм ЕУ, као и степена до којег су усклађене националне стратегије информационе безбедности држава чланица.

Група за сарадњу је НИС 2 Директивом добила задатак да до 17. јануара 2025. године, уз помоћ Европске Комисије, ЕНИСА и Мреже ЦСИРТ-ова, успостави методологију и организационе аспекте партнерских прегледа (енг. *peer reviews*), са сврхом учења из туђих искустава, ојачавања узајамног поверења, постизања високог заједничког нивоа информационе безбедности и побољшања капацитета и политика држава чланица да имплементирају ову Директиву. Партнерски прегледи морају бити доброољни и спровођени од стране најмање два експерта у области информационе безбедности који нису из државе чланице у којој се врши преглед. Партнерски прегледи морају обухватити макар једну од следећих процена:

- ниво имплементације мера за управљање ризицима у информационој безбедности и имплементације обавеза у вези извештавања утврђених овом Директивом;
- ниво способности, укључујући расположиве финансијске, техничке и људске ресурсе, и ефикасност извршавања задатака;
- оперативне способности ЦСИРТ-ова;
- ниво имплементације узајамне помоћи;
- ниво имплементације размене информација;
- посебна питања прекограничне или међусекторске природе.

НИС 2 Директивом је прописано да државе чланице могу захтевати од есенцијалних и важних ентитета да користе одређене ИКТ производе, услуге и процесе, који су сертификовани према европским шемама сертификације за информациону безбедност усвојеним у складу са Актом о сајбер безбедности. Поред тога, Европска Комисија има овлашћења да допуни ову Директиву прецизирајући које категорије есенцијалних и важних ентитета треба да користе одређене сертификоване ИКТ производе, услуге и процесе. Ако одговарајућа европска шема сертификације за информациону безбедност није доступна, Европска Комисија може захтевати од ЕНИСА да припреми ову шему.

Због наведених измена правног оквира Европске уније ствара се јаз у прописима које Република Србија, не само због обавеза преузетих у процесу хармонизације и прикључења Европској унији, већ због унапређења саме области, мора да превазиђе. Стога је неопходно извршити усклађивање правног оквира и Закон о информационој безбедности хармонизовати са наведеном Директивом.

Недостатак капацитета надлежних органа

Током имплементације Закона утврђено је да ИКТ системи од посебног значаја не достављају информације о свим инцидентима који значајно угрожавају информациону безбедност, иако су обавезни да то чине. Услед тога Национални ЦЕРТ није у могућности да у потпуности прати трендове у овој области, што има утицај и на анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањања потенцијалних инцидената.

За испуњавање свих законом предвиђених надлежности неопходно је да Национални ЦЕРТ и остали ЦЕРТ-ови основани у Републици Србији имају адекватне ресурсе. Постоји генерално мишљење у стручној јавности да се област информационе безбедности не схвата довољно озбиљно и да се могуће последице од напада на ИКТ системе потцењују, односно не придаје им се довољна пажња. Једно од питања које се често поставља је могућност обезбеђења неопходних људских ресурса и адекватна накнада за њихов рад, имајући у виду ситуацију на тржишту са овим кадром насупрот ограничењима која намећу прописи у јавном сектору. У том контексту потребно је сагледати капацитете (пре свега кадровске али и организационо-техничке) надлежног органа (у даљем тексту: Министарство). Као и код других државних и осталих органа, и Министарство се суочава са проблемом да привуче и задржи довољно стручан кадар који ће се бавити информационом безбедношћу.

Проблем са кадровима се посебно односи на послове инспекције за информациону безбедност, односно на чињеницу да тренутно инспекција броји два инспектора. Законом о

информационој безбедности предвиђено је да ова инспекција врши надзор над применом закона и над радом ИКТ система од посебног значаја. Имајући у виду број ИКТ система од посебног значаја јасно је да два инспектора не могу благовремено да спроведе надзор над већим бројем ИКТ система од посебног значаја. Законом је предвиђено да инспектор има овлашћења да наложи отклањање утврђених неправилности и да забрани коришћење поступака или техничких средстава којима се угрожава или нарушава информациона безбедност, као и да остави рок за примену наложених мера. С обзиром да је ово начин да се примене неке мере неопходне за сузбијање инцидената, у случају одсуства инспектора не постоји алтернативни начин за налагање тих мера.

Недостатак оперативних капацитета за реаговање на инциденте

У Републици Србији су у последњих неколико година развијани капацитети за реаговање на инциденте у неколико органа управе, али у већини организација, како у јавном сектору тако и генерално у онима које су надлежне за управљање ИКТ системима који припадају критичној инфраструктури, нема довољно изграђених капацитета, па углавном зависе од трећих лица. Национални ЦЕРТ реагује 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, док се надлежности ЦЕРТ-а органа власти у Канцеларији за информационе технологије и електронску управу односе, пре свега, на заштиту информационо-комуникационих система јединствене информационо-комуникационе мреже електронске управе.

Имајући ово у виду, чак ни законски није покривена оперативна помоћ другим ИКТ системима од посебног значаја, осим оних који се налазе у оквиру система електронске управе. У претходном периоду извршено је неколико озбиљних напада на ИКТ системе у јавном сектору у Србији (поменимо само нападе на ЈКП Информатика из Новог Сада и на Републички геодетски завод) који су захтевали ангажовање неких оперативних тимова из јавног сектора којима овакве интервенције нису у надлежности, али и специјализованих приватних компанија. Овакви примери јасно указују да постоји потреба за успостављањем оперативног тима који би имао надлежност, али и знање, да оперативно реагује у случајевима инцидената у ИКТ системима од посебног значаја када оператор угроженог ИКТ система нема сопствене капацитете за решавање инцидента.

Такође, један од идентификованих проблема је непостојање обавезних вежби на којима би се преиспитивале и увежбавале процедуре за реаговање у случају инцидента. Овакве вежбе су устаљена пракса у развијеним земљама, док се у Србији нису организовале у значајној мери. Изузетак су сајбер вежбе „Сајбер Тесла" које се од 2016. године у Републици Србији организују на годишњем нивоу у сарадњи Војске Србије и Националне гарде Охаја. У циљу подизања капацитета запослених у ЦЕРТ-овима у Републици Србији, укључујући и ЦЕРТ-ове самосталних оператора, у оквиру пројекта „Унапређење информационе безбедности на Западном Балкану" организоване су тренинзи и обуке. Један од идентификованих проблема приликом организације оваквих вежби је редован изостанак доносиоца одлука, односно делегирање ниже рангираних службеника у својству замене.

Недостатак системског прикупљања и размене информација

Национални ЦЕРТ има надлежност да прикупља и размењује информације о ризицима за безбедност ИКТ система, као и о 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. Национални ЦЕРТ је и тачка контакта са другим сличним организацијама ван Србије и са међународним организацијама и удружењима. У међународној пракси национални ЦЕРТ-ови добијају посебан положај и приступ информацијама у вези информационе безбедности које нису јавно објављене, како би могли да их дистрибуирају до субјеката којима су ове информације потребне. По овом питању Национални

ЦЕРТ је већ спровео одређене активности, као што су оне на имплементацији MISP платформе. Ове активности свакако треба наставити али је потребно укључити већи број субјеката.

Пријава инцидената је један од важних облика прикупљања информација. Може се констатовати да се побољшава дисциплина по питању поштовања ове законске обавезе али се не може рећи да се она у потпуности поштује, јер је извесно да се многи инциденти не пријављују, а откривају се у медијима или путем других канала комуникације. Разлози за непријављивање су разни – необавештеност да је пријављивање обавезно, недовољна свест о значају пријављивања, страх од угрожавања репутације, заузетост другим пословима, или једноставна небрига. Потребно је у континуитету подстицати пријављивање инцидената, посебно ако би то обезбедило и одређени ниво приступа систему за размену информација.

Низак степен превенције и заштите ИКТ система од посебног значаја

Законом о информационој безбедности дефинисано је да су ИКТ системи од посебног значаја системи који се користе у обављању послова у органима власти, за обраду посебних врста података о личности, у обављању делатности од општег интереса и других делатности у одређеним секторима (енергетика, саобраћај, здравство, банкарство и финансијска тржишта, дигитална инфраструктура, добра од општег интереса, услуге информационог друштва и остале области) и у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање претходно наведених делатности.

ИКТ системи од посебног значаја по овом Закону имају обавезу да се упишу у евиденцију оператора ИКТ система од посебног значаја, предузму мере заштите овог система, донесу акт о безбедности, врше периодичну проверу усклађености примењених мера заштите са усвојеним актом о безбедности, уреде однос са трећим лицима у складу са законом ако њима поверавају активности у вези са ИКТ системом од посебног значаја, достављају обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система и достављају статистичке податке о инцидентима у ИКТ систему.

Угрожавање ИКТ система од посебног значаја могло би да изазове последице по функционисање организација које њима управљају, али и на права и интересе грађана и привреде, као и на националну и јавну безбедност. Идентификовани проблеми са којима се суочавају ИКТ системи од посебног значаја односе се на недостатак довољног броја запослених (посебно оних са адекватим знањем), неодговарајућу опрему и недовољно развијену свест руководства о значају информационе безбедности. Ови проблеми су посебно изражени у јавном сектору. У приватном сектору постоји издвајање већих финансијских средстава за информациону безбедност.

Недостатак капацитета за реаговање на инциденте у државним институцијама

И поред обавезе предвиђене Законом о информационој безбедности, нису све институције у јавном сектору развиле капацитете за реаговање на инциденте. Органи управе имају проблем са привлачењем и задржавањем кадра за ове послове, о чему се посебно мора водити рачуна у будућности. Чак и институције које су формално успоставиле своје организационе целине и радиле на изградњи њихових капацитета морају континуирано да унапређују своје капацитете, док они који своје капацитете још увек нису изградиле могу добити, и добијају је, од стране оних који су одмакли у овом процесу.

Национални ЦЕРТ, који је основан 2017. године, и даље има потребе за подизањем капацитета без обзира што је у претходном периоду доста учињено по питању ангажовања нових запослених, набавке опреме и опремања простора. Сарадња са ЦЕРТ-ом органа власти и ЦЕРТ-овима самосталних оператора ИКТ система је успостављена и редовна, али може бити побољшана кроз интензивнију размену знања и искустава и брзу помоћ у случају инцидената.

Ради ефикаснијег реаговања у случају озбиљнијих инцидената, посебно оних од националног значаја, потребно је успоставити одговарајуће протоколе и процедуре за сарадњу, одредити особе за контакт и оранизовати редовне вежбе.

ЦЕРТ органа власти је превасходно усмерен на заштиту у оквиру јединствене информационо-комуникационе мреже електронске управе. Значајан број органа јавне власти повезан је на мрежу електронске управе и од велике користи би било подизање њихових капацитета за реаговање у случају инцидента и побољшање размене информација са ЦЕРТ-ом органа власти.

Недостатак координације за откривање рањивости

Овај аспект последњих година добија све више на значају на глобалном нивоу. Многи истраживачи и стручњаци раде на откривању рањивости и њиховом отклањању пре него што их открију криминалци и злонамерни корисници. У таквим ситуацијама чешће се догађа да криминалци добију отворену могућност да угрозе одређени ИКТ систем него да организација успе да за кратко време отклони рањивост, па је успостављање модела за систематично обавештавање о рањивостима начин да се ови проблеми отклоне.

Недовољна координација међународних активности

Република Србија активно учествује у многим међународним организацијама и процесима у области информационе безбедности, како на глобалном тако и на регионалном нивоу, као и у билатералним активностима. Између осталог, Република Србија учествује у раду Отворене радне групе УН за питања информационе безбедности, имала је представника у петој Групи владиних експерата УН, активно учествује у раду Неформалне радне групе ОЕБС основане одлуком Сталног савета број 1039, спонзор је имплементације Мере ОЕБС за изградњу поверења број 9, члан је Глобалног форума за сајбер експертизу и има именоване представнике у свих пет радних група овог Форума. Институције из Републике Србије често учествују у активностима које се реализују у оквиру међународних пројеката из области информационе безбедности, укључујући обуке, радионице, састанке и конференције.

Досадашња пракса подразумевала је ангажовање представника из неколико институција из јавног сектора у међународним организацијама и телима. Таква пракса није проблем сама по себи, али може довести до неконзистентног става различитих представника због мањка информација о позицији Србије или активностима представника у другим организацијама. Значајно би било успостављање обавезних консултација представника Србије у међународним организацијама у области информационе безбедности, узимајући у обзир надлежности Министарства спољних послова.

4) Која промена се предлаже и да ли је промена заиста неопходна и у ком обиму?

Измене Закона о информационој безбедности инициране су пре свега због усклађивања са европском НИС 2 Директивом (енг. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 - NIS 2 Directive) усвојеној 14. децембра 2022. године, али и у делу сертификације ИКТ система са Актом о сајбер безбедности - Уредба 2019/881 (енг. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) усвојеној 17. априла 2019. године.

Поред тога, на основу досадашње примене Закона утврђене су и друге потребе које због недовољне имплементације свих законских решења захтевају не само измену правног, већ и институционалног оквира. Због тога ће посебно бити представљене најпре промене важећег институционалног оквира уређеног Законом, а затим и друге измене, као резултат хармонизације са европским правним оквиром.

Предлози измена институционалног оквира

Недостатак капацитета надлежних органа у области информационе безбедности захтева и измену институционалног оквира. У циљу проналажења најбољег модела анализирани су примери институционалног оквира три европске земље: Савезне Републике Немачке, Великог Војводства Луксембург и Краљевине Холандије који су представљени у наставку.

Савезна Република Немачка

За област информационе безбедности на федералном нивоу у Немачкој је надлежно федерално Министарство унутрашњих послова (Министарство унутрашњих послова и заједнице). Међутим, Немачка је земља са јаким федерализмом и надлежности федералних јединица су веома широке, па је регулисање области информационе безбедности представљало велики изазов за ову државу, што је чак довело и до измена Устава.

Прву стратегију информационе безбедности Немачка је усвојила 2011. године, 2016. године је усвојила измене те стратегије, а 2021. године је усвојила нову Стратегију информационе безбедности за Немачку. У новој Стратегији дефинисана су четири принципа:

- Успостављање информационе безбедности као заједничког задатка за Владу, приватни сектор, истраживачку заједницу и друштво у целини,
- Оснаживање дигиталног суверенитета Владе, приватног сектора, истраживачке заједнице и друштва у целини,
- Остваривање безбедне дигиталне трансформације и
- Постављање мерљивих и транспарентних циљева.

Надлежност пружања информационе безбедности на националном нивоу има Федерална канцеларија за информациону безбедност (Bundesamt für Sicherheit in der Informationstechnik, BSI). Ова Канцеларија успостављена је 1991. године и припада немачком федералном Министарству унутрашњих послова, а надлежности су јој додељене Актом о Федералној канцеларији за информациону безбедност који је регулисао област информационе безбедности у Немачкој на националном нивоу. Седиште Канцеларије је у Бону, а тренутно има преко 1400 запослених.

Након усвајања НИС Директиве ЕУ, у Немачкој је њихов правни систем усклађен амандманима на Акт о Федералној канцеларији за информациону безбедност и на неколико других закона у области јавних сервиса. Неке од надлежности које има БСИ како би испунила своје задатке су:

- Превенција претњи по безбедност федералних ИКТ система,
- Тестирање и процена безбедности ИКТ система и компоненти и издавање безбедносних сертификата, и
- Развој техничких безбедносних стандарда за федералне ИКТ системе.

Нове измене правног оквира направљене су 2021. године усвајањем у Бундестагу Акта о ИТ безбедности Немачке 2.0 (прва верзија усвојена је 2015. године) којима је Федерална канцеларија за информациону безбедност добила нове и ојачала постојеће надлежности у следећим областима:

- Детекција и одбрана – повећане надлежности у детекцији безбедносних рањивости и одбрани од сајбер напада, овлашћења за постављање обавезујућих минималних стандарда за федералне институције, мониторинг имплементације постављених стандарда, постављање правила за безбедну дигитализацију;
- Безбедност у мобилним мрежама – уређење забране коришћења критичних компоненти, безбедносни захтеви за операторе мобилних сервиса, обавеза сертификације критичних компоненти, примена информационе безбедности у 5G мобилним мрежама;
- Заштита потрошача – саветовања потрошача о безбедносним питањима (нова функција Канцеларије), увођење ознаке „IT Security Mark“ на производима;
- Безбедност пословања – проширење критичне инфраструктуре на област одлагања смећа, обавеза имплементације безбедносних мера за организације од посебног јавног интереса (које не припадају критичној инфраструктури);

- Национална сајбербезбедносна сертификација – надлежности Националног ауторитета за сајбербезбедносну сертификацију (у складу са Актом о сајбер безбедности ЕУ).

Организациона структура Федералне канцеларије за информациону безбедност састављена је од осам директората:

- Централни послови,
- Технички центар изврсности,
- Технологије информационих уверења и управљање ИТ,
- Оперативна информациона безбедност,
- Стандардизација, сертификација и информациона безбедност телекомуникационих мрежа,
- Информациона безбедност за дигитализацију и електронске идентитете,
- Консултације за институције Федерације, федералних јединица и локалних власти и
- Информациона безбедност за приватни сектор и друштво.

Сваки од директората организован је кроз ниже организационе јединице. Канцеларијом управља председник, којем су директно подређене још три организационе јединице:

- Биро за стратешке комуникације и медије,
- Јединица за стратешку контролу и интерне провере и
- Јединица за стратешку и извршну подршку.

У оквиру Канцеларије делују неке од најзначајнијих организационих целина за сајбер одбрану:

- Национални центар за сајбер одбрану – платформа за сарадњу и размену информација о сајбер претњама и за усклађивање активности Владе на превенцији и сузбијању сајбер напада; у раду Националног центра учествују представници полиције, служби безбедности (војних и цивилних), федералне канцеларије за цивилну заштиту и помоћ у ванредним ситуацијама и војне сајбер команде;
- Савез за информациону безбедност – јавно-приватно партнерство у области информационе безбедности у којем учествује преко 4000 компанија;
- Федерални ЦЕРТ (CERT-Bund) – централна тачка контакта за превентивне и реактивне мере у случајевима сајбер инцидената у федералним институцијама; и
- ИТ Ситуациони центар – надлежан за координацију одговора у случајевима сајбер инцидената.

Савет за информациону безбедност формиран је 2011. године на основу Стратегије за информациону безбедност Немачке и са циљем да унапреди сарадњу на нивоу федералне Владе у области информационе безбедности. Измене Стратегије из 2016. године дефинисале су перманентну улогу овог Савета као саветодавног органа федералне Владе. Састанцима Савета руководи Главни службеник за информисање (CIO) федералне Владе. Савет има обавезу да Влади подноси извештаје о стратешким питањима у области информационе безбедности о којима расправља. Од 2018. године успостављена је и посебна радна група са задатком да помаже Савету у раду.

Проблем са којим се суочавају све земље, па и Немачка, јесте прављење разлике између унутрашње безбедности, која је традиционално у надлежности полиције, и спољне безбедности, која је традиционално у надлежности војске. У сајбер простору ова граница није сасвим јасна, а све већа употреба сајбер простора за војне активности намеће потребу да се одређене активности дефинишу и спроведу. Из тог разлога Немачка је 2017. године дефинисала сајбер и информациони војни домен, поред постојећих копненог, поморског и ваздушног, и успоставила нову службу надлежну за овај домен. Према расположивим подацима у овој служби је 2020. године било запослено преко 14.000 цивилног и војног особља. Такође, из разлога специфичности сајбер простора по питању унутрашње и спољне безбедности, договором немачких политичких партија је 2018. године одлучено да се формира заједничка агенција Министарства одбране и Министарства унутрашњих послова са задатком да спроводи

креативне и иновативне пројекте из области информационе безбедности. На основу овог договора, 2020. године формирана је Сајбер агенција (Agentur für Innovation in der Cybersicherheit или Cyberagentur) у форми компаније са ограниченом одговорношћу (GmbH) чији је једини акционар федерална Влада. Ова Агенција има око 100 запослених (према расположивим подацима) и не спроводи самостално истраживања, већ у сарадњи са академијом и индустријом спроводи иновативне пројекте за које се процени да су од изузетног националног значаја (посебно их интересују теме као што су поуздане и отпорне информационе технологије, интеракција човека и технологије, вештачка интелигенција, нано и квантна технологија, свемирска и поморска безбедност, бионика, интерфејси мозак-рачунар, предиктивна аналитика, криптографија или аутономни системи). Агенција је за своје активности добила иницијални буџет од 280 милиона евра од којих је већи део већ уложила у истраживачке пројекте.

Још једна значајна платформа коју је покренуло немачко Министарство одбране је Сајбер иновациони хаб, са намером да привуче младе и креативне умове да кроз стартап-ове и окружење које више одговара њиховом начину размишљања реализују пројекте од значаја за одбрану. Сајбер иновациони хаб је у суштини платформа за реализацију пројеката, а формално је организован као огранак компаније која пружа ИТ услуге за немачку армију, која доноси крајњу одлуку који пројекти ће се финансирати.

Велико Војводство Луксембург

Документ јавних политика у области информационе безбедности у Луксембургу је национална стратегија информационе безбедности. До сада је Луксембург усвојио четири стратегије, а последња се односи на период од 2021. до 2025. године. Свака од стратегија доносила је одређена унапређења, па је тако прва стратегија иницирала оснивање Владиног ЦЕРТ-а, друга успостављање Националне агенције за безбедност информационих система (фра. *Agence nationale de la sécurité des systèmes d'information - ANSSI*), трећа формирање Центра за компетенције у области информационе безбедности (енг. *Cybersecurity Competence Center - C3*), успостављање методологије за анализу ризика *MONARC* и формирање Међуминистарског координационог комитета за сајбер превенцију и информациону безбедност (Comité interministériel de coordination en matière de cyberprévention et de cybersécurité), док четврта предвиђа формирање *SOC* за критичну инфраструктуру, формирање Националног центра за филтрирање *DDoS* напада, развој платформе за анализу и управљање ризицима *SERIMA* намењене операторима есенцијалних сервиса и друго. Институција надлежна за израду и координацију стратегије је Високи комесаријат за националну заштиту (HCPN).

Луксембург је у мају 2019. године транспоновао НИС Директиву ЕУ у своје законодавство и одредио Регулаторни институт Луксембурга *ILR* за јединствену тачку контакта и надлежни орган за секторе енергетике, транспорта, здравља, пијаће воде и дигиталне инфраструктуре, док је Комисија за надзор сектора финансија *CSSF* надлежни орган за секторе инфраструктуре финансијских тржишта и кредитних институција.

Луксембург нема централни орган који би обједињавао надлежности у области информационе безбедности, него су надлежности дате различитим институцијама. Стратешке надлежности имају две институције: Тело за информациону безбедност *CSB* и Међуминистарски координациони комитет за сајбер превенцију и информациону безбедност (CIC-CPCS). Надлежност над координацијом активности ова два тела и задатак стратешког вођства има Високи комесаријат за националну заштиту.

Тело за информациону безбедност формирано је 2011. године са задатком да имплементира и надзире извршавање прве националне стратегије, а од 2019. године налази се у надлежности Министарства државе.

Међуминистарски координациони комитет за сајбер превенцију и информациону безбедност успостављен је 2017. године са циљем да се, у сарадњи са Телом за

информациону безбедност, ангажује на координацији оперативних активности. У раду Комитета учествују представници следећих институција:

- Министарство државе,
- Високи комесаријат за националну заштиту,
- Одбрана Луксембурга (Директорат за одбрану и Оружане снаге Луксембурга),
- Министарство привреде,
- економска интересна група SECURITYMADEIN.LU,
- Владин центар за информационе технологије (CTIE),
- Државна обавештајна служба,
- Национална агенција за безбедност информационих система (ANSSI) и
- Владин ЦЕРТ (GovCERT).

Радом комитета председава Високи комесар за националну заштиту. Задаци који су постављени пред овај Комитет су:

- обезбеђење конзистентности акција и иницијатива,
- координација имплементације иницијатива које долазе од ЕУ или са других међународних нивоа,
- надзор над имплементацијом ових иницијатива,
- давање савета Влади по питањима информационе безбедности и
- дискусија о ставовима националних представника.

Високи комесаријат за националну заштиту је тело које је постојало током Хладног рата као канцеларија Комитета за националну заштиту (са задацима везаним за заштиту органа власти и становништва, прикупљање обавештајних података, спровођење психолошких операција и слично) и потом укинуто, али је реактивирано након терористичких напада 11. септембра 2001. са новим надлежностима у области заштите критичне инфраструктуре и од 2016. године уврштено у састав Министарства државе. Високи комесаријат је надлежан за превенцију и управљање сајбер кризама и за планирање одговора на ванредне ситуације у области информационе безбедности. За сајбер дипломатију надлежно је Министарство спољних и европских послова.

Национална агенција за безбедност информационих система (ANSSI) је надлежна за системе у државним органима. Ова Агенција је формирана 2015. године и саставни је део Високог комесаријата за националну заштиту као регулаторни орган. Неке од надлежности ANSSI су:

- израда политика и водича за заштиту класификованих и некласификованих информација,
- обезбеђење примене мера заштите информационих система,
- сертификација начина обраде некласификованих информација,
- функције Националног и Владиног ЦЕРТ-а и
- надлежни орган за ТЕМПЕСТ.

ANSSI је до 2018. године био и надлежни орган за одобравање криптографских производа, када су те надлежности пренете на Владин центар за информационе технологије (CTIE). ANSSI је до те године био и тело надлежно за управљање сајбер инцидентима, када је та улога пренета на Владин ЦЕРТ. Владин центар за информационе технологије (CTIE) је основан 2009. године и представља централни орган за послове везане за информационе технологије за министарства и државну администрацију. CTIE је такође и надлежни орган за дистрибуцију криптографског материјала и надлежни орган за криптографску акредитацију, а у надлежности му спадају и заштићена комуникација и размена информација између државних органа.

Владин ЦЕРТ (GovCERT) је основан 2013. године са задатком да решава све озбиљније сајбер инциденте у ИКТ системима Владе. Од 2015. године GovCERT је од ANSSI преузео надлежности управљања сајбер инцидентима и објединио улоге Националног и Владиног

ЦЕРТ-а, а од 2018. године му је, поред постојећих, поверена и функција Војног ЦЕРТ-а (MilCERT) и смештен је у Високи комесаријат за националну заштиту. У оквиру надлежности Националног ЦЕРТ-а, GovCERT је званична национална тачка контакта са ЦЕРТ-овима других земаља и тачка за контакт и размену информација са секторским ЦЕРТ-овима у Луксембургу. GovCERT, у оквиру својих надлежности као Војни ЦЕРТ, делује као званична тачка контакта за војне ЦЕРТ-ове других земаља, али и прати и реагује на инциденте у ИКТ системима Оружаних снага.

Економска интересна група Security Made in Lëtzebuerg (познатија као SECURITYMADEIN.LU) је основана 2010. године са мандатом од Министарства привреде (које и надзире њен рад) да спроводи истраживања на међународном нивоу, дели информације о претњама, имплементира мрежу сензора за рана упозорења и делује као хаб за економске активности у овој области. Финансијска средства за рад групе обезбеђује држава. SECURITYMADEIN.LU у свом саставу има три организационе јединице: Центар за реаговање на компјутерске инциденте (енг. *Computer Incident Response Center Luxembourg - CIRCL*), Сервисе подизања безбедносне свести у сајбер свету и безбедносна побољшања (CASES) и Центар за компетенције у области информационе безбедности (C3).

Можда и најпознатија организација из области информационе безбедности из Луксембурга је CIRCL који је надлежан за приватни сектор, локалну самоуправу и невладине организације. CIRCL је глобално познат по својој платформи за дељење информација о претњама MISP, а од других иницијатива у којима учествује вреди поменути заједницу CERT.LU која обезбеђује размену информација и сарадњу приватних ЦЕРТ-ова са CIRCL и GovCERT.

Cyberworld Awareness and Security Enhancement Services Luxembourg (CASES) обезбеђује публикације, едукативни материјал, примере најбољих пракси и разне алате везане за информациону безбедност (између осталог, метод за анализу ризика MONARC).

Центар за компетенције у области информационе безбедности (C3) активности реализује кроз давање мишљења, тренирање и тестирање, претежно за приватни сектор.

Национални ауторитет за сертификацију у области информационе безбедности је Институт за стандардизацију, акредитацију, сигурност и квалитет производа и услуга (ILNES).

Луксембург има усвојен план за реаговање у случају сајбер кризе (фра. *Plan d'intervention d'urgence en cas d'attaque contre les systèmes d'information ou de faille technique des systèmes d'information - PIU Cyber*) за чију рализацију је одговоран директно премијер. Овај план је развијен од стране Високог комесаријата за националну заштиту и има четири главна циља:

- усвајање заштитних и превентивних мера,
- дефинисање улоге ентитета за управљање кризама,
- дефинисање мера, поступака и актера у случајевима ванредних ситуација и
- узбуњивање и информисање јавности.

План предвиђа успостављање четири *ad-hoc* јединице за решавање кризе: јединице за кризу, оперативне јединице, јединице за процену сајбер ризика и јединице за комуникације и информисање. План укључује задатке сваке од ових јединица, њихов састав, субординацију, извештавање и све остале елементе који су потребни за успешно решавање кризе.

Краљевина Холандија

Холандија је прву стратегију информационе безбедности усвојила 2011. године, а тренутно важећа је стратегија усвојена за период од 2022. до 2028. године. Нова Стратегија усмерава активности у четири главна смера:

- побољшање друштвене отпорности кроз заједничке напоре јавног, приватног и невладиног сектора,
- подстицање безбедности дигиталних производа и услуга у складу са прописима ЕУ,

- сузбијање сајбер претњи које потичу од држава и криминалаца кроз побољшање прикупљања и дељења информација, и у јавном и приватном сектору и
- обезбеђење квалитетне радне снаге у области информационе безбедности, образовање и подизање свести грађана.

Једна од најважнијих активности планирана Стратегијом је спајање неколико организација са преклапајућим надлежностима - NCSC, Центра за дигитално поверење (DTC) и ЦСИРТ-а провајдера дигиталних сервиса (CSIRT-DSP) у једну организацију, која ће постати јединствени национални ауторитет за информациону безбедност. Холандија је овом Стратегијом исказала снажну посвећеност обједињавању постојећих капацитета и неопходност брзе спознаје информација о претњама и рањивостима и реаговања на ове информације. Стратегијом је чак наглашена потреба сузбијања фрагментације у дељењу информација кад год је могуће и потреба за рестриктивношћу у формирању нових ЦЕРТ-ова. У том циљу, нови ауторитет (за који се очекује да ће бити успостављен током 2024. године) радиће у сарадњи са јавним и приватним сектором и пружати информације о безбедности свим секторима, организацијама које спадају и које не спадају у критичну инфраструктуру и генералној јавности.

У Холандији је препознато више од 20 институција са индивидуалном и колективном одговорношћу у области информационе безбедности. На политичком и стратешком нивоу најважније тело је Савет за информациону безбедност.

Савет за информациону безбедност формиран је 2011. године као тело које треба да повеже различите актере из јавног и приватног сектора и са мандатом да саветује Владу и приватни сектор, постави националне приоритете, процени потребе за истраживањем и развојем и обезбеди размену знања у оквиру јавног и приватног сектора. За рад Савета надлежно је Министарство безбедности и правде, а у раду Савета учествују представници из јавног и приватног сектора. Јавни сектор је заступљен са 15 представника из следећих институција:

- Национални координатор за безбедност и сузбијање тероризма (у саставу Министарства безбедности и правде),
- Министарство економских послова,
- Министарство одбране,
- Генерални обавештајни и безбедносни сервис,
- Агенција за националне полицијске сервисе и
- Генерални одбор тужилаца.

Из приватног сектора у раду Савета учествују представници водећих провајдера телекомуникационих услуга, водећих снабдевача ИКТ опремом, корисника ИТ услуга, малих и средњих предузећа, оператора критичне инфраструктуре и академских институција. Радом Савета копредседавају Национални координатор за безбедност и сузбијање тероризма и представник приватног сектора (који се периодично мења).

Национални центар за информациону безбедност (NCSC) формиран је 2012. године са задатком да унапреди разумевање развоја, претњи и трендова у области информационе безбедности и преузме одговорност у решавању сајбер инцидената и управљању сајбер кризама. У састав NCSC приликом оснивања инкорпориран је постојећи Владин ЦЕРТ (GOVCERT.NL). У надлежност NCSC спада пружање услуга Влади и ИКТ системима критичне инфраструктуре у јавном и приватном сектору, као и унапређење јавно-приватног партнерства. NCSC је организационо смештен у Директорату за информациону безбедност Министарства безбедности и правде, а директно је потчињен Националном координатору за безбедност и сузбијање тероризма. NCSC чине три тима са надлежностима за реаговање на инциденте, едукацију и развој. У Директорату за информациону безбедност постоји и посебно Одељење за политике у чијој је надлежности развој политика и стратегија у области информационе безбедности.

Надлежност NCSC обухвата поступање са претњама и инцидентима, подизање безбедносне свести, давање савета, реаговање у случају кризе и пружање платформе за сарадњу. NCSC је такође веома активан у међународној сарадњи и национална тачка контакта Холандије. NCSC има кључну координациону улогу у случају озбиљног сајбер инцидента или сајбер кризе. Да би успешно остварио овај задатак, NCSC континуално прати стање, врши процене угрожености и могућих последица и реагује у случају потребе. Једна од најважнијих активности NCSC је управо прикупљање информација, како од јавног и приватног сектора у Холандији тако и од међународних партнера.

У случају озбиљног сајбер инцидента или сајбер кризе NCSC активира Одбор за ИКТ одговор (IRB) и даје подршку његовим активностима кроз прибављање и дистрибуцију информација и административну подршку. С обзиром да је у Холандији велики део критичне инфраструктуре у приватном сектору, у раду IRB учествују, поред представника институција Владе, и представници провајдера телекомуникационих услуга, енергетског и финансијског сектора, а по потреби се могу укључити и други експерти. Радом IRB руководи представник Министарства економских послова. Примарни задатак IRB је да саветује национална тела за управљање кризама о мерама које треба предузети, али такође и да служи као тело које у случају кризе спаја технички и административни ниво.

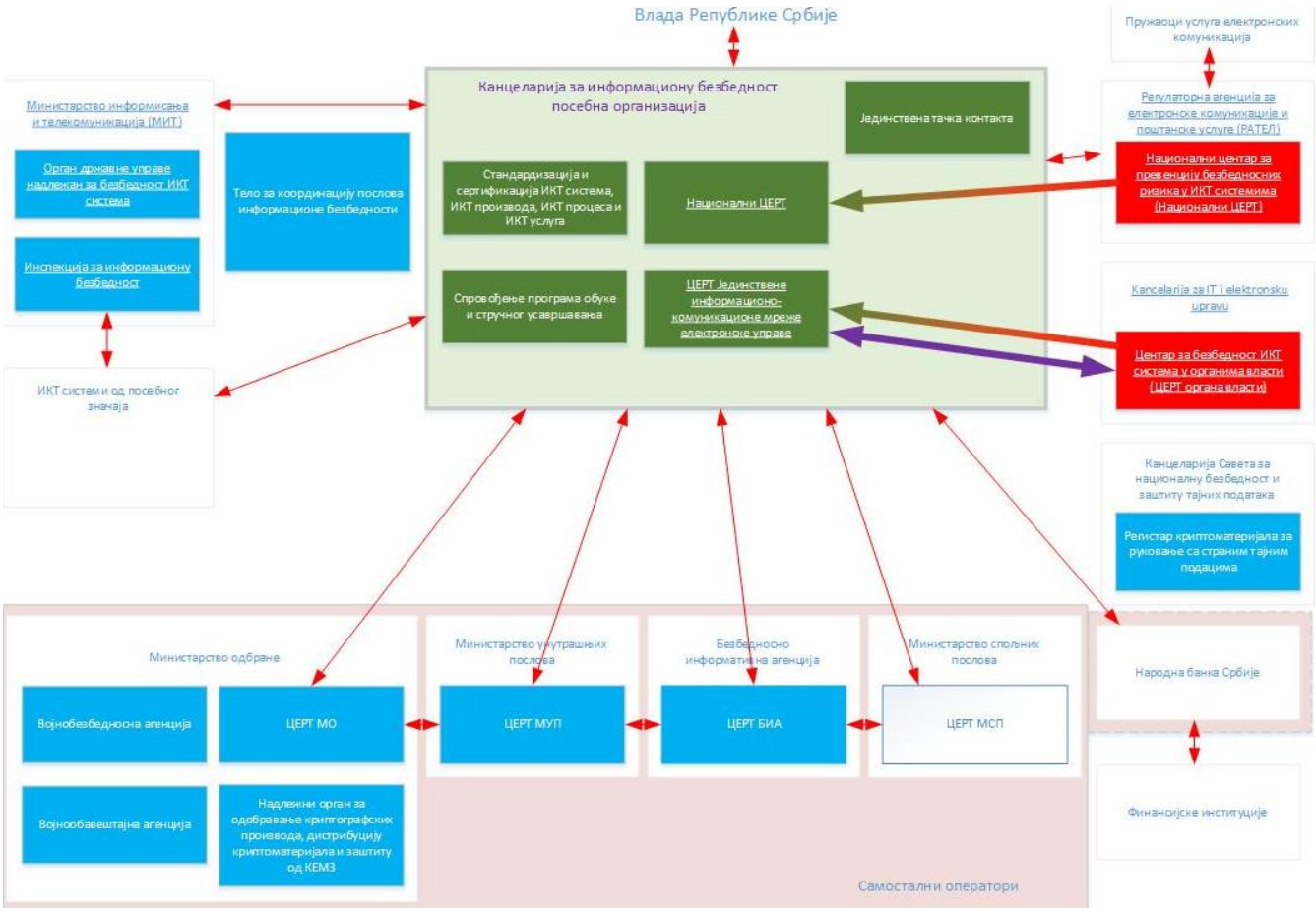
Холандија је 2012. године препознала сајбер простор као пети домен војних операција (поред земље, мора, ваздуха и свемира) и дефинисала шест области развоја сајбер капацитета: одбрана, напад, обавештајне активности, адаптивност, иновације и сарадња. Заједничка команда за управљање информацијама (JIVC) формирана је 2013. године, а у њен састав ушао је и ЦЕРТ одбране (DefCERT) формиран годину дана раније. Надлежности DefCERT су у домену безбедности ИКТ система Министарства одбране и Оружаних снага Холандије, подршке војним операцијама, процене претњи и рањивости, давања савета и слично, али такође и подршка државним органима у заједничком одговору на сајбер претње. DefCERT и NCSC су потписали меморандум о разумевању и интензивно сарађују кроз размену информација и узајамну подршку.

Одбрамбена сајбер команда је формирана 2014. године са примарним фокусом на успостављање одбрамбених, нападачких и обавештајних капацитета у сајбер простору. У састав Одбрамбене сајбер команде приликом успостављања ушле су организационе јединице осталих служби, чиме је успостављена јединствена целина у одбрамбеном систему Холандије надлежна за ову област.

Предлози унапређења институционалног оквира у Републици Србији

Анализа постојећег институционалног оквира показује расипање капацитета надлежних органа за превентивно и благовремено реаговање на инциденте у сајбер простору.

У складу са наведеним моделима европским земаља приликом израде Нацрта анализирана су три модела институционалне промене који су дати у наставку текста.



Дијаграм 19 Институционални оквир - модел 1

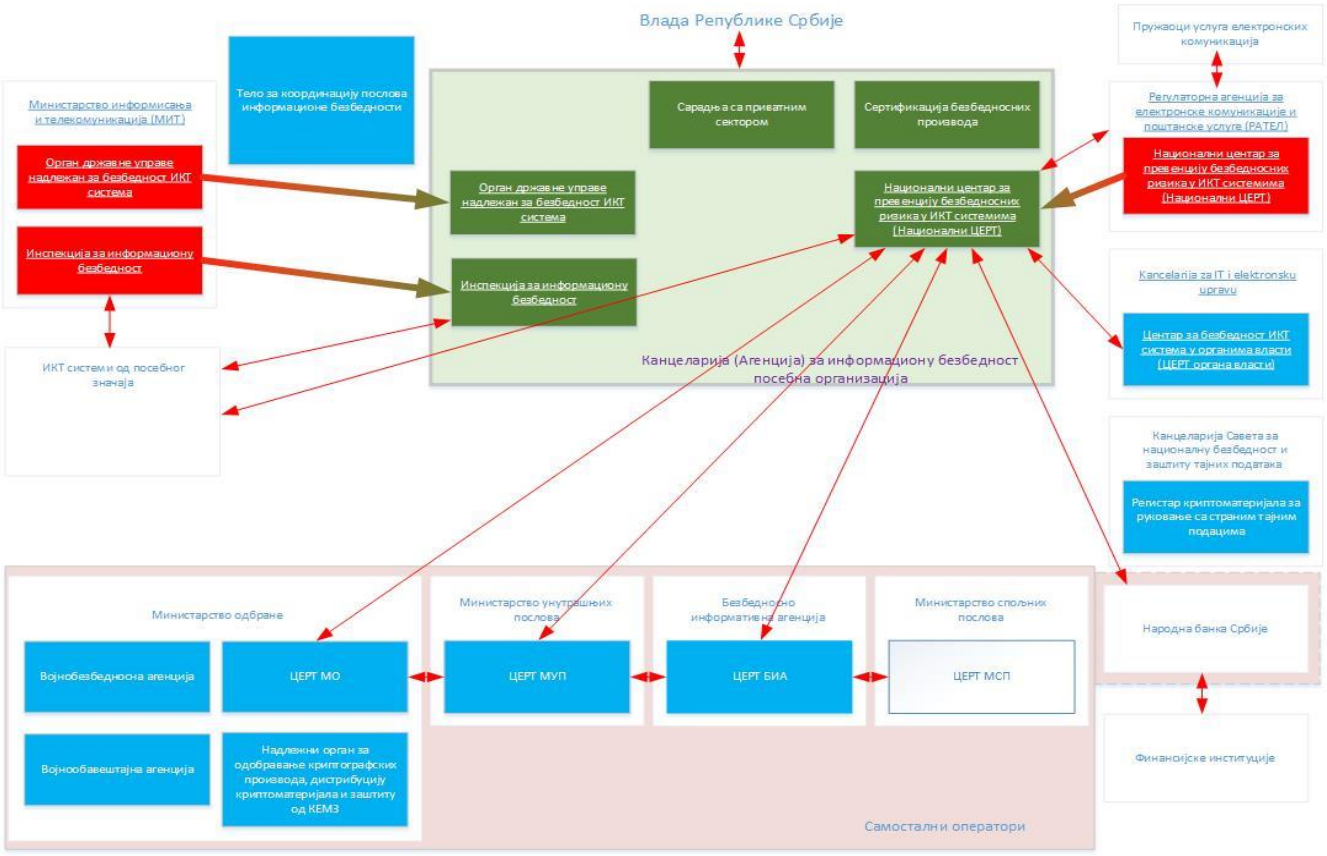
Новина:

- Формира се посебна организација - Канцеларија за информациону безбедност која постаје јединствена тачка контакта
- На нову Канцеларију преносе се надлежности Националног ЦЕРТ-а и Владиног ЦЕРТ-а (и постојеће организационе јединице и запослени).

Предности оваквог модела институционалног оквира су у успостављању јединствене, препознатљиве институције (посебне организације), груписању постојећих капацитета, стварању услова за бољу и бржу размену информација, као и услова за конкретну помоћ другим органима државне управе у случају сајбер инцидената (на пример МСП-у или Канцеларији за ИТ и еУправу). Недостатак оваквог модела институционалног оквира су потенцијални проблем за цео јавни сектор у случају недовољних капацитета нове Канцеларије и недостатак подршке да се прихвати пренос својих надлежности и запослених у нову Канцеларију.

Другим моделом:

- Формира се посебна организација - Канцеларија за информациону безбедност која постаје Надлежни орган и јединствена тачка контакта
- На нову Канцеларију преносе се надлежности Инспекције за информациону безбедност и Националног ЦЕРТ-а.



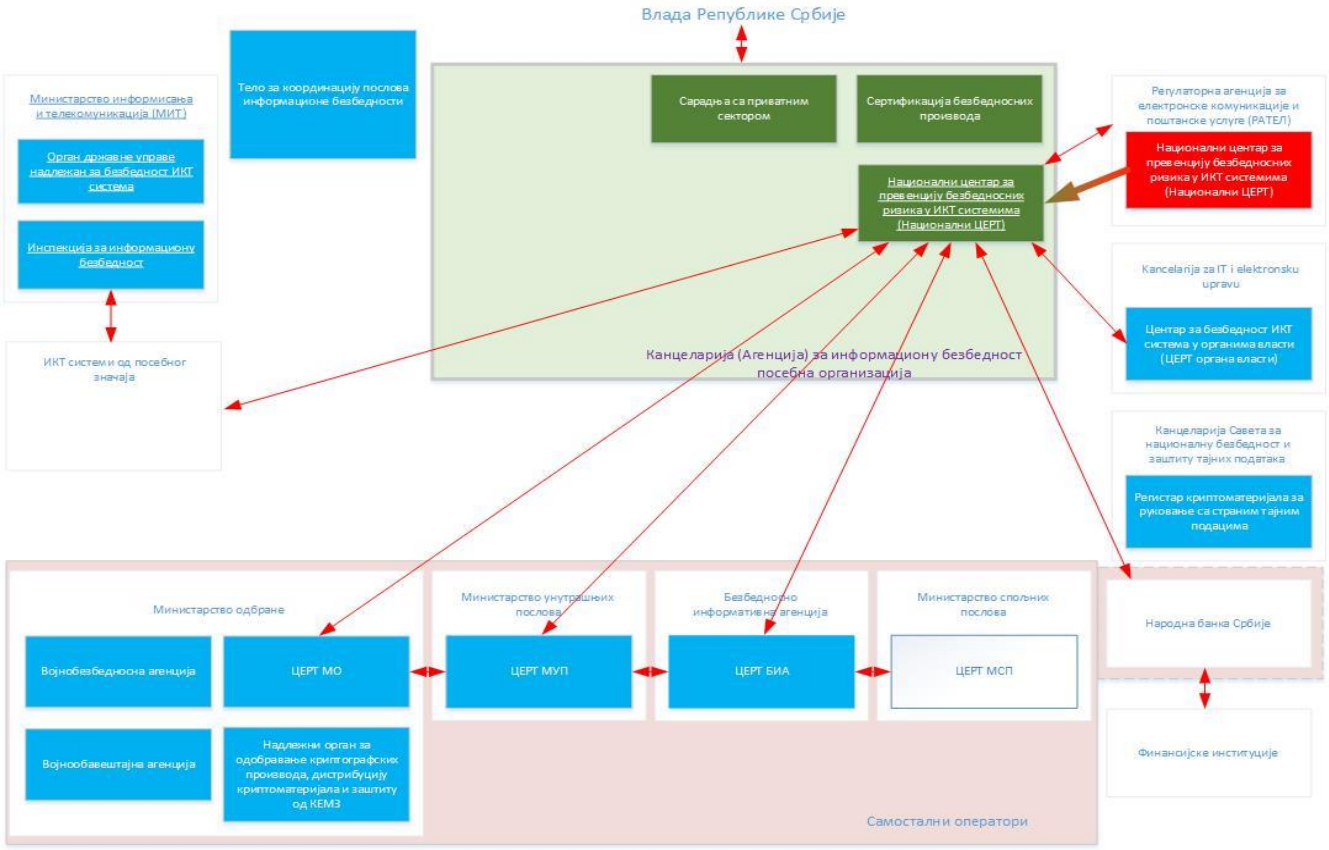
Дијаграм 20 Институционални оквир - модел 2

Предности оваквог модела институционалног оквира су у повећању капацитета за подршку ИКТ системима од посебног значаја и стварање услова за бољу и бржу размену информација. Недостатак оваквог модела институционалног оквира су ограничене могућности за сарадњу по питању оперативних активности, као и недостатак политичке подршке да се прихвати пренос својих надлежности и запослених у нову Канцеларију.

Трећим моделом:

- Формира се посебна организација - Канцеларија (Агенција) на коју се преносе надлежности Националног ЦЕРТ-а.

Предности оваквог модела институционалног оквира је у бржој имплементацији модела која не захтева велике промене, док су недостаци оваквог модела институционалног оквира у формирању још једне посебне организације која ће се делимично бавити питањима информационе безбедности.



Дијаграм 21 Институционални оквир - модел 3

Након анализе модела и пракси европских земаља одлучено је да се прихвати први модел.

У Предлогу закона предложено је у члану 28. оснивање Канцеларија за информациону безбедност, као посебне организације у смислу закона којим се уређује положај државне управе ради обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији. Канцеларија има својство правног лица. Радом Канцеларије руководи директор кога именује Влада, у складу са законом којим се уређује положај државних службеника, а кога председнику Владе предлаже министар надлежан за послове информационе безбедности.. Канцеларија има заменика директора, који мора бити лице одговарајуће стручности, који се поставља у складу са прописима којим се уређује положај државних службеника и има овлашћења у складу са прописима о државној управи.

Надзор над радом Канцеларије у вршењу послова спроводи Министарство, у складу са законом којим се уређује државна управа.

Надлежности Канцеларије за информациону безбедност уређене су члановима 30-34. Канцеларија за информациону безбедност успоставља се и послове из своје надлежности прописане овим законом почиње да обавља 1. јануара 2027. године.

Послове Канцеларије за информациону безбедност прописане овим законом обавља Канцеларија за информационе технологије и електронску управу у периоду који почиње даном наступања 12 месеци од дана ступања на снагу овог закона и који траје до 1. јануара 2027. године.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 12 месеци од дана ступања на снагу овог закона.

Министарство и даље води евиденцију оператора ИКТ система од посебног значаја и врши надзор над радом новоосноване Канцеларије. На овај начин удружују се постојећи капацитети два ЦЕРТ-а, што би у значајној мери требало да побољша координацију и реаговање на инциденте.

Усклађивање са европским прописима

Директива ЕУ 2022/2555 о мерама за висок заједнички ниво информационе безбедности широм Уније утврђује мере које имају за циљ постизање високог заједничког нивоа информационе безбедности унутар ЕУ како би се побољшало функционисање унутрашњег тржишта. Овом Директивом дати су амандмани на Уредбу ЕУ 910/2014 о електронској идентификацији и услугама од поверења (eIDAS) и на Директиву ЕУ 2018/1972 о кодексу електронских комуникација.

Директивом се:

- утврђује обавеза за све државе чланице да усвоје националну стратегију о безбедности мрежних и информационих система, да именују националне надлежне органе (компетентне ауторитете), органе надлежне за управљање сајбер кризама, јединствене тачке контакта и ЦСИРТ-ове;
- утврђују обавезе по питањима мера за управљање ризиком и извештавање за ентитете одређене као есенцијалне или важне у складу са овом Директивом, као и за ентитете идентификоване као критичне у складу са Директивом ЕУ 2022/2557 (CER Директива);
- утврђују правила и обавезе у вези дељења информација; и
- утврђују обавезе држава чланица ЕУ по питањима примене ове Директиве и надзора над применом.

Предлогом Закона о информационој безбедности (у даљем тексту: Предлог закона):

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

Директива НИС 2 је применљива на ентитете који се сматрају предузећима најмање средње величине и који своје делатности обављају унутар Европске Уније у секторима који су одређени као високо критични или критични. Поред тога, ова Директива примењује се и на ентитете, без обзира на њихову величину, који су идентификовани као критични у складу са Директивом 2022/2557 или који пружају услуге регистрације имена домена, као и на све друге ентитете из високо критичних или критичних сектора, без обзира на њихову величину:

- који пружају услуге јавних електронских комуникационих мрежа, услуге од поверења, услуге регистрације домена највишег нивоа или услуге ДНС;
- који су једини пружаоци неке есенцијалне услуге у држави чланици;
- чији би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље;
- чији би прекид у пружању услуга могао имати значајан системски ризик;

- који су критични због специфичне важности на националном или регионалном нивоу;
- који спадају у државне органе на централном нивоу, или спадају у државне органе на регионалном нивоу ако би прекид пружања њихових услуга имао значајан утицај на критичне друштвене или економске активности.

Ова Директива не примењује се на државне органе надлежне за националну безбедност, јавну безбедност, одбрану и спровођење закона. Директивом су дефинисане две категорије ентитета: есенцијални и важни.

Есенцијалним ентитетима сматрају се:

- ентитети који превазилазе величину средњих предузећа (имају више од 250 запослених и обрт од преко 50 милиона евра) и који своју делатност обављају у неком од високо критичних сектора;
- пружаоци квалификованих услуга од поверења, пружаоци услуге регистрације домена највишег нивоа и пружаоци услуга ДНС без обзира на величину;
- пружаоци услуга јавних електронских комуникационих мрежа или јавно доступних електронских комуникационих услуга који спадају у предузећа средње величине;
- органи државне управе на централном нивоу;
- сви други ентитети који своје делатности обављају у високо критичним или критичним секторима, а које је држава чланица идентификовала као есенцијалне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу;
- ентитети идентификовани као критични у складу са Директивом 2022/2557;
- сви други ентитети идентификовани као есенцијални у складу са Директивом 2016/1148 (НИС Директива), ако држава чланица процени да је то потребно.

Важним ентитетима сматрају се ентитети који своје делатности обављају у високо критичним или критичним секторима, а који не испуњавају критеријуме да буду идентификовани као есенцијални. Такође, важним ентитетима се сматрају и они које је држава чланица идентификовала као важне јер су једини пружаоци неке есенцијалне услуге, јер би прекид у пружању услуга могао имати значајан утицај на јавну сигурност, јавну безбедност и јавно здравље, јер би прекид у пружању услуга могао имати значајан системски ризик, или који су критични због специфичне важности на националном или регионалном нивоу. У секторе високе критичности спадају:

- енергетика,
- саобраћај,
- банкарство,
- инфраструктуре финансијских тржишта,
- здравље,
- пијаћа вода,
- отпадне воде,
- дигитална инфраструктура,
- управљање ИКТ услугама,
- јавна администрација и
- свемир.

У остале критичне секторе спадају:

- поштанске и курирске услуге,
- управљање отпадом,
- производња и снабдевање хемикалијама,
- производња, обрада и дистрибуција хране,

- друге производне делатности (производња медицинских уређаја и *in vitro* дијагностичких медицинских средстава, рачунара, електронских и оптичких производа, електричне опреме, машина и уређаја, моторних возила, приколица и полуприколица и производња остале опреме за превоз),
- пружање дигиталних услуга и
- истраживање.

Предлогом закона дефинисани су оператори приоритетних ИКТ система од посебног значаја који су пандан есенцијалним ентитетима, и оператори важних ИКТ система од посебног значаја који су пандан важним ентитетима из НИС 2 Директиве. Чланом 5. Предлога закона прописано је да су оператори приоритетних ИКТ система од посебног значаја:

- *органи;*
- *субјекти који су одређени као оператори критичне инфраструктуре у складу са прописима којима се уређује критична инфраструктура;*
- *правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:*
  - *енергетика,*
  - *саобраћај,*
  - *банкарство и финансијска тржишта,*
  - *здравство,*
  - *вода за пиће,*
  - *отпадне воде,*
  - *дигитална инфраструктура,*
  - *управљање ИКТ услугама које се пружају операторима приоритетних ИКТ система од посебног значаја,*
  - *остале области (управљање нуклеарним објектима, пружање квалификованих услуга од поверења, пружање услуга ДНС-а, управљање регистром домена највишег нивоа са изузетком оператора коренских сервера имена, пружање услуга мреже за испоруку садржаја, обављање делатности електронских комуникација, тачка за размену интернет саобраћаја, области у којој у Републици Србији постоји само један пружалац услуге и која је неопходна за обављање критичних друштвених и привредних делатности).*

Чланом 6. Предлога закона прописано је да су оператори важних ИКТ система од посебног значаја:

- *научноистраживачке институције;*
- *правна и физичка лица у својству регистрованог субјекта и органи који не спадају у операторе приоритетних ИКТ система од посебног значаја према критеријумима за одређивање оператора;*
- *правна лица која су дефинисана као оператори ИКТ система од посебног значаја у складу са постојећим Законом о информационој безбедности;*
- *правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:*
  - *поштанске услуге;*
  - *управљање отпадом;*
  - *производња и снабдевање хемикалијама;*
  - *производња, прерада и дистрибуција хране;*
  - *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.*

Евиденцију приоритетних и важних ИКТ система од посебног значаја успоставља и води министарство надлежно за послове информационе безбедности.

НИС 2 Директива даје дефиниције 41 термина.

У Предлогу закона дато је објашњење 58 термина, од којих 34 (идентично или у истом смислу) постоје и у НИС 2 Директиви. Термини из Предлога закона који имају свој пандан у НИС 2 Директиви су:

- *информационо-комуникациони систем*
- *оператор ИКТ система*
- *информациона безбедност*
- *ризик*
- *рањивост*
- *избегнути инцидент*
- *претња*
- *озбиљна претња*
- *инцидент*
- *управљање инцидентом*
- *криза информационе безбедности*
- *орган*
- *услуга информационог друштва*
- *пружалац услуге информационог друштва*
- *мрежа за испоруку садржаја*
- *тачка за размену интернет саобраћаја*
- *систем назива домена (ДНС)*
- *пружалац услуге ДНС-а*
- *услуга од поверења*
- *пружалац услуге од поверења*
- *квалификована услуга од поверења*
- *пружалац квалификоване услуге од поверења*
- *услуге рачунарства у клауду*
- *услуга центра за управљање и чување података*
- *научноистраживачка организација*
- *јавна електронска комуникациона мрежа*
- *електронска комуникациона услуга*
- *пружалац управљаних услуга*
- *пружалац управљаних безбедносних услуга*
- *регистар назива домена највишег нивоа*
- *пружалац услуге регистрације назива домена*
- *ИКТ производ*
- *ИКТ услуга*

- *ИКТ процес*

Термини који су дефинисани у Предлогу закона, а нису у НИС 2 Директиви су:

- *тајност*
- *интегритет*
- *расположивост*
- *аутентичност*
- *поверљивост*
- *непорецивост*
- *управљање ризиком*
- *јединствени систем за пријем обавештења о инцидентима*
- *мере заштите ИКТ система*
- *тајни податак*
- *ИКТ систем за рад са тајним подацима*
- *служба безбедности*
- *самостални оператори ИКТ система*
- *ЦЕРТ*
- *компромитујуће електромагнетно зрачење (КЕМЗ)*
- *криптобезбедност*
- *криптозаштита*
- *криптографски производ*
- *криптоматеријали*
- *безбедносна зона*
- *информациона добра*
- *TLP (Traffic Light Protocol)*

Посебно је занимљиво дефинисање два централна термина ова два документа: информационе безбедности и сајбер безбедности. У Предлогу закона термин „информациона безбедност" има дефиницију идентичну дефиницији термина „безбедност мрежних и информационих система (security of network and information systems)" у НИС 2 Директиви, али у Предлогу (нити у било којем другом правном документу у Србији) не постоји дефиниција сајбер безбедности, а такође ни у НИС 2 Директиви не постоји дефиниција информационе безбедности. Мада није експлицитно дефинисан ни у НИС 2 Директиви (ни у претходној НИС Директиви) ни у Акту о сајбер безбедности, под термином „информациона безбедност" у Европској Унији се подразумева очување поверљивости, интегритета и расположивости, у складу са дефиницијом из прегледа сајбер безбедности и сродних термина који је објавила ЕНИСА[6] и дефиницијом из стандарда ИСО 27000[7].

Дефиниција термина „сајбер безбедност" је у НИС 2 Директиви референцирана на дефиницију из Акта о сајбер безбедности (Уредба ЕУ 2019/881), према којој „сајбер безбедност означава активности неопходне за заштиту мрежних и информационих система, корисника тих система и других особа на које утичу сајбер претње". Ова дефиниција може у одређеној мери да се упореди са дефиницијом термина „мере заштите ИКТ система" из Предлог закона, према којој су то „техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система". Ипак, за ове две дефиниције не може се тврдити да имају

[6] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

исти смисао, па су зато у претходном набрајању сврстане у групе термина чије дефиниције немају свој пандан у другом акту.

НИС 2 Директива налаже државама чланицама да усвоје националну стратегију информациону безбедности и даје оквир тема које требају бити обухваћене стратегијом.

Предлогом закона нису прописане одредбе у вези стратегије, али је Закон препознат у Стратегији развоја информационог друштва и информационе безбедности за период 2021-2026. године.

НИС 2 Директивом је прописано да државе чланице морају одредити један или више надлежних органа (са надлежностима у одређеним секторима којима припадају оператори есенцијалних сервиса), као и јединствену тачку контакта за комуникацију са надлежним органима других земаља чланица и учешће у Групи за сарадњу. Ако је националним законодавством дефинисан само један надлежни орган, онда је тај орган истовремено и јединствена тачка контакта.

Чланом 26. Предлога закона прописано је да надлежни орган буде министарство надлежно за послове информационе безбедности. У оквиру својих надлежности ово министарство:

- *припрема и предлаже прописе и планска докумената;*
- *води евиденцију оператора ИКТ система од посебног значаја;*
- *врши надзор над радом Канцеларије за информациону безбедност;*
- *врши инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја;*
- *остварује међународну сарадњу у оквиру својих надлежности.*

Ипак, ово министарство није одређено за јединствену тачку контакта, већ је чланом 34. Предлого закона прописано да јединствена тачка контакта буде Канцеларија за информациону безбедност.

Свака држава чланица треба да одреди или успостави један или више надлежних органа одговорних за управљање великим инцидентима и кризама. Ако се одреди више органа, мора се недвосмислено одредити која институција координира њихов рад у случају великих инцидената и криза. Државе чланице такође морају усвојити национални план за одговор на велике инциденте и кризе који мора садржати:

- циљеве због којих се предузимају мере и активности,
- задатке и одговорности надлежних органа,
- процедуре за реаговање и њихово уклапање у општи оквир за реаговање у случају националне кризе, као и канале за размену информација,
- мере које је потребно предузети ради припреме, укључујући вежбе и обуке,
- организације из јавног и приватног сектора и инфраструктуру која се ангажује,
- процедуре и споразуме између националних надлежних органа.

Инциденти у ИКТ системима од посебног значаја класификовани су у Члану 16. Предлог закона у четири категорије: низак, средњи, висок и веома висок. Канцеларија за информациону безбедност управља одговором на инциденте ниског, средњег и високог нивоа у сарадњи са операторима ИКТ система од посебног значаја, министарством надлежним за послове информационе безбедности, Телом за координацију послова информационе безбедности и другим надлежним органима по потреби. Инциденти веома високог нивоа сматрају се кризом информационе безбедности и у том случају руковођење и координацију спровођења мера и задатака предузима Влада, која на предлог министарства надлежног за послове информационе безбедности, а по прибављеном мишљењу Канцеларије за информациону безбедност,

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

Предлого закона предвиђена је израда План за реаговање у случају инцидента високог нивоа и криза информационе безбедности.

НИС 2 Директивом је одређено да свака земља чланица мора успоставити један или више ЦСИРТ-ова који морају покривати све секторе којима припадају оператори есенцијалних сервиса и сервисе које пружају оператори дигиталних сервиса и бити одговорни за поступање са инцидентима.

Чланом 28. Предлога закона прописано је успостављање Канцеларије за информациону безбедност као посебне организације у смислу закона којим се уређује положај државне управе и ради обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији. Члан 30. прописисује надлежности Канцеларије за информациону безбедност:

1) врши превенцију и заштиту од безбедносних ризика на националном нивоу у складу са овим законом (послови Националног ЦЕРТ-а);

2) предузима превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе у складу са овим законом (послови ЦЕРТ-а органа власти);

3) обавља сарадњу на националном нивоу у области информационе безбедности;

4) врши послове јединствене тачке контакта;

5) врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности;

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 невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности;

8) обавља сарадњу и размену информација на међународном нивоу у области информационе безбедности у циљу праћења и усаглашавања са међународним прописима и стандардима;

9) врши стручни надзор над радом оператора ИКТ система од посебног значаја;

10) води базу рањивости ИКТ производа и ИКТ услуга;

11) извештава Министарство на кварталном нивоу о предузетим активностима;

12) обавља друге послове у складу са овим законом.

Канцеларија за информациону безбедност успоставља се и послове из своје надлежности прописане овим законом почиње да обавља 1. јануара 2027. године.

Послове Канцеларије за информациону безбедност прописане овим законом обављаће Канцеларија за информационе технологије и електронску управу у периоду који почиње даном наступања 12 месеци од дана ступања на снагу овог закона и који траје до 1. јануара 2027. године.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 12 месеци од дана ступања на снагу овог закона..

Надзор над радом Канцеларије за информациону безбедност врши министарство надлежно за информациону безбедност.

Предлог закона, као и постојећи Закон о информационој безбедности, препознаје самосталне операторе ИКТ система (министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове, службе безбедности и Народна банка Србије) који покривају своје ИКТ системе и на које се не примењују одредбе о пријављивању инцидената који значајно угрожавају информациону безбедност и одредбе о достављању статистичких података о инцидентима. Самостални оператор ИКТ система има обавезу да:

1) поднесе пријаву за упис 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 у складу са сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима;

6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима. Предлогом закона су препознати и Посебни ЦЕРТ-ови за превенцију ризика у ИКТ системима који обављају послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

НИС 2 Директивом је прописано да ЦСИРТ -ови морају испуњавати следеће захтеве:

- морају обезбедити висок ниво доступности својих комуникационих сервиса избегавањем јединствене тачке прекида и имати увек на располагању више начина да буду контактирани и да они контактирају друге;
- запослени и информациони системи које користе морају бити смештени на безбедним локацијама;
- морају бити опремљени одговарајућим системима за управљање и прослеђивање захтева;

- морају обезбедити поверљивост и поузданост својих операција;
- морају бити попуњени адекватним бројем и квалитетом запослених;
- морају имати осигуран континуитет рада инфраструктуре, укључујући редундантни простор и опрему.

Послови ЦСИРТ-ова морају обухватити:

- праћење и анализирање сајбер претњи, рањивости и инцидената на националном нивоу и, на захтев, пружање помоћи есенцијалним и важним ентитетима,
- пружање раних упозорења и других информација о ризицима и инцидентима есенцијалним и важним ентитетима, надлежним органима и другим субјектима од значаја,
- реаговање на инциденте и пружање помоћи есенцијалним и важним ентитетима (где је применљиво),
- пружање динамичке анализе ризика и инцидената и указивање на тренутну ситуацију,
- пружање есенцијалним и важним ентитетима услуге проактивног скенирања мрежних и информационих система ради откривања рањивости,
- учешће у Мрежи ЦСИРТ-ова,
- координацију активности усмерених на координисано откривање рањивости (где је применљиво), и
- допринос примени безбедних алата за размену информација.

Такође, прописано је да ЦСИРТ-ови промовишу усвајање и употребу уобичајених или стандардизованих пракси, класификационих шема и таксономија у вези са:

- процедурама за решавање инцидената,
- управљањем кризама и
- координисаним откривањем рањивости.

Чланом 31. Предлога закона прописано је да Канцеларија за информациону безбедност у оквиру послова Националног ЦЕРТ-а има следећи делокруг рада:

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 претњама, рањивостима 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) припрема извештаје на кварталном нивоу о предузетим активностима;

13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима.

Поред тога, Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за:

- *управљање инцидентима,*
- *класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената,*
- *управљање кризним ситуацијама и*
- *координисано откривање рањивости.*

Чланом 32. Предлога закона прописано је да Канцеларија за информациону безбедност обавља следеће послове у оквиру послова ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе:

- *врши заштиту мреже еУправе,*
- *обавља координацију и сарадњу са операторима ИКТ система које повезује мрежа еУправе у превенцији инцидената,*
- *активно учествује у откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената,*
- *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,*
- *у случају откривене рањивости:*
    - *обавести операторе ИКТ система који су корисници мреже еУправе о томе,*
    - *налаже операторима ИКТ система од посебног значаја који су корисници мреже да предузму адекватне мере заштите у циљу спречавања, смањења и отклањања последица индицента,*

- *издаје стручне препоруке за заштиту ИКТ система органа, осим ИКТ система за рад са тајним подацима,*
- *доноси акт којим се уређује поступање оператора ИКТ система од посебног значаја који користе мреже у случају инцидента,*
- *у сарадњи са надлежним органима врши процену потребе за стручним усавршавањем запослених у операторима ИКТ система од посебног значаја који користе мрежу,*
- *планира и организује процедуралне и практичне вежбе у области информационе безбедности за запослене у операторима ИКТ система од посебног значаја који користе мрежу,*
- *израђује предлоге за унапређење безбедносних карактеристика мреже еУправе,*
- *израђује анализе ризика и инцидената у оквиру мреже еУправе,*
- *обавља друге послове у складу са законом у циљу унапређења информационе безбедности мреже еУправе.*

Одредбе о координисаном откривању рањивости су уведене у НИС 2 Директиву као нова тема (која није постојала у НИС Директиви). НИС 2 Директивом прописано је да државе чланице треба да одреде ЦСИРТ који ће бити координатор ових активности. Тај ЦСИРТ треба да делује као посредник од поверења и олакша комуникацију између оног ко пријављује рањивост (било да је у питању правно или физичко лице) и произвођача потенцијално рањивог производа или пружаоца потенцијално рањиве услуге. Задаци овог ЦСИРТ-а укључују:

- идентификацију и успостављање контакта са предметним странама,
- помоћ страни која пријављује рањивост и
- договарање о роковима за објављивање, као и управљање рањивостима које утичу на више ентитета.

Страни која пријављује рањивост мора бити загарантована анонимност ако то жели.

НИС 2 Директива даје задатак ЕНИСА-и да развије и одржава Европску базу рањивости, укључујући одговарајући информациони систем, политике и процедуре, као и да предузме неопходне техничке и организационе мере које ће гарантовати безбедност и интегритет ове базе података. База података ће бити доступна свим значајним ентитетима, а садржаће следеће податке:

- опис рањивости,
- обухваћене производе или услуге и озбиљност рањивости у смислу околности под којима она може бити експлоатисана и
- доступност одговарајуће закрпе или упутство за умањење ризика ако закрпа не постоји.

Чланом 36. Предлога закона прописано је орган, односно организација надлежна за послове Националног 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:

- *податке о рањивости и*
- *податке о ИКТ производима или ИКТ услугама на које рањивост утиче.*

Орган, односно организација из става 1. овог члана прописује садржај, процедуре верификације рањивости, процедуре за управљање техничким рањивостима ИКТ производа и ИКТ услуга, начин уписа и вођења регистра.

НИС 2 Директивом је прописано да надлежни орган, јединствена тачка контакта и ЦСИРТ-ови једне државе чланице међусобно сарађују у циљу испуњавања обавеза које су им постављене овом Директивом. Ово се посебно односи на размену информација о инцидентима, избегнутим инцидентима и претњама. Такође, прописана је размена информација између надлежних органа успостављених овом Директивом и Директивом 2022/2557.

Предлог закона прописује сарадњу Канцеларије са, министарством надлежним за информациону безбедност, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система.

Један од облика сарадње на националном нивоу прописан Предлогом закона је кроз активности Тела за координацију послова информационе безбедности, које је координационо тело Владе и 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 за информационе технологије и електронску управу, 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.

Есенцијални и важни ентитети морају спроводити одговарајуће и пропорционалне техничке, оперативне и организационе мере за управљање ризицима по мрежне и информационе системе које користе за пружање својих услуга. Ове мере морају обухватити најмање:

- политике у вези анализе ризика и безбедности информационих система;
- руковање инцидентима;
- континуитет пословања и управљање кризама;
- безбедност ланца снабдевања;
- безбедност у набавци, развоју и одржавању мрежних и информационих система, укључујући руковање и откривање рањивостима;
- политике и процедуре за процену ефикасности мера за управљање ризиком;
- практиковање основних мера сајбер хигијене и обуке у циљу подизања безбедносне свести;
- политике и процедуре везане за коришћење криптографских метода;
- безбедност људских ресурса, политике контроле приступа и управљање асетима;
- коришћење мултифакторске аутентификације и других метода јаке аутентификације и коришћење безбедних комуникационих система, посебно у случају ванредних ситуација.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о процени ризика за ИКТ системе којима управља, којим се врши 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. Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система, којим се 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.

Овим мерама се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената, а оне се односе на:

- *успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;*
- *прикупљање података о претњама по информациону безбедност ИКТ система;*
- *постизање безбедности рада на даљину и употребе мобилних уређаја;*
- *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, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедности ради обезбеђивања континуиране едукације;*
- *обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу;*
- *заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;*
- *идентификовање информационих добара и одређивање одговорности за њихову заштиту;*
- *класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;*
- *заштиту носача података;*
- *ограничење приступа подацима и средствима за обраду података;*
- *одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;*
- *утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;*
- *предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података;*
- *примена мера заштите ради спречавања отицања података;*
- *физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;*
- *заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;*
- *обезбеђивање исправног и безбедног функционисања средстава за обраду података;*
- *примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду;*
- *праћење ИКТ система у циљу откривања рањивости и претњи*
- *ограничење приступа интернет страницама које могу потенцијално да наруше безбедност ИКТ система;*
- *заштиту података и средства за обраду података од злонамерног софтвера;*
- *заштиту од губитка података редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за размену података;*
- *чување података о догађајима који могу бити од значаја за безбедност ИКТ система;*
- *обезбеђивање интегритета софтвера и оперативних система;*
- *заштиту од злоупотребе техничких безбедносних слабости ИКТ система;*
- *обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања;*
- *заштиту података у комуникационим мрежама укључујући уређаје и водове;*

- *безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;*
- *испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;*
- *заштиту података који се користе за потребе тестирања ИКТ система односно делова система;*
- *процедуре за чување и брисање информација у ИКТ системима, у складу са прописима;*
- *заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;*
- *одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;*
- *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;*
- *мере које обезбеђују континуитет обављања посла у ванредним околностима које су дефинишу Планом континуитета обављања посла;*
- *усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите;*
- *употребу мултифакторске аутентикације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система.*

НИС 2 Директива одређује да оператори есенцијалних и важних сервиса, без непотребног одлагања, обавесте надлежни орган или ЦСИРТ о инцидентима који имају или могу имати значајан утицај на континуитет сервиса који пружају, са довољно информација да се може одредити да ли постоји и прекогранични утицај. Параметри који одређују да је инцидент значајан су:

- инцидент је проузроковао или има капацитет да проузрокује озбиљне прекиде пружања услуга или озбиљне финансијске губитке угроженом ентитету, и
- инцидент је утицао или има капацитет да утиче на друга физичка или правна лица путем наношења значајне материјалне или нематеријалне штете.

Предлогом закона прописано је да оператори ИКТ система од посебног значаја имају обавезу да путем јединственог система за пријем обавештења о инцидентима пријаве инциденте који могу да имају значајан утицај на нарушавање информационе безбедности (односно Народној банци Србије, Комисији за хартије од вредности или Регулаторном телу за електронске комуникације и поштанске услуге ако су у питању оператори ИКТ система који спадају у њихову надлежност).

Чланом 13. Предлога закона прописани су критеријуми за одређивање инцидената који могу да имају значајан утицај на нарушавање информационе безбедности:

- *који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;*
- *који утичу на велики број корисника услуга, или трају дужи временски период;*
- *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;*
- *који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;*

- *који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;*
- *који су настали као последица инцидента у приоритетном ИКТ систему од посебног значаја, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге приоритетног ИКТ система од посебног значаја који припрада области дигиталне инфраструктуре;*
- *инциденте који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима.*

Државе чланице могу захтевати од есенцијалних и важних ентитета да користе одређене ИКТ производе, услуге и процесе који су сертификовани према европским шемама сертификације за информациону безбедност усвојеним у складу са Актом о сајбер безбедности (Уредба ЕУ 2019/881).

Чланом 30. Предлога закона прописано је да Канцеларија за информациону безбедност, између осталог, обавља послове стандардизације и сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга. У Нацрту закона, осим навођења у овом члану, нема ближих одредница везаних за ову надлежност.

Са друге стране, у Предлогу закона задржано је читаво поглавље из постојећег Закона о информационој безбедности са осам чланова који детаљно обрађују криптобезбедност и заштиту од компромитујућег електромагнетног зрачења. Предлогом закона, као и постојећим Законом о информационој безбедности, прописано је да је за ове послове надлежно министарство надлежно за послове одбране.

НИС 2 Директива прописује да државе чланице обезбеде надзор над спровођењем и предузму неопходне мере за обезбеђење усклађености са овом Директивом.

Предлогом закона предвиђено је да 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) врши инспекција за информациону безбедност. Послове инспекције за информациону безбедност обавља министарство надлежно за информациону безбедност преко инспектора за информациону безбедност.

Овлашћења у вези надзора над спровођењем ове Директиве у системима есенцијалних ентитета су:

- инспекције на лицу места и надзор ван локације, укључујући насумичне провере које спроводе обучени стручњаци;
- редовне и циљане безбедносне ревизије које спроводи независно тело или надлежни орган;
- ванредне ревизије, укључујући оне које се спроводе због значајног инцидента или кршења ове Директиве;
- безбедносна скенирања заснована на критеријумима за процену ризика, у сарадњи са предметним субјектом;
- захтеви за информацијама неопходним за процену мера за управљање ризиком;
- захтеви за приступ подацима, документима и информацијама неопходним за обављање надзорних задатака;
- захтеви за доказима о примени политика информационе безбедности.

Државе чланице ће обезбедити да њихови надлежни органи према есенцијалним ентитетима имају овлашћење најмање да:

- издају упозорења о кршењу ове Директиве;
- усвоје обавезујућа упутства, укључујући она у вези са мерама неопходним за спречавање или отклањање инцидента, као и временске рокове за спровођење тих мера и извештавање о њиховој примени;
- наређе предметним субјектима да престану са кршењем одредби ове Директиве;
- наређе предметним субјектима да обезбеде да су њихове мере за управљање ризиком информационе безбедности и извештавања у складу са овом Директивом;
- наложе предметним субјектима да физичким или правним лицима којима пружају услуге пруже обавештења о актуелној претњи, природи претње, као и о свим могућим мерама које могу предузети та физичка или правна лица као одговор на ту претњу;
- наложе предметним субјектима да у разумном року спроведу препоруке дате као резултат ревизије безбедности;
- Одреде службеника за праћење усклађености предметних субјеката са наложеним мерама за управљање ризиком и извештавање;
- наређе предметним субјектима да на одређен начин објаве аспекте кршења ове Директиве;
- наметну или затраже изрицање административне казне.

Овлашћења у вези надзора над спровођењем ове Директиве у системима важних ентитета су:

- инспекције на лицу места и надзор ван локације које спроводе обучени стручњаци;
- циљане безбедносне ревизије које спроводи независно тело или надлежни орган;
- безбедносна скенирања заснована на критеријумима за процену ризика, у сарадњи са предметним субјектом;
- захтеви за информацијама неопходним за процену мера за управљање ризиком;
- захтеви за приступ подацима, документима и информацијама неопходним за обављање надзорних задатака;
- захтеви за доказима о примени политика информационе безбедности.

Државе чланице ће обезбедити да њихови надлежни органи према важним ентитетима имају овлашћење најмање да:

- издају упозорења о кршењу ове Директиве;
- усвоје обавезујућа упутства или налог за отклањање уочених недостатака;
- наређе предметним субјектима да престану са кршењем одредби ове Директиве;
- наређе предметним субјектима да обезбеде да су њихове мере за управљање ризиком информационе безбедности и извештавања у складу са овом Директивом;
- наложе предметним субјектима да физичким или правним лицима којима пружају услуге пруже обавештења о актуелној претњи, природи претње, као и о свим могућим мерама које могу предузети та физичка или правна лица као одговор на ту претњу;
- наложе предметним субјектима да у разумном року спроведу препоруке дате као резултат ревизије безбедности;
- наређе предметним субјектима да на одређен начин објаве аспекте кршења ове Директиве;
- наметну или затраже изрицање административне казне.

Предлогом закона прописано је да инспектор за информациону безбедност има овлашћења да:

- *наложи отклањање утврђених неправилности и за то утврди разуман рок;*

- *забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок;*
- *захтева од оператора ИКТ система од посебног значаја да изврши скенирање мреже у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;*
- *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;*
- *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.*

Измене Закона неопходне су и због доношења Уредбе 881/2019 Парламента и Савета ЕУ о Агенцији Европске Уније за сајбер безбедност (ЕНИСА) (енг. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 - Cybersecurity Act*) која је усвојена 17. априла 2019. године. Уредбом су проширене надлежности ЕНИСА. Ова Уредба значајна је за сертификацију у области информационе безбедности коју је потребно предвидети изменама Закона.

Шема сајбербезбедносне сертификације ЕУ представља свеобухватан сет правила, техничких захтева, стандарда и процедура који је успостављен на нивоу ЕУ и који се односи на сертификацију или процену усаглашености одређених ИКТ производа, сервиса и процеса. Шема националне сајбербезбедносне сертификације односи се на свеобухватан сет правила, техничких захтева, стандарда и процедура развијених и усвојених од стране националних ауторитета и који се односе на сертификацију или процену усаглашености ИКТ производа, сервиса и процеса који спадају у оквир те шеме. Европски сајбербезбедносни сертификат је документ издат од стране релевантне организације којим се потврђује да је одређени ИКТ производ, сервис или процес проверен на испуњавање специфичних безбедносних захтева постављених у шеми сајбербезбедносне сертификације ЕУ.

ИКТ производ представља елемент или групу елемената мрежног или информационог система. ИКТ сервис означава сервис који се у потпуности или углавном односи на пренос, складиштење, преузимање или обраду информација у мрежном или информационом систему. ИКТ процес представља сет активности које се обављају у сврху дизајна, развоја, испоруке или одржавања ИКТ производа или ИКТ сервиса.

Разлог за успостављање оквира за сајбербезбедносну сертификацију је побољшање услова за функционисање интерног тржишта кроз повећање нивоа информационе безбедности и успостављање јединственог приступа сајбербезбедносној сертификацији на нивоу ЕУ. ЕНИСА је Уредбом добила обавезу да до 28. јуна 2020. године објави програм рада по питањима сајбербезбедносне сертификације. Комисија може од ЕНИСА тражити да на основу тог програма направи шему сајбербезбедносне сертификације за кандидата или да преуреди постојећу шему сајбербезбедносне сертификације ЕУ.

Шема треба да обезбеди испуњење следећих циљева:

- Заштиту складиштених, преношених или на други начин обрађиваних података од случајног или намерног складиштења, обраде, приступа или објављивања током целог животног циклуса ИКТ производа, сервиса или процеса;
- Заштиту складиштених, преношених или на други начин обрађиваних података од случајног или намерног уништења, губљења, измене или недоступности током целог животног циклуса ИКТ производа, сервиса или процеса;
- Приступ подацима, сервисима или функцијама само од стране ауторизованих особа, програма или машина и само у мери у којој им је приступ одобрен;

- Идентификацију и документацију познатих зависности и рањивости;
- Бележење свих приступа, коришћења и обраде података, сервиса или функција са свим потребним информацијама;
- Омогућавање провере белешки о приступима, коришћењу и обради података, сервиса или функција;
- Верификацију да ИКТ производи, сервиси и процеси не садрже познате рањивости;
- Благовремено враћање доступности и приступа подацима, сервисима и функцијама у случају физичког или техничког инцидента;
- Безбедност ИКТ производа, сервиса и процеса по дефиницији и по дизајну; и
- Испорука ИКТ производа, сервиса и процеса са ажурним хардвером и софтвером без јавно познатих рањивости и са механизмима за безбедносно ажурирање.

Сразмерно ризику придруженом намени и сврси коришћења и у складу са вероватноћом и утицајем могућег сајбер инцидента, ИКТ производима, сервисима и процесима може се доделити ниво уверења „основни”, „знатан” или „висок”. „Основни” ниво даје уверење да ИКТ производ, сервис или процес испуњава одговарајуће безбедносне захтеве у погледу минимизације основних ризика од сајбер инцидената и напада, а провера испуњености ових захтева мора укључивати најмање преглед техничке документације. Ниво „знатан” даје уверење да ИКТ производ, сервис или процес, поред критеријума за ниво „основни”, испуњава одговарајуће безбедносне захтеве у погледу минимизације познатих ризика од сајбер инцидената и напада и ризике од сајбер инцидената и напада спроведених од стране актера са ограниченим вештинама и ресурсима, а провера испуњености ових захтева мора укључивати најмање проверу да не постоје јавно познате рањивости и проверу да су неопходне безбедносне функционалности коректно имплементиране. Ниво „висок” даје уверење да ИКТ производ, сервис или процес испуњава одговарајуће безбедносне захтеве у погледу минимизације ризика од најсавременијих сајбер напада спроведених од стране актера са значајним вештинама и ресурсима, а провера испуњености ових захтева мора укључивати најмање проверу да не постоје јавно познате рањивости, проверу да су неопходне и најсавременије безбедносне функционалности коректно имплементиране и примену пенетрационих тестирања ради процене отпорности на нападе од стране актера са значајним вештинама.

За ниво уверења „основни”, произвођачима је дозвољено да врше самопроцену усаглашености и да самостално издају уверење, при чему сносе потпуну одговорност за сагласност са захтевима.

Свака земља чланица ЕУ у обавези је да одреди један или више националних ауторитета за сајбербезбедносну сертификацију и да о томе обавести Комисију (ако их је више, сваки треба да има своју засебну надлежност). На нивоу ЕУ формираће се Група за европску сајбербезбедносну сертификацију (ECCG) састављена од представника националних ауторитета за сајбербезбедносну сертификацију или других националних ауторитета која ће, између осталог, имати следеће задатке:

- Да саветује и пружи помоћ Комисији у осигурању доследне имплементације програма сајбербезбедносне сертификације;
- Да пружи помоћ, саветује и сарађује са ЕНИСА у припреми шема сертификације;
- Да олакша сарадњу између националних ауторитета за сајбербезбедносну сертификацију кроз изградњу капацитета и размену информација;
- Да олакша прилагођење шема сајбербезбедносне сертификације ЕУ међународно препознатим стандардима итд.

Националне шеме информационе безбедносне сертификације које не спадају у оквир шеме сајбербезбедносне сертификације ЕУ могу да наставе са издавањем сертификата и након ступања на снагу шеме сајбербезбедносне сертификације ЕУ, док оне националне шеме које спадају под овај оквир не смеју више издавати сертификате.

Предлогом Закона у члану 30. су послови сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга поверени новооснованој Канцеларији за информациону безбедност.

5) На које циљне групе ће утицати предложена промена? Утврдити и представити циљне групе на које ће промена имати непосредан односно посредан утицај.

Нови Закон о информационој безбедности имаће непосредан утицај на:

- ИКТ системе од посебног значаја;
- Национални ЦЕРТ;
- ЦЕРТ органа власти - Јединствене информационо-комуникационе мреже електронске управе;
- нове ИКТ системе од посебног значаја;
- ЦЕРТ-ове самосталних оператора ИКТ система.

6) Због чега је неопходно постићи жељену промену на нивоу друштва? (одговором на ово питање дефинише се општи циљ).

Измене националног оквира треба да буду усмерене ка постизању развијеног информационог друштва и електронске управе у служби грађана и привреде, као и унапређену информациону безбедност грађана, јавне управе и привреде, што се постиже:

- побољшањем постојећих и изградњом недостајућих капацитета,
- успостављањем оквира за правовремену и ефикасну размену информација на свим нивоима, а посебно између надлежног органа за информациону безбедност и органа безбедности и одбране,
- координисаном и усклађеном међународном сарадњом,
- усаглашеним моделом образовања и дефинисањем профила људских ресурса у области информационе безбедности,
- ефикасном превентивном и реактивном заштитом критичне информационо-комуникационе инфраструктуре,
- подстицањем истраживачких и развојних капацитета и реализацијом заједничких пројеката јавног, приватног и академског сектора,
- побољшањем информационе безбедности ИКТ система који не спадају у критичну инфраструктуру и становништва у целини,
- успостављањем оквира за безбедносну сертификацију,
- усклађивањем са најбољим праксама, а нарочито са легислативом Европске уније.

Нови Закон о информационој безбедности треба да се донесе првенствено ради потпуног усклађивања са ЕУ регулативом у овој области, а потом ради боље повезаности свих релевантних актера у области информационе безбедности, чиме се доприноси адекватнијем нивоу безбедности информационих система од посебног значаја у Републици Србији, као и подизању информационе безбедности друштва у целини.

Када је реч о ефектима на грађане, треба истаћи да се применом закона очекује следеће:

- већа поузданост услуга које грађани користе путем информационо-комуникационих система од посебног значаја;
- заштита података грађана који се обрађују у ИКТ системима од посебног значаја;
- стварање механизама за подизање свести грађана о значају информационе безбедности;

- успостављање канала путем којих ће грађани моћи да комуницирају са органима у случају проблема и штете који су настали услед нарушавања информационе безбедности;
- обавештавање корисника у случају инцидената који значајно угрожавају ИКТ системе од посебног значаја чије услуге користе и добијање инструкција које мере треба да предузму ради превенције и санирања потенцијалне штете.

7) Шта се предметном променом жели постићи? (одговором на ово питање дефинишу се посебни циљеви, чије постизање треба да доводе до остварења општег циља. У односу на посебне циљеве, формулишу се мере за њихово постизање).

Новим законом успоставља се нова посебна организација Канцеларија за информациону безбедност, што ће допринети бољој координацији између Министарства и Канцеларије (у којој се обједињавају послови Националног ЦЕРТ-а и ЦЕРТ-а органа власти) са једне стране, али и побољшању сарадње са посебним ЦЕРТ-овима и ИКТ системима од посебног значаја са друге стране.

Такође се предвиђа јачање капацитета Националног ЦЕРТ-а и то технолошких, људских и организационих капацитета, што ће Националном ЦЕРТ-у омогућити прелазак са информативне и саветодавне улоге на оперативнију улогу. Пружајући адекватнију помоћ ИКТ системима од посебног значаја у случају пријављених инцидената, поспешиће се међусобна сарадња и створити поверење што ће последично довести до тога да ИКТ системи од посебног значаја пријављују инциденте у складу са Законом.

Прецизнијим регулисањем појмова (дефиниција) стварају се бољи услови за препознавање и разумевање сајбер претњи.

Давањем већег значаја ЦЕРТ-овима и редефинисањем обавеза оператора информационо-комуникационих система од посебног значаја олакшава се њихово деловање и пружа адекватнији одговор на инциденте.

Израда националног плана деловања у случају великих инцидената утицаће на брже и ефикасније реаговање на сајбер претње.

Унапређење институционалног оквира и побољшање механизама реаговања на инциденте у сајбер простору омогућиће остваривање циљева, и то:

- безбедност информационо-комуникационих система која се односи на ризике нарушавања функционисања органа управе, привреде и организација као последица инцидената у информационо-комуникационим системима и
- информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система.

8) Да ли су општи и посебни циљеви усклађени са важећим документима јавних политика и постојећим правним оквиром, а пре свега са приоритетним циљевима Владе?

Предлог закона у потпуности је усклађен са Стратегијом развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године. Општим циљем Стратегије ***Развијено информационо друштво и електронска управа у служби грађана и привреде и унапређена информациона безбедност грађана, јавне управе и привреде*** препознат је значај информационе безбедности за друштво у целини. Посебан циљ ***Унапређење информационе безбедности грађана, јавне управе и привреде*** остварује се кроз реализацију следећих мера:

- подизање свести и знања у области информационе безбедности грађана, јавних службеника и привреде,
- подизање капацитета ИКТ система од посебног значаја за примену мера заштите,
- подизање капацитета Националног ЦЕРТ-а, ЦЕРТ-а органа власти и ЦЕРТ-ова самосталних оператора ИКТ,
- подизање капацитета инспекције за информациону безбедност,
- подстицање јавно-приватног партнерства у области информационе безбедности и
- унапређење регионалне и међународне сарадње.

У оквиру мере *Унапређење сарадње и подизање капацитета ИКТ система од посебног значаја за примену мера заштите* предвиђена је посебна активност **Усклађивање прописа са регулативом ЕУ у области информационе безбедности**, што и јесте кључни разлог доношења новог Закона о информационој безбедности. Праћењем европских токова у овој области не врши се само хармонизација прописа, већ и унапређење институционалног оквира и побољшање механизама реаговања на инциденте у сајбер простору, као и превентивног деловања ради очувања информационе безбедности.

9) На основу којих показатеља учинка ће бити могуће утврдити да ли је дошло до остваривања општих односно посебних циљева?

Основни показатељи учинка доношења Закона огледају се у следећем:

- утврђени су начини и механизми за подизање капацитета ИКТ система од посебног значаја
- унапређена је платформа за размену информација између Националног ЦЕРТа и ИКТ система од посебног значаја са механизмом за брзо реаговање
- побољшана је сарадња између ЦЕРТ-ова у Републици Србији и координисан је одговор на кризне ситуације
- број успостављених ЦЕРТ-ова самосталних оператора се повећава
- број обучених запослених у ЦЕРТ-у органа власти и у самосталним операторима ИКТ се повећава
- број запослених инспектора за информациону безбедност се повећава
- боље је управљање ризиком.

Показатељ	Базна година и вредност	2024	2025	2026
Број организованих сајбер вежби	2023 (1)	2	3	4
Додат број нових функционалности платформи за размену података о инцидентима	2023 (0)	1	2	3
Број састанака ЦЕРТ-ова годишње	2023 (3)	4	5	6
Број полазника обука	2022 (20)	30	40	50
Број запослених инспектора	2023 (2)	3	4	5

Број адекватно сачињених аката о процени ризика	2023 (0)	1 00	200	300	

Усвајање НИС 2 Директиве у децембру 2022. године је био је подстицај да се направи анализа садашњег правног и институционалног оквира, поставе нови циљеви. *Предлогом* закона остварује се напредак у односу на постојеће стање, како у домену прецизнијег уређивања области, тако и у креирању функционалнијег и ефикаснијег институционалног оквира.

Један од задатака које је Европска унија поставила пред ЕНИСА је и израда оквира за сертификацију производа, сервиса и услуга, који има за циљ да се одреди ниво заштите који могу да пруже одређени производи, сервиси и услуге и да се ојача поверење у дигиталне технологије и провајдере дигиталних сервиса. *Предлогом* закона уводи се обавеза сертификације ИКТ система која ће се вршити када и европске земље ближе регулишу ово питање.

Без обзира што је позиција Србије у међународних оквирима све боља у овом домену, постоје значајне могућности за побољшање. Међународну сарадњу су остваривали представници Министарства информисања и телекомуникација, РАТЕЛ-а, Министарства спољних послова, Министарства унутрашњих послова и Министарства одбране, што ће се вероватно наставити и у наредном периоду. Важно је да наступи представника Србије у међународним институцијама буду координисани како би могли на најбољи начин да обављају своје послове.

Правовремено откривање и отклањање рањивости је стални изазов на којем заједнички ради више земаља како би се пронашао адекватан начин решавања. Благовременим откривањем претњи јача се степен информационе безбедности као и поверење у институције које се том темом баве.

Предлог закона уређује оквир за поступање у кризним ситуацијама и заједнички одговор ЦЕРТ-ова.

Поред промоције и подршке учешћу представника институција и организација из Србије на међународним вежбама, ради успостављања одговарајућег одговора на инциденте већих размера неопходна је организација националних сајбер вежби. Ове вежбе треба да организује и спроводи новооснована Канцеларија за информациону безбедност, а сврха вежби треба да буде провера и увежбавање процедура за реаговање.

Због тога је неопходно развијати партнерске односе са академским институцијама које имају програме за информациону безбедност на основном, мастер и докторском нивоу студија. Канцеларија треба да подстиче научне радове из ових области и учешће академских институција у међународним пројектима јер се на тај начин стичу нова знања и наши академски људски ресурси стимулишу да буду укључени у најновија достигнућа у овој области.

Увођењем механизма сарадње између ЦЕРТ-ова у Републици Србији доприноси се већем степену заштите ИКТ система у свим областима у Републици Србији и бољој координацији у случају инцидената који могу да угрозе информациону безбедност, али и националну безбедност Републике Србије.

10) Да ли је финансијске ресурсе за спровођење изабране опције потребно обезбедити у буџету, или из других извора финансирања и којих?

Средства потребна за реализацију обавеза из Закона о информационој безбедности потребно је обезбедити у буџету, за потребе подизања капацитета новоосноване Канцеларије за информациону безбедност. С обзиром да Канцеларија за информациону безбедност преузима права, обавезе, запослене, предмете, опрему, средства за рад Канцеларије за информационе технологије и електронску управу у делокругу послова ЦЕРТ-а органа власти, као и 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, потребно је извршити одговарајући пренос финансијских средстава.

11) Колики су процењени трошкови увођења промена који проистичу из спровођења изабране опције (оснивање нових институција, реструктурирање постојећих институција и обука државних службеника) исказани у категоријама капиталних трошкова, текућих трошкова и зарада и да ли је могуће финансирати расходе изабране опције кроз редистрибуцију постојећих средстава?

Будући да је *Предлог* закона предвиђено формирање посебне организације и повећавање кадровских и техничких капацитета у наредном периоду предвиђа се повећавање броја запослених као и куповина неопходне опреме.

12) Које трошкове и користи (материјалне и нематеријалне) ће изабрана опција проузроковати привреди, појединој грани, односно одређеној категорији привредних субјеката?

ИКТ системи од посебног значаја у области дигиталне инфраструктуре и услуга информационог друштва који су предвиђени изменама и допунама Закона су у обавези да примене мере заштите, односно техничке и организационе мере у циљу успостављања адекватног нивоа безбедности система.

Уколико су ти привредни субјекти већ успоставили систем управљања информационом безбедношћу у складу са међународним стандардима и добром праксом у овој области, не очекује се да примена закона изазове значајне трошкове. Међутим, привредни субјекти који представљају операторе ИКТ система од посебног значаја у складу са новим законом, а који до сада нису успоставили одговарајући систем управљања информационом безбедношћу имаће одређене трошкове за испуњење законских обавеза који се огледају у евентуалном додатном технолошком опремању, обуци запослених, ангажовању нових стручњака и слично. Прецизни износи додатних трошкова за наведене субјекте варирају у великом распону, будући да исти зависе од више фактора који могу да буду веома различити у различитим привредним субјектима. Наиме, колико ће финансијских средстава за примену закона издвојити ови привредни субјекти зависи од њихове величине, односно броја запослених, технолошке опремљености (поседовање рачунарске опреме, информационог система), обучености запослених за коришћење информационих технологија у домену информационе безбедности, и других фактора од којих функционисање информационе безбедности зависи у једном привредном субјекту. Сходно наведеном, није могуће дати ни тачне, ни оквирне износе по привредном субјекту.

13) Да ли је за спровођење изабране опције обезбеђена подршка свих кључних заинтересованих страна и циљних група? Да ли је спровођење изабране опције приоритет за доносиоце одлука у наредном периоду (Народну скупштину, Владу, државне органе и слично)?

Министарство информисања и телекомуникација је почетком 2023. године формирало радну групу за израду Нацрта Закона о информационој безбедности кога су чинили

представници релевантних министарстава, посебних организација, агенција, академске заједнице и привреде. Током припреме Нацрта одржано је неколико консултација са различитим интересним групама. Са привредом су одржане консултације 22. јуна у Националној алијанси за локални економски развој на којима су представљени предлози текста Нацрта. Састанку је присуствовало близу 20 привредних субјеката.

Министарство информисања и телекомуникација спровело је јавну расправу о Нацрту Закона о информационој безбедности у периоду од 27.јула до 30. августа 2023. године, на основу закључка Владе. У оквиру јавне расправе, одржана су два округла стола у Београду и Крагујевцу. У јавној расправи учествовали представници државних органа, привредног сектора, академске заједнице, невладиних организација и еминентни стручњаци у овој области.

Иако је текст закона незнатно измењен у односу на 2023. годину, у 2024. години из процедуралних разлога поновљена је јавна расправа и то у периоду од 3. јула до 23. јула 2024. године, на основу које је Министарство објавило извештај о јавној расправи на сајту Министарства и порталу „еКонсултације“.

Доношење закона је приоритет имајући у виду чињеницу да се истим врши усклађивање са европском регулативом.

14) Које додатне мере треба спровести и колико времена ће бити потребно да се спроведе изабрана опција и обезбеди њено касније доследно спровођење, односно њена одрживост?

Ради реализације закона, предвиђено је доношење следећих подзаконских аката:

- Уредба којом се ближе уређују услови, општи и секторски критеријуми за одређивање оператора приоритетних и важних ИКТ система од посебног значаја;
- Подзаконски акт којим се ближе уређује садржај и структура евиденције, као и начин подношења захтева за унос и промену података у Евиденцији;
- Подзаконски акт којим се уређују ближи услове за прикупљање, чување, верификацију и објављивање тачних и потпуних података о регистрацији домена у посебној бази података;
- Подзаконски акт којим се ближе уређују услови за проверу КЕМЗ и начин процене ризика од отицања података путем КЕМЗ;
- Подзаконски акт којим се ближе уређују услови које морају да испуњавају криптографски производи;
- 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 вођења регистра издатих одобрења за криптографски производ;
- Подзаконски акт којим се ближе уређује вођење регистара криптографских производа, криптоматеријала, правила и прописа и лица која обављају послове криптозаштите;
- Уредбе о ближем садржају акта о безбедности ИКТ од посебног значаја, начину провере и садржај извештаја о провери, као и достављање извештаја надлежном органу;
- Уредбе о ближем уређењу мера заштите ИКТ система од посебног значаја;
- Уредба о поступку обавештавања о инцидентима, обрасцима за обавештавање, листи инцидената према врстама и класификацији инцидената према нивоу опасности;
- Уредбе о начину спровођења мера за безбедност и заштиту деце на интернету;

- Правилника о општој методологији за процену ризика у ИКТ системима од посебног значаја;
- Правилника о врсти, форми и начину достављања статистичких података о инцидентима у информационо-комуникационим системима од посебног значаја;
- Правилника о садржају, начину уписа и вођењу евиденције посебних центара за превенцију безбедносних ризика у информационо-комуникационим системима;
- Правилника о садржају, процедури верификације рањивости, , процедуре за управљање техничким рањивостима ИКТ производа и ИКТ услуга, начин уписа и вођења регистра.

Ради упознавања јавности са новим законским решењима, Министарство информисања и телекомуникација одржаваће посебне скупове на којима ће упознавати сва заинтересована лица о усвојеним одредбама. Посебан фокус ће бити на операторе ИКТ система од посебног значаја, којима се овим законом прописују обавезе у циљу заштите њихових система. Очекује се да ће се ове активности почети да спроводе одмах по доношењу закона, односно подзаконских акта које овај закон предвиђа, и да ће трајати најмање годину дана, а по потреби и дуже.

Међуинституционална сарадња између органа који спроводе овај закон успоставиће се на више начина:

- Кроз рад Владиног Тела за координацију послова информационе безбедности, које окупља све органе чији су послови од великог значаја за информациону безбедност у Републици Србији;
- У поступку обавештавања о инцидентима који значајно угрожавају информациону безбедност у Републици Србији, надлежни органи остварују сарадњу по питању размене информација, посебно ако је реч о инцидентима који представљају кривично дело или угрожавају одбрану и националну безбедност Републике Србије, односно критичну инфраструктуру.

Закон предвиђа и међусобну сарадњу ЦЕРТ-ова (Националног ЦЕРТ-а, ЦЕРТ-а Јединствене информационо-комуникационе мреже електронске управе, Посебних ЦЕРТ-ова и других ЦЕРТ-ова).

15) Да ли су обезбеђена финансијска средства за спровођење изабране опције? Да ли је за спровођење изабране опције обезбеђено довољно времена за спровођење поступка јавне набавке уколико је она потребна?

Средства за реализацију законских обавеза обезбеђују се у буџету Републике Србије кроз буџет Канцеларије за информациону безбедност, као посебне организације која ће обављати послове Националног ЦЕРТ-а и ЦЕРТ-а органа власти. Канцеларија за информациону безбедност успоставља се и послове из своје надлежности прописане овим законом почиње да обавља 1. јануара 2027. године. Послове Канцеларије за информациону безбедност прописане овим законом обављаће Канцеларија за информационе технологије и електронску управу у периоду који почиње даном наступања 12 месеци од дана ступања на снагу овог закона и који траје до 1. јануара 2027. године. Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до истека периода од 12 месеци од дана ступања на снагу овог закона. Канцеларија за информационе технологије и електронску управу 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 12 месеци од дана ступања на снагу овог закона, потребне за вршење стручних послова утврђених овим законом. Канцеларија за информациону безбедност почев од датума претходно наведеног преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Канцеларије за информационе технологије и електронску управу насталу у обављању послова прописаних овим законом из надлежности Канцеларије за информациону безбедност.

ИЗЈАВА О УСКЛАЂЕНОСТИ ПРОПИСА СА ПРОПИСИМА ЕВРОПСКЕ УНИЈЕ

1. Овлашћени предлагач прописа: Влада

Обрађивач: Министарство информисања и телекомуникација

2. Назив прописа:

Предлог закона о информационој безбедности

Draft Law on Information Security

3. Усклађеност прописа с одредбама Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране („Службени гласник РС”, број 83/08) (у даљем тексту: Споразум):

а) Одредба Споразума која се односе на нормативну садржину прописа:

Члан 105. Информационо друштво - Споразум о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране.

б) Прелазни рок за усклађивање законодавства према одредбама Споразума:

Три године.

в) Оцена испуњености обавезе које произлазе из наведене одредбе Споразума:

Испуњава у потпуности.

г) Разлози за делимично испуњавање, односно неиспуњавање обавеза које произлазе из наведене одредбе Споразума:

/

д) Веза са Националним програмом за усвајање правних тековина Европске уније:

2024-0

4. Усклађеност прописа са прописима Европске уније:

а) Навођење одредби примарних извора права Европске уније и оцене усклађености са њима:

Consolidated version of the Treaty on the Functioning of the European Union

PART THREE UNION POLICIES AND INTERNAL ACTIONS

TITLE VII COMMON RULES ON COMPETITION, TAXATION AND APPROXIMATION OF LAWS, CHAPTER 3 APPROXIMATION OF LAWS

Article 114 (ex Article 95 TEC)

CELEX 12016E114

Потпуно усклађено

б) Навођење секундарних извора права Европске уније и оцене усклађености са њима:

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)- **потпуно усклађено**

32022L2555

Директива (ЕУ) 2022/2055 Европског парламента и Савета од дана 14. децембра 2022. године о мерама за висок заједнички ниво сајбер безбедности, измени Уредбе (ЕУ) бр. 910/2014 и Директиве (ЕУ) бр. 2018/1972 и стављању ван снаге Директиве (ЕУ) 2016/1148

в) Навођење осталих извора права Европске уније и усклађеност са њима:

Нема.

г) Разлози за делимичну усклађеност, односно неусклађеност:

д) Рок у којем је предвиђено постизање потпуне усклађености прописа са прописима Европске уније:

5. Уколико не постоје одговарајуће надлежности Европске уније у материји коју регулише пропис, и/или не постоје одговарајући секундарни извори права Европске уније са којима је потребно обезбедити усклађеност, потребно је образложити ту чињеницу. У овом случају, није потребно попуњавати Табелу усклађености прописа. Табелу усклађености није потребно попуњавати и уколико се домаћим прописом не врши пренос одредби секундарног извора права Европске уније већ се искључиво врши примена или спровођење неког захтева који произилази из одредбе секундарног извора права (нпр. Предлогом одлуке о изради стратешке процене утицаја биће спроведена обавеза из члана 4. Директиве 2001/42/ЕЗ, али се не врши и пренос те одредбе директиве).

6. Да ли су претходно наведени извори права Европске уније преведени на српски језик?
Не.

7. Да ли је пропис преведен на неки службени језик Европске уније?

Преведен је на енглески језик.

8. Сарадња са Европском унијом и учешће консултаната у изради прописа и њихово мишљење о усклађености:

Предлог закона је прослеђен Европској комисији ради давања мишљења. Европска комисија је у децембру 2024. године доставила своје коментаре и сугестије који су инкорпорирани у текст Предлога закона.

1. Назив прописа Европске уније : **Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)** **Директива (ЕУ) 2022/2055 Европског парламента и Савета од дана 14. децембра 2022. године о мерама за висок заједнички ниво сајбер безбедности, измени Уредбе (ЕУ) бр. 910/2014 и Директиве (ЕУ) бр. 2018/1972 и стављању ван снаге Директиве (ЕУ) 2016/1148**	2. „CELEX" ознака ЕУ прописа 32022L2555
3. Овлашћени предлагач прописа: Влада	4. Датум израде табеле:
Министарство информисања и телекомуникација	10. фебруар 2025.
5. Назив (нацрта, предлога) прописа чије одредбе су предмет анализе усклађености са прописом Европске уније: **1. Предлог закона о информационој безбедности** **2. Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању** **3. Закон о инспекцијском надзору** **4. Закон о прекршајима** **5. Закон о заштити података о личности**	6. Бројчане ознаке (шифре) планираних прописа из базе НПАА: 2024-0
7. Усклађеност одредби прописа са одредбама прописа ЕУ: ПОТПУНО УСКЛАЂЕНО	

а)	а1)	б)	б1)	в)	г)	д)

Одредба прописа ЕУ	Садржина одредбе	Одредбе прописа Р. Србије	Садржина одредбе	Усклађеност[1]	Разлози за делимичну усклађеност, неусклађеност или непреносивост	Напомена о усклађености
1. 1.	***Subject matter***	1.1.	Предмет уређивања Члан 1.	ПУ		

[1] Потпуно усклађено - ПУ, делимично усклађено - ДУ, неусклађено - НУ, непреносиво – НП

	This Directive lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market.		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.			
1.2.	To that end, this Directive lays down: (a) obligations that require Member States to adopt national cybersecurity strategies and to designate or establish competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs); (b) cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities under Directive (EU) 2022/2557; (c) rules and obligations on cybersecurity information sharing; (d) supervisory and enforcement obligations on Member States.	1. 1.	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.	ПУ		
2.1.	***Scope*** This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union. Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this Directive.	1.5. 1.6.	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:	ПУ		Разликовање оператора по величини биће утврђено подзаконским актом из члана 6. став 3.

			1) правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима: (1) Енергетика - производња електричне енергије, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - комбинована производња електричне и топлотне енергије; - снабдевање електричном енергијом; - пренос електричне енергије и управљање преносним системом; - дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом; - складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - 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 и производња нафте и природног гаса; - производња деривата нафте; - складиштење нафте и деривата нафте; - транспорт и управљање транспортним системом за природни гас; - складиштење и управљање складиштем природног гаса; - дистрибуција и управљање дистрибутивним системом за природни гас; - снабдевање и јавно снабдевање природним гасом; - производња и прерада угља; - 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; - сервис за управљање бродским саобраћајем (VTS); - речни информациони сервиси (RIS); - управљање путном инфраструктуром; - управљање интелигентним транспортним системима (ИТС). (3) Банкарство и финансијска тржишта - послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно 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 односно салдирања 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 фармацеутских лекова и препарата намењених за здравствену употребу; - производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја 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; - пружање услуга мреже за испоруку садржаја; - 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; - управљање амбалажним отпадом, у смислу закона којим се уређује управљање амбалажним отпадом; - производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије; - производња, прерада 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 послове информационе безбедности. Министарства у чијим надлежностима су области у којима оператори приоритетних и важних ИКТ система од посебног значаја обављају делатности, 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.			
2.2.	Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where: (a)services are provided by: (i)providers of public electronic communications networks or of publicly available electronic communications services; (ii)trust service providers; (iii)top-level domain name registries and domain name system service providers; (b)the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities; (c)disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; (d)disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;	1.5.	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, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - комбинована производња електричне и топлотне енергије; - снабдевање електричном енергијом; - пренос електричне енергије и управљање преносним системом;	ПУ		

	(e)the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State; (f)the entity is a public administration entity: (i)of central government as defined by a Member State in accordance with national law; or (ii)at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.		- дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом; - складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - 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 и производња нафте и природног гаса; - производња деривата нафте; - складиштење нафте и деривата нафте; - транспорт и управљање транспортним системом за природни гас; - складиштење и управљање складиштем природног гаса; - дистрибуција и управљање дистрибутивним системом за природни гас; - снабдевање и јавно снабдевање природним гасом; - производња и прерада угља; - 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; - сервис за управљање бродским саобраћајем (VTS);		

			- речни информациони сервиси (RIS); - управљање путном инфраструктуром; - управљање интелигентним транспортним системима (ИТС). (3) Банкарство и финансијска тржишта - послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно 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 односно салдирања 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 фармацеутских лекова и препарата намењених за здравствену употребу; - производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја 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; - пружање услуга мреже за испоруку садржаја; - 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.			
2.3.	Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.	1.5.2.3.	3) субјекти који су одређени као оператори критичне инфраструктуре у складу са прописима којима се уређује критична инфраструктура	ПУ		
2.4.	Regardless of their size, this Directive applies to entities providing domain name registration services.	1.5.2.1.9.	(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; - пружање услуга мреже за испоруку садржаја; - обављање делатности електронских комуникација; - тачка за размену интернет саобраћаја; - издавање Службеног гласника	ПУ		

			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.			
2.5.	Member States may provide for this Directive to apply to: (a)public administration entities at local level; (b)education institutions, in particular where they carry out critical research activities.	1.5.2.2. 1.6.2.2.	2) органи 2) научноистраживачке институције	ПУ		
2.6.	This Directive is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.	1.2.1.1.25. 1.8.	25) 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 Обавезе самосталних оператора Члан 8. Самостални оператор дужан је да: 1) поднесе пријаву за упис 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 у складу са сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима; 6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима. Самостални оператори могу да међусобно	ПУ		

			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, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ система од посебног значаја. Самостални оператори, у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе. 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.			
2.7.	This Directive does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.	1.2.1.1.25. 1.8.	25) 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 Обавезе самосталних оператора Члан 8. Самостални оператор дужан је да: 1) поднесе пријаву за упис 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 у складу са	ПУ		

			сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима; 6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима. 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, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ система од посебног значаја. Самостални оператори, у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе. 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.			
2.8.	Member States may exempt specific entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities referred to in paragraph 7 of this Article, from the obligations laid down in Article 21 or 23 with regard to those activities or services. In such cases, the supervisory and enforcement measures referred to in Chapter VII shall not apply in relation to those specific activities	1.8.	25) 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 Обавезе самосталних оператора Члан 8. Самостални оператор дужан је да: 1) поднесе пријаву за упис у евиденцију ИКТ	ПУ		

	or services. Where the entities carry out activities or provide services exclusively of the type referred to in this paragraph, Member States may decide also to exempt those entities from the obligations laid down in Articles 3 and 27.		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 у складу са сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима; 6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима. 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, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ система од посебног значаја. Самостални оператори, у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе. 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.			
2.9.	Paragraphs 7 and 8 shall not apply where an entity acts as a trust service provider.	2.37.	Државни орган као пружалац квалификованих услуга од поверења	ПУ	Другим законом (Законом о	

		2.64.	Члан 37. Државни орган може пружати квалификоване услуге од поверења уколико испуњава услове за пружање услуга предвиђене овим законом. Оцењивање испуњености услова државног органа за пружање услуге од поверења врши министарство, односно инспектор за електронску идентификацију и услуге од поверења, након поднетог захтева. Изузетно од става 2. овог члана оцењивање испуњености услова врши се на основу интерне контроле у сарадњи са надлежним министарством само у случају када је пружалац квалификоване услуге од поверења министарство надлежно за послове одбране, уз обавезу достављања извештаја о извршеној интерној контроли надлежном министарству. Након провере испуњености услова Влада уредбом утврђује да државни орган може да обавља квалификовану услугу од поверења која је била предмет оцењивања из става 2. овог члана. Министарство врши упис државног органа у регистар из члана 35. овог закона, на основу уредбе из става 4. овог члана. Послови инспекције за електронску идентификацију и услуге од поверења у електронском пословању Члан 64. Инспекција за електронску идентификацију и услуге од поверења у електронском пословању врши инспекцијски надзор над применом овог закона и радом пружалаца услуга електронске идентификације и пружалаца услуга од поверења (у даљем тексту: пружаоци услуга) преко инспектора за електронску идентификацију и услуге од поверења (у даљем тексту: инспектор). У оквиру инспекцијског надзора пружалаца услуга инспектор утврђује да ли су испуњени услови прописани овим законом и прописима донетим за спровођење овог закона.		електронском документу, електронској идентификацији и услугама од поверења) предвиђено је да се надзор може вршити над ентитетима из параграфа 7 и 8.	

2.10.	This Directive does not apply to entities which Member States have exempted from the scope of Regulation (EU) 2022/2554 in accordance with Article 2(4) of that Regulation.			НУ	Тачан опсег ових субјеката уредиће се подзаконским актом.	
2.11.	The obligations laid down in this Directive shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.	1.2.1.1.25. 1.8.	25) 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 Обавезе самосталних оператора Члан 8. Самостални оператор дужан је да: 1) поднесе пријаву за упис 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 у складу са сопственим правилима за проверу усклађености мера заштите, а 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 са трећим лицима; 6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима. 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, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ	ПУ		

			система од посебног значаја. Самостални оператори, у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе. 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.			
2.12.	This Directive applies without prejudice to Regulation (EU) 2016/679, Directive 2002/58/EC, Directives 2011/93/EU (27) and 2013/40/EU (28) of the European Parliament and of the Council and Directive (EU) 2022/2557.			НП		Однос са другим прописима ЕУ
2.13.	Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of entities concerned.			НП		Обавеза држава чланица у размени информација са Комисијом.
2.14.	Entities, the competent authorities, the single points of contact and the CSIRTs shall process personal data to the extent necessary for the purposes of this Directive and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof. The processing of personal data pursuant to this Directive by providers of public electronic communications networks or providers of publicly available electronic communications services shall be carried out in accordance with Union data	1.4.	Обрада података о личности Члан 4. На обраду података о личности која је неопходна за вршење надлежности и испуњење обавеза из овог закона примењују се одредбе овог закона, одредбе посебних закона којима се уређују одређене области, као и одредбе закона којим се уређује заштита података о личности.	ПУ		

	protection law and Union privacy law, in particular Directive 2002/58/EC.					
3.1.	***Essential and important entities*** For the purposes of this Directive, the following entities shall be considered to be essential entities: (a)entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC; (b)qualified trust service providers and top-level domain name registries as well as DNS service providers, regardless of their size; (c)providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC; (d)public administration entities referred to in Article 2(2), point (f)(i); (e)any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e); (f)entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive; (g)if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 or national law.	1.5. 1.6.	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, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - комбинована производња електричне и топлотне енергије; - снабдевање електричном енергијом; - пренос електричне енергије и управљање преносним системом; - дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом; - складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - 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	ПУ		

			облицима транспорта; - истраживање и производња нафте и природног гаса; - производња деривата нафте; - складиштење нафте и деривата нафте; - транспорт и управљање транспортним системом за природни гас; - складиштење и управљање складиштем природног гаса; - дистрибуција и управљање дистрибутивним системом за природни гас; - снабдевање и јавно снабдевање природним гасом; - производња и прерада угља; - 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; - сервис за управљање бродским саобраћајем (VTS); - речни информациони сервиси (RIS); - управљање путном инфраструктуром; - управљање интелигентним транспортним системима (ИТС). (3) Банкарство и финансијска тржишта - послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно 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 односно салдирања			

			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 фармацеутских лекова и препарата намењених за здравствену употребу; - производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја 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; - пружање услуга мреже за испоруку садржаја;			

			- 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; - управљање амбалажним отпадом, у смислу закона којим се уређује управљање амбалажним отпадом; - производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије; - производња, прерада 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 послове информационе безбедности. Министарства у чијим надлежностима су области у којима оператори приоритетних и важних ИКТ система од посебног значаја обављају делатности, 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.			
3.2.	For the purposes of this Directive, entities of a type referred to in Annex I or II which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be important entities. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).	1.6.2.3.	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.	ПУ		
3.3.	By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and			НП		Није потребна законска одредба да би се ово реализовало.

	at least every two years thereafter.					Може да се реализује применом постојећег законодавства.
3.4.	For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities: (a)the name of the entity; (b)the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers; (c)where applicable, the relevant sector and subsector referred to in Annex I or II; and (d)where applicable, a list of the Member States where they provide services falling within the scope of this Directive. The entities referred to in paragraph 3 shall notify any changes to the details submitted pursuant to the first subparagraph of this paragraph without delay, and, in any event, within two weeks of the date of the change. The Commission, with the assistance of the European Union Agency for Cybersecurity (ENISA), shall without undue delay provide guidelines and templates regarding the obligations laid down in this paragraph. Member States may establish national mechanisms for entities to register themselves.	1.9.	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 става 1. тач. 4), 5), 6) и 8) овог члана. Подзаконски акт којим се ближе уређује садржај	ПУ		

			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 ст. 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 законом којим се уређује заштита података о личности и чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 5. овог члана. Министарство ставља на располагање ажурну Евиденцију Канцеларији за информациону безбедност ради извршења одредби овог закона у погледу прикупљања и размене информација о претњама, рањивостима и инцидентима и пружања подршке, упозоравања и саветовања лица која управљају ИКТ системима. Евиденција представља тајни податак у смислу закона којим се уређује тајност података.			
3.5.	By 17 April 2025 and every two years thereafter, the competent authorities shall notify: (a)the Commission and the Cooperation Group of the number of essential and important entities listed pursuant to paragraph 3 for each sector and subsector referred to in Annex I or II; and (b)the Commission of relevant information about			НП	Обавеза Комисије и других тела ЕУ.	

	the number of essential and important entities identified pursuant to Article 2(2), points (b) to (e), the sector and subsector referred to in Annex I or II to which they belong, the type of service that they provide, and the provision, from among those laid down in Article 2(2), points (b) to (e), pursuant to which they were identified.					
3.6.	Until 17 April 2025 and upon request of the Commission, Member States may notify the Commission of the names of the essential and important entities referred to in paragraph 5, point (b).			НП	Обавеза Комисије и других тела ЕУ.	
4.1.	***Sector- specific Union legal acts*** Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.			НП	Остварљиво применом општих правних начела.	
4.2.	The requirements referred to in paragraph 1 of this Article shall be considered to be equivalent in effect to the obligations laid down in this Directive where: (a)cybersecurity risk-management measures are at least equivalent in effect to those laid down in Article 21(1) and (2); or (b)the sector-specific Union legal act provides for immediate access, where appropriate automatic and direct, to the incident notifications by the CSIRTs, the competent authorities or the single points of contact under this Directive and where requirements to notify significant incidents are at			НП	У вези је са претходним чланом.	

	least equivalent in effect to those laid down in Article 23(1) to (6) of this Directive.					
4.3.	3. The Commission shall, by 17 July 2023, provide guidelines clarifying the application of paragraphs 1 and 2. The Commission shall review those guidelines on a regular basis. When preparing those guidelines, the Commission shall take into account any observations of the Cooperation Group and ENISA.			НП	Обавеза Комисије.	
5.1.	***Minimum harmonisation*** This Directive shall not preclude Member States from adopting or maintaining provisions ensuring a higher level of cybersecurity, provided that such provisions are consistent with Member States' obligations laid down in Union law.			НП	Одредба о важењу прописа ЕУ.	
6 (1)	***Definitions*** For the purposes of this Directive, the following definitions apply: (1)'network and information system' means: (a)an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972; (b)any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or (c)digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	1.2.1.1.	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.	ПУ		
6 (2)	(2)'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and	1.2.1.3.	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	ПУ		

	information systems;		пружају или су доступне путем тог ИКТ система;			
6 (3)	(3)‘cybersecurity’ means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881;			НУ	Нисмо увели у законску терминологију израз сајбер безбедност. Крећемо се у оквиру термина информационе безбедности који подразумева и сајбер безбедност и безбедност информационих система и мрежа.	
6 (4)	(4)‘national cybersecurity strategy ’ means a coherent framework of a Member State providing strategic objectives and priorities in the area of cybersecurity and the governance to achieve them in that Member State;			ПУ	Применом прописа који уређују област усвајања планских докумената (међу којима су и стратегије) и других закона у ефекту смо у складу са овом одредбом. Није потребно да је додатно пропишемо и у секторском закону.	
6 (5)	(5)‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;	1.2.1.12.	12) избегнути инцидент представља идентификовани догађај у ИКТ систему који је могао довести до значајног угрожавања расположивости, аутентичности, интегритета или поверљивости података, услуга или система, али је правовременом интервенцијом или заштитним мерама спречено остваривање штетних последица;	ПУ		
6 (6)	(6)‘incident’ means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;	1.2.1.15.	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;	ПУ		
6 (7)	(7)‘large-scale cybersecurity incident’ means an incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States;			НП	Термин који се користи за инциденте који погађају државе чланице ЕУ.	
6 (8)	(8)‘incident handling’ means any actions and procedures aiming to prevent, detect, analyse, and	1.2.1.18.	18) управљање инцидентом подразумева предузимање свих радњи и поступака чији је	ПУ		

	contain or to respond to and recover from an incident;		циљ спречавање, откривање, анализа и прекид инцидента, као и предузимање других мера ради одговора на инцидент и отклањања његових последица;			
6 (9)	(9)‘risk’ means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;	1.2.1.9.	9) ризик представља могућност настанка догађаја или услова који могу угрозити ниво информационе безбедности или исправно функционисање ИКТ система, што се утврђује на основу процене вероватноће догађаја и величине његовог потенцијалног утицаја на ниво информационе безбедности;	ПУ		
6 (10)	(10)‘cyber threat’ means a cyber threat as defined in Article 2, point (8), of Regulation (EU) 2019/881;	1.2.1.13.	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 са јасном вероватноћом настајања штете у случају да изостане реакција;	ПУ		
6 (11)	(11)‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage;	1.2.1.14.	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;	ПУ		
6 (12)	(12)‘ICT product’ means an ICT product as defined in Article 2, point (12), of Regulation (EU) 2019/881;	1.2.1.53.	53) ИКТ производ је елемент или група елемената у оквиру информационо-комуникационог система;	ПУ		
6 (13)	(13)‘ICT service’ means an ICT service as defined in Article 2, point (13), of Regulation (EU) 2019/881;	1.2.1.54.	54) ИКТ услуга је услуга која се у потпуности или у већој мери састоји из преноса, чувања, преузимања или обраде података коришћењем ИКТ система;	ПУ		
6 (14)	(14)‘ICT process’ means an ICT process as defined in Article 2, point (14), of Regulation (EU) 2019/881;	1.2.1.55.	55) ИКТ процес је скуп активности који се обавља у циљу израде, развоја, коришћења и одржавања ИКТ производа или ИКТ услуге;	ПУ		
6 (15)	(15)‘vulnerability’ means a weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat;	1.2.1.10.	10) рањивост представља слабост или недостатак у ИКТ производима или услугама који се могу искористити за реализацију једне или више претњи;	ПУ		
6 (17)	(17)‘technical specification’ means a technical specification as defined in Article 2, point (4), of Regulation (EU) No 1025/2012;			ПУ		Област регулисања других општих прописа.

6 (18)	(18)‘internet exchange point’ means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;	1.2.1.37.	37) 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 аутономних система прође кроз трећи аутономни систем, те која такав саобраћај не мења и не утиче на њега на други начин;	ПУ		
6 (19)	(19)‘domain name system’ or ‘DNS’ means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;	1.2.1.38.	38) систем назива домена (ДНС) 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;	ПУ		
6 (20)	(20)‘DNS service provider’ means an entity that provides: (a)publicly available recursive domain name resolution services for internet end-users; or (b)authoritative domain name resolution services for third-party use, with the exception of root name servers;	1.2.1.39.	39) 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;	ПУ		
6 (21)	(21)‘top-level domain name registry’ or ‘TLD name registry’ means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;	1.2.1.51.	51) 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;	ПУ		
6 (22)	(22)‘entity providing domain name registration services’ means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;	1.2.1.52.	52) пружалац услуге регистрације назива домена је регистратор назива домена или други субјект који делује у име регистратора;	ПУ		

6 (23)	(23)‘digital service’ means a service as defined in Article 1(1), point (b), of Directive (EU) 2015/1535 of the European Parliament and of the Council	1.2.1.37.	37) 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 аутономних система прође кроз трећи аутономни систем, те која такав саобраћај не мења и не утиче на њега на други начин;	ПУ		
6 (24)	(24)‘trust service’ means a trust service as defined in Article 3, point (16), of Regulation (EU) No 910/2014;	1.2.1.40.	40) услуга од поверења је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању	ПУ		
6 (25)	(25)‘trust service provider’ means a trust service provider as defined in Article 3, point (19), of Regulation (EU) No 910/2014;	1.2.1.41.	41) пружалац услуге од поверења је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању	ПУ		
6 (26)	(26)‘qualified trust service’ means a qualified trust service as defined in Article 3, point (17), of Regulation (EU) No 910/2014;	1.2.1.42.	42) квалификована услуга од поверења је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању	ПУ		
6 (27)	(27)‘qualified trust service provider’ means a qualified trust service provider as defined in Article 3, point (20), of Regulation (EU) No 910/2014;	1.2.1.43.	43) пружалац квалификоване услуге од поверења је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању	ПУ		
6 (28)	(28)‘online marketplace’ means an online marketplace as defined in Article 2, point (n), of Directive 2005/29/EC of the European Parliament and of the Council			НУ	Област је предмет уређивања других закона. За сада није дефинисан термин у правном систему РС.	
6 (29)	(29)‘online search engine’ means an online search engine as defined in Article 2, point (5), of Regulation (EU) 2019/1150 of the European Parliament and of the Council			НУ	Област је предмет уређивања других закона. За сада није дефинисан термин у правном систему РС.	
6 (30)	(30)‘cloud computing service’ means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several	1.2.1.44.	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,	ПУ		

	locations;		укључујући и ситуације када су такви ресурси распоређени на неколико локација;			
6 (31)	(31)‘data centre service’ means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control;	1.2.1.45.	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;	ПУ		
6 (32)	(32)‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers;	1.2.1.36.	36) мрежа за испоруку садржаја (Content Delivery Network – CDN) означава мрежу географски распоређених сервера која је осмишљена да обезбеди високу доступност, приступачност и брзу испоруку дигиталног садржаја и услуга корисницима интернета, у име пружалаца садржаја и услуга;	ПУ		
6 (33)	(33)‘social networking services platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;			НУ	Област је предмет уређивања других закона. За сада није дефинисан термин у правном систему РС.	
6 (34)	(34)‘representative’ means a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under this Directive;			НУ	Област је предмет уређивања других закона. За сада није дефинисан термин у правном систему РС.	
6 (35)	(35)‘public administration entity’ means an entity recognised as such in a Member State in accordance with national law, not including the judiciary, parliaments or central banks, which complies with the following criteria:	1.2.1.23.	орган је државни орган, орган аутономне покрајине, јединица локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења	ПУ		

	(a)it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; (b)it has legal personality or is entitled by law to act on behalf of another entity with legal personality; (c)it is financed, for the most part, by the State, regional authorities or by other bodies governed by public law, is subject to management supervision by those authorities or bodies, or has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities or by other bodies governed by public law; (d)it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital;					
6 (36)	(36)'public electronic communications network' means a public electronic communications network as defined in Article 2, point (8), of Directive (EU) 2018/1972;	1.2.1.47.	јавна електронска комуникациона мрежа је електронска комуникациона мрежа у смислу закона којим се уређују електронске комуникације;	ПУ		
6 (37)	(37)'electronic communications service' means an electronic communications service as defined in Article 2, point (4), of Directive (EU) 2018/1972;	1.2.1.48.	електронска комуникациона услуга је услуга у смислу закона којим се уређују електронске комуникације;	ПУ		
6 (38)	(38)'entity' means a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;	1.2.1.2.	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;	ПУ		
6 (39)	(39)'managed service provider' means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;	1.2.1.49.	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;	ПУ		
6 (40)	(40)'managed security service provider' means a managed service provider that carries out or provides assistance for activities relating to	1.2.1.50.	пружалац управљаних безбедносних услуга је пружалац управљаних услуга који спроводи или пружа помоћ у спровођењу активности у вези са	ПУ		

	cybersecurity risk management;		управљањем ризиком у области безбедности.			
6 (41)	(41)‘research organisation’ means an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions.	1.2.1.46.	научноистраживачка организација је организација у смислу закона којим се уређују наука и истраживање	ПУ		
7.1.	***National cybersecurity strategy*** Each Member State shall adopt a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include: (a)objectives and priorities of the Member State’s cybersecurity strategy covering in particular the sectors referred to in Annexes I and II; (b)a governance framework to achieve the objectives and priorities referred to in point (a) of this paragraph, including the policies referred to in paragraph 2; (c)a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs under this Directive, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts; (d)a mechanism to identify relevant assets and an assessment of the risks in that Member State; (e)an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors; (f)a list of the various authorities and stakeholders			ПУ	Применом општих прописа за израду планских докумената осигурана је правилна примена ове одредбе. Није потребно додатно прописивати секторским прописом.	

	involved in the implementation of the national cybersecurity strategy; (g)a policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities under Directive (EU) 2022/2557 for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate; (h)a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens.					
7.2.	As part of the national cybersecurity strategy, Member States shall in particular adopt policies: (a)addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services; (b)on the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products; (c)managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under Article 12(1); (d)related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables; (e)promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures; (f)promoting and developing education and training on cybersecurity, cybersecurity skills, awareness			ПУ	Применом општих прописа за израду планских докумената осигурана је правилна примена ове одредбе. Није потребно додатно прописивати секторским прописом.	

	raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities; (g)supporting academic and research institutions to develop, enhance and promote the deployment of cybersecurity tools and secure network infrastructure; (h)including relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law; (i)strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs; (j)promoting active cyber protection.					
7.3.	Member States shall notify their national cybersecurity strategies to the Commission within three months of their adoption. Member States may exclude information which relates to their national security from such notifications.			НП	Обаваза држава чланица према Комисији.	
7.4.	Member States shall assess their national cybersecurity strategies on a regular basis and at least every five years on the basis of key performance indicators and, where necessary, update them. ENISA shall assist Member States, upon their request, in the development or the update of a national cybersecurity strategy and of key performance indicators for the assessment of that strategy, in order to align it with the requirements and obligations laid down in this Directive.			ПУ	Имплементација ове одредбе осигурана је применом општих прописа који уређују питања израде планских докумената у Републици Србији.	
8.1.	***Competent authorities and single points of contact*** Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred	1.26. 1.30.1.4.	Надлежни орган Члан 26. Орган државне управе надлежан за информациону безбедност је министарство надлежно за послове информационе	ПУ		

	to in Chapter VII (competent authorities).		безбедности. У оквиру својих надлежности Министарство: 1) припрема и предлаже прописе и планска документа из области информационе безбедности у складу са овим законом; 2) води евиденцију оператора ИКТ система од посебног значаја; 3) врши надзор над радом Канцеларије у вршењу послова за које је надлежна у складу са овим законом; 4) 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; 5) остварује међународну сарадњу у оквиру својих надлежности. Канцеларија у оквиру своје надлежности обавља следеће послове и то: 4) врши послове јединствене тачке контакта;			
8.2.	The competent authorities referred to in paragraph 1 shall monitor the implementation of this Directive at national level.	1.26. 1.27. 1.28. 1.29. 1.30.	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 документа 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 у вршењу послова за које је надлежна у складу са овим законом; 4) 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; 5) остварује међународну сарадњу у оквиру својих надлежности. Тело за координацију послова информационе безбедности	ПУ		

			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, послове правосуђа, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, 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, у складу са законом којим се		

			уређује положај државних службеника, а кога председнику Владе предлаже министар надлежан за послове информационе безбедности. Канцеларија има заменика директора, који мора бити лице одговарајуће стручности, који се поставља у складу са прописима којим се уређује положај државних службеника и има овлашћења у складу са прописима о државној управи. Надзор над радом Канцеларије Члан 29. Надзор над радом Канцеларије у вршењу послова спроводи Министарство, у складу са законом којим се уређује државна управа. Надлежности Канцеларије Члан 30. Канцеларија у оквиру своје надлежности обавља следеће послове и то: 1) врши превенцију и заштиту од безбедносних ризика на националном нивоу у складу са овим законом (послови Националног ЦЕРТ-а); 2) предузима превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе у складу са овим законом (послови ЦЕРТ-а органа власти); 3) обавља сарадњу на националном нивоу у области информационе безбедности; 4) врши послове јединствене тачке контакта; 5) врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима; 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 невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности; 8) обавља сарадњу и размену информација на међународном нивоу у области информационе безбедности у циљу праћења и усаглашавања са међународним прописима и стандардима; 9) врши стручни надзор над радом оператора ИКТ система од посебног значаја; 10) води базу рањивости ИКТ производа и ИКТ услуга; 11) извештава Министарство на кварталном нивоу о предузетим активностима; 12) обавља друге послове у складу са овим законом.			
8.3.	Each Member State shall designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to paragraph 1, that competent authority shall also be the single point of contact for that Member State.	1.34.	Међународна сарадња и послови јединствене тачке контакта Члан 34. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да	ПУ		

			обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
8.4.	Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State.	1.34.	Међународна сарадња и послови јединствене тачке контакта Члан 34. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду	ПУ		

			усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
8.5.	Member States shall ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive.			ПУ	Одредба се имплементира применом општих прописа и других нерегулаторних активности.	
8.6.	Each Member State shall notify the Commission without undue delay of the identity of the competent authority referred to in paragraph 1 and of the single point of contact referred to in paragraph 3, of the tasks of those authorities, and of any subsequent changes thereto. Each Member State shall make public the identity of its competent authority. The Commission shall make a list of the single points of contact publicly available.			НП	Обавеза државе чланице према Комисији.	
9.1.	***National cyber management frameworks*** Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.			НП	Односи се на инциденте који погађају државе чланице. Овим законом се успостављају надлежни органи који су формирани тако да ступањем Републике Србије у чланство ЕУ могу да преузму и имплементацију ове одредбе.	

9.2.	Where a Member State designates or establishes more than one cyber crisis management authority pursuant to paragraph 1, it shall clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises.	1.27.	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, послове правосуђа, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, 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.	ПУ		
9.3.	Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis for the purposes of this Directive.	1.13 1.14. 1.15.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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:	ПУ		

			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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби.			
9.4.	Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: (a)the objectives of national preparedness measures and activities;	1.13 1.14. 1.15.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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	ПУ		

	(b)the tasks and responsibilities of the cyber crisis management authorities; (c)the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels; (d)national preparedness measures, including exercises and training activities; (e)the relevant public and private stakeholders and infrastructure involved; (f)national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level.		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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби.			
9.5.	Within three months of the designation or establishment of the cyber crisis management authority referred to in paragraph 1, each Member State shall notify the Commission of the identity of its authority and of any subsequent changes thereto. Member States shall submit to the Commission and to the European cyber crisis liaison organisation network (EU-CyCLONe) relevant information relating to the requirements of paragraph 4 about			НП	Организована мрежа држава чланица ЕУ	

	their national large-scale cybersecurity incident and crisis response plans within three months of the adoption of those plans. Member States may exclude information where and to the extent that such exclusion is necessary for their national security.					
10.1.	***Computer security incident response teams (CSIRTs)*** Each Member State shall designate or establish one or more CSIRTs. The CSIRTs may be designated or established within a competent authority. The CSIRTs shall comply with the requirements set out in Article 11(1), shall cover at least the sectors, subsectors and types of entity referred to in Annexes I and II, and shall be responsible for incident handling in accordance with a well-defined process.	1.31.	Послови превенције и заштите од безбедносних ризика на националном нивоу (Национални ЦЕРТ) 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 претњама, рањивостима 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;	ПУ		

			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) припрема извештаје на кварталном нивоу о предузетим активностима; 13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за: 1) управљање инцидентима; 2) класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената; 3) управљање кризним ситуацијама; 4) координирано откривање рањивости. Канцеларија је овлашћена 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. Канцеларија обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације. У оквиру обављања послова Националног ЦЕРТ-а потребно је обезбедити следеће захтеве: 1) висок ниво доступности комуникационих канала избегавањем јединствених тачака прекида и коришћење више средстава за двосмерно контактирање;		

			2) просторије Националног ЦЕРТ-а и информациони системи за подршку треба да буду смештени на сигурним локацијама; 3) употребу одговарајућег система за управљање захтевима и њихово усмеравање, посебно како би се олакшала ефикасна и ефективна размена информација; 4) обезбеђивање поверљивости и поузданости својих активности; 5) постојање адекватних кадровских капацитета; 6) опремљеност редундантним системима и резервним радним простором како би се осигурао континуитет услуга.			
10.2.	Member States shall ensure that each CSIRT has adequate resources to carry out effectively its tasks as set out in Article 11(3).			ПУ	Имплементација се обезбеђује другим општим прописима, алокацијом ресурса, финансирањем и другим нерегулаторним мерама.	
10.3.	Member States shall ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders. To that end, Member States shall ensure that each CSIRT contributes to the deployment of secure information-sharing tools.			ПУ	Имплементација се обезбеђује другим општим прописима, алокацијом ресурса, финансирањем и другим нерегулаторним мерама.	
10.4.	The CSIRTs shall cooperate and, where appropriate, exchange relevant information in accordance with Article 29 with sectoral or cross-sectoral communities of essential and important entities.	1.33.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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	ПУ		

			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 Канцеларија је дужна 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.			
10.5.	The CSIRTs shall participate in peer reviews organised in accordance with Article 19.			НП	Прописано на начин да може да се реализује само међу чланицама ЕУ. Не постоје препреке да ЦЕРТ суделује у овоме према постојећем законодавству Републике Србије када се за то створе услови.	
10.6.	Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network.	1.33.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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.	ПУ		

10.7.	The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams. As part of such cooperation relationships, Member States shall facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams, using relevant information-sharing protocols, including the traffic light protocol. The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law.	1.33. 1.34.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система.	ПУ		

			Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
10.8.	The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies, in particular for the purpose of providing them with cybersecurity assistance.	1.34.	Међународна сарадња и послови јединствене тачке контакта Члан 34. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана	ПУ		

			подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
10.9.	Each Member State shall notify the Commission without undue delay of the identity of the CSIRT referred to in paragraph 1 of this Article and the CSIRT designated as coordinator pursuant to Article 12(1), of their respective tasks in relation to essential and important entities, and of any subsequent changes thereto.			НП	Обавеза држава чланица према Комисији.	
10.10.	Member States may request the assistance of ENISA in developing their CSIRTs.			НП	Право држава чланица у односу на ЕНИСА-у.	
11.1.	***Requirements, technical capabilities and tasks of CSIRTs*** The CSIRTs shall comply with the following requirements: (a)the CSIRTs shall ensure a high level of availability of their communication channels by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times; they shall clearly			ПУ	Спровођење одредбе осигурано применом општих прописа, алокацијом ресурса, финансирањем и другим нерегулаторним мерама.	

	specify the communication channels and make them known to constituency and cooperative partners; (b)the CSIRTs' premises and the supporting information systems shall be located at secure sites; (c)the CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular to facilitate effective and efficient handovers; (d)the CSIRTs shall ensure the confidentiality and trustworthiness of their operations; (e)the CSIRTs shall be adequately staffed to ensure availability of their services at all times and they shall ensure that their staff is trained appropriately; (f)the CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of their services. The CSIRTs may participate in international cooperation networks.					
11.2.	Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the tasks referred to in paragraph 3. Member States shall ensure that sufficient resources are allocated to their CSIRTs to ensure adequate staffing levels for the purpose of enabling the CSIRTs to develop their technical capabilities.			ПУ	Спровођење одредбе осигурано применом општих прописа, алокацијом ресурса, финансирањем и другим нерегулаторним мерама.	
11.3.	The CSIRTs shall have the following tasks: (a)monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems; (b)providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant	1.31.	Послови превенције и заштите од безбедносних ризика на националном нивоу (Национални ЦЕРТ) 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	ПУ		

	stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time; (c)responding to incidents and providing assistance to the essential and important entities concerned, where applicable; (d)collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity; (e)providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact; (f)participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request; (g)where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure under Article 12(1); (h)contributing to the deployment of secure information-sharing tools pursuant to Article 10(3). The CSIRTs may carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities. Such scanning shall be carried out to detect vulnerable or insecurely configured network and information systems and inform the entities concerned. Such scanning shall not have any negative impact on the functioning of the entities' services. When carrying out the tasks referred to in the first subparagraph, the CSIRTs may prioritise particular tasks on the basis of a risk-based approach.		Србији; 3) пружа рана упозорења, узбуне и најаве и информише релевантна лица о претњама, рањивостима 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) припрема извештаје на кварталном нивоу о предузетим активностима; 13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима			

			Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за: 1) управљање инцидентима; 2) класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената; 3) управљање кризним ситуацијама; 4) координирано откривање рањивости. Канцеларија је овлашћена 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. Канцеларија обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације. У оквиру обављања послова Националног ЦЕРТ-а потребно је обезбедити следеће захтеве: 1) висок ниво доступности комуникационих канала избегавањем јединствених тачака прекида и коришћење више средстава за двосмерно контактирање; 2) просторије Националног ЦЕРТ-а и информациони системи за подршку треба да буду смештени на сигурним локацијама; 3) употребу одговарајућег система за управљање захтевима и њихово усмеравање, посебно како би се олакшала ефикасна и ефективна размена информација; 4) обезбеђивање поверљивости и поузданости својих активности; 5) постојање адекватних кадровских капацитета; 6) опремљеност редундантним системима и резервним радним простором како би се осигурао континуитет услуга.			
11.4.	The CSIRTs shall establish cooperation relationships with relevant stakeholders in the private sector, with a view to achieving the objectives of this Directive.	1.33.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге,	ПУ		

			Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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.			
11.5.	In order to facilitate cooperation referred to in paragraph 4, the CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to: (a)incident-handling procedures; (b)crisis management; and (c)coordinated vulnerability disclosure under Article 12(1).	1.31.	Послови превенције и заштите од безбедносних ризика на националном нивоу (Национални ЦЕРТ) 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 претњама, рањивостима 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;	ПУ		

			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) припрема извештаје на кварталном нивоу о предузетим активностима; 13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за: 1) управљање инцидентима; 2) класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената; 3) управљање кризним ситуацијама; 4) координирано откривање рањивости. Канцеларија је овлашћена 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. Канцеларија обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације. У оквиру обављања послова Националног ЦЕРТ-а потребно је обезбедити следеће захтеве: 1) висок ниво доступности комуникационих канала избегавањем јединствених тачака прекида и коришћење више средстава за двосмерно контактирање; 2) просторије Националног ЦЕРТ-а и информациони системи за подршку треба да буду смештени на сигурним локацијама; 3) употребу одговарајућег система за управљање захтевима и њихово усмеравање, посебно како би се олакшала ефикасна и ефективна размена информација; 4) обезбеђивање поверљивости и поузданости својих активности; 5) постојање адекватних кадровских капацитета; 6) опремљеност редундантним системима и резервним радним простором како би се осигурао континуитет услуга. Превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе (ЦЕРТ органа власти)			
12.1.	***Coordinated vulnerability disclosure and a European vulnerability database*** Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party. The tasks of the CSIRT designated as coordinator	1.36.	База рањивости Члан 36. Орган, односно организација надлежна за послове Националног ЦЕРТ-а 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:	ПУ		

	shall include: (a)identifying and contacting the entities concerned; (b)assisting the natural or legal persons reporting a vulnerability; and (c)negotiating disclosure timelines and managing vulnerabilities that affect multiple entities. Member States shall ensure that natural or legal persons are able to report, anonymously where they so request, a vulnerability to the CSIRT designated as coordinator. The CSIRT designated as coordinator shall ensure that diligent follow-up action is carried out with regard to the reported vulnerability and shall ensure the anonymity of the natural or legal person reporting the vulnerability. Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.		1) податке о рањивости; 2) податке о рањивостима ИКТ производа или ИКТ услуга. Орган, односно организација из става 1. овог члана прописује садржај, процедуре верификације рањивости, процедуре за управљање техничким рањивостима ИКТ производа и ИКТ услуга, начин уписа и вођења регистра.			
12.2.	ENISA shall develop and maintain, after consulting the Cooperation Group, a European vulnerability database. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures, and shall adopt the necessary technical and organisational measures to ensure the security and integrity of the European vulnerability database, with a view in particular to enabling entities, regardless of whether they fall within the scope of this Directive, and their suppliers of network and information systems, to disclose and register, on a voluntary basis, publicly known vulnerabilities in ICT products or ICT services. All stakeholders shall be provided access to the information about the vulnerabilities contained in the European vulnerability database. That database shall include: (a)information describing the vulnerability;			НП	Обавезе ЕНИСА	

	(b)the affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited; (c)the availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated.					
13.1.	***Cooperation at national level*** Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive.			ПУ	Имплементација је осигурана применом прописа који уређују сарадњу државних органа и међународну сарадњу.	
13.2.	Member States shall ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents pursuant to Article 23, and incidents, cyber threats and near misses pursuant to Article 30.	1.13 1.14. 1.15.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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 тешкоћа у вршењу послова и пружању услуга и имају утицај на	ПУ		

			већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од		

			посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби.			
13.3.	Member States shall ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted pursuant to this Directive.	1.13 1.14. 1.15.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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 тешкоћа у вршењу	ПУ		

			послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности.			

			Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби.			
13.4.	In order to ensure that the tasks and obligations of the competent authorities, the single points of contact and the CSIRTs are carried out effectively, Member States shall, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection authorities, the national authorities under Regulations (EC) No 300/2008 and (EU) 2018/1139, the supervisory bodies under Regulation (EU) No 910/2014, the competent authorities under Regulation (EU) 2022/2554, the national regulatory authorities under Directive (EU) 2018/1972, the competent authorities under Directive (EU) 2022/2557, as well as the competent authorities under other sector-specific Union legal acts, within that Member State.	1.33. 1.34.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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.	ПУ		

			Међународна сарадња и послови јединствене тачке контакта Члан 34. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			

13.5.	Member States shall ensure that their competent authorities under this Directive and their competent authorities under Directive (EU) 2022/2557 cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities under Directive (EU) 2022/2557, and the measures taken in response to such risks, threats and incidents. Member States shall also ensure that their competent authorities under this Directive and their competent authorities under Regulation (EU) No 910/2014, Regulation (EU) 2022/2554 and Directive (EU) 2018/1972 exchange relevant information on a regular basis, including with regard to relevant incidents and cyber threats.			ПУ	Имплементација осигурана применом прописа о сарадњи државних органа и међународној сарадњи.	
13.6.	Member States shall simplify the reporting through technical means for notifications referred to in Articles 23 and 30.	1.2.1.17.	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;	ПУ		
14.1.	***Cooperation Group*** In order to support and facilitate strategic cooperation and the exchange of information among Member States, as well as to strengthen trust and confidence, a Cooperation Group is established.	1.27.	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, послове правосуђа, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Народне банке Србије и Регулаторног	ПУ		

			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.			
14.2.	The Cooperation Group shall carry out its tasks on the basis of biennial work programmes referred to in paragraph 7.			ПУ	Осигурано применом одредби које уређују начин рада и надлежности Владиних тела.	
14.3.	The Cooperation Group shall be composed of representatives of Member States, the Commission and ENISA. The European External Action Service shall participate in the activities of the Cooperation Group as an observer. The European Supervisory Authorities (ESAs) and the competent authorities under Regulation (EU) 2022/2554 may participate in the activities of the Cooperation Group in accordance with Article 47(1) of that Regulation. Where appropriate, the Cooperation Group may invite the European Parliament and representatives of relevant stakeholders to participate in its work. The Commission shall provide the secretariat.			НП	Односи се само на тела која се оснују на нивоу ЕУ.	
14.4.	The Cooperation Group shall have the following tasks: (a)to provide guidance to the competent authorities in relation to the transposition and implementation of this Directive; (b)to provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure, as referred to in Article 7(2), point (c); (c)to exchange best practices and information in			НП	Односи се само на тела која се оснују на нивоу ЕУ.	

	relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities pursuant to Article 2(2), points (b) to (e); (d)to exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements; (e)to exchange advice and cooperate with the Commission on draft delegated or implementing acts adopted pursuant to this Directive; (f)to exchange best practices and information with relevant Union institutions, bodies, offices and agencies; (g)to exchange views on the implementation of sector-specific Union legal acts that contain provisions on cybersecurity; (h)where relevant, to discuss reports on the peer review referred to in Article 19(9) and draw up conclusions and recommendations; (i)to carry out coordinated security risk assessments of critical supply chains in accordance with Article 22(1); (j)to discuss cases of mutual assistance, including experiences and results from cross-border joint supervisory actions as referred to in Article 37; (k)upon the request of one or more Member States concerned, to discuss specific requests for mutual assistance as referred to in Article 37; (l)to provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;					

	(m)to exchange views on the policy on follow-up actions following large-scale cybersecurity incidents and crises on the basis of lessons learned of the CSIRTs network and EU-CyCLONe; (n)to contribute to cybersecurity capabilities across the Union by facilitating the exchange of national officials through a capacity building programme involving staff from the competent authorities or the CSIRTs; (o)to organise regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges; (p)to discuss the work undertaken in relation to cybersecurity exercises, including the work done by ENISA; (q)to establish the methodology and organisational aspects of the peer reviews referred to in Article 19(1), as well as to lay down the self-assessment methodology for Member States in accordance with Article 19(5), with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts in accordance with Article 19(6); (r)to prepare reports for the purpose of the review referred to in Article 40 on the experience gained at a strategic level and from peer reviews; (s)to discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware. The Cooperation Group shall submit the reports referred to in the first subparagraph, point (r), to the Commission, to the European Parliament and to the Council.					

14.5.	Member States shall ensure effective, efficient and secure cooperation of their representatives in the Cooperation Group.			НП	Односи се само на тела која се оснују на нивоу ЕУ.	
14.6.	The Cooperation Group may request from the CSIRTs network a technical report on selected topics.			НП	Односи се само на тела која се оснују на нивоу ЕУ.	
14.7.	By 1 February 2024 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.			НП	Правило о примени директиве.	
14.8.	The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first subparagraph of this paragraph in accordance with paragraph (4), point (e).			НП	Обавеза Комисије.	
14.9.	The Cooperation Group shall meet on a regular basis and in any event at least once a year with the Critical Entities Resilience Group established under Directive (EU) 2022/2557 to promote and facilitate strategic cooperation and the exchange of information.			НП	Односи се само на тела која се оснују на нивоу ЕУ.	
15.1.	***CSIRTs network*** In order to contribute to the development of confidence and trust and to promote swift and effective operational cooperation among Member States, a network of national CSIRTs is established.			НП	Односи се на ЦЕРТове држава чланица ЕУ.	
15.2.	The CSIRTs network shall be composed of representatives of the CSIRTs designated or established pursuant to Article 10 and the computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU). The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively provide assistance for			НП	Односи се на ЦЕРТове држава чланица ЕУ.	

	the cooperation among the CSIRTs.					
15.3.	The CSIRTs network shall have the following tasks: (a)to exchange information about the CSIRTs' capabilities; (b)to facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs; (c)to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities; (d)to exchange information with regard to cybersecurity publications and recommendations; (e)to ensure interoperability with regard to information-sharing specifications and protocols; (f)at the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities; (g)at the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State; (h)to provide Member States with assistance in addressing cross-border incidents pursuant to this Directive; (i)to cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators pursuant to Article 12(1) with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;			НП	Односи се на ЦЕРТове држава чланица ЕУ.	

	(j)to discuss and identify further forms of operational cooperation, including in relation to: (i)categories of cyber threats and incidents; (ii)early warnings; (iii)mutual assistance; (iv)principles and arrangements for coordination in response to cross-border risks and incidents; (v)contribution to the national large-scale cybersecurity incident and crisis response plan referred to in Article 9(4) at the request of a Member State; (k)to inform the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (j), and, where necessary, request guidance in that regard; (l)to take stock of cybersecurity exercises, including those organised by ENISA; (m)at the request of an individual CSIRT, to discuss the capabilities and preparedness of that CSIRT; (n)to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union; (o)where relevant, to discuss the peer-review reports referred to in Article 19(9); (p)to provide guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.					
15.4.	By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40,			НП	Правило примене одредби директиве.	

	assess the progress made with regard to the operational cooperation and adopt a report. The report shall, in particular, draw up conclusions and recommendations on the basis of the outcome of the peer reviews referred to in Article 19, which are carried out in relation to the national CSIRTs. That report shall be submitted to the Cooperation Group.					
15.5.	The CSIRTs network shall adopt its rules of procedure.			НП	Односи се на ЦЕРТове држава чланица ЕУ.	
15.6.	The CSIRTs network and EU-CyCLONe shall agree on procedural arrangements and cooperate on the basis thereof.			НП	Односи се на ЦЕРТове држава чланица ЕУ.	
16.1.	***European cyber crisis liaison organisation network (EU-CyCLONe)*** EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.			НП	Организована мрежа за државе чланице ЕУ.	
16.2.	EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer. ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information. Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.			НП	Организована мрежа за државе чланице ЕУ.	
16.3.	EU-CyCLONe shall have the following tasks:			НП	Организована мрежа за	

	(a)to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises; (b)to develop a shared situational awareness for large-scale cybersecurity incidents and crises; (c)to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures; (d)to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises; (e)to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).				државе чланице ЕУ.	
16.4-16.7.	EU-CyCLONe shall adopt its rules of procedure. EU-CyCLONe shall report on a regular basis to the Cooperation Group on the management of large-scale cybersecurity incidents and crises, as well as trends, focusing in particular on their impact on essential and important entities. EU-CyCLONe shall cooperate with the CSIRTs network on the basis of agreed procedural arrangements provided for in Article 15(6). By 17 July 2024 and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.			НП	Организована мрежа за државе чланице ЕУ.	
17.1.	***International cooperation*** The Union may, where appropriate, conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with			НП	Организована мрежа за државе чланице ЕУ.	

	Union data protection law.					
18.1.	***Report on the state of cybersecurity in the Union*** ENISA shall adopt, in cooperation with the Commission and the Cooperation Group, a biennial report on the state of cybersecurity in the Union and shall submit and present that report to the European Parliament. The report shall, inter alia, be made available in machine-readable data and include the following: (a)a Union-level cybersecurity risk assessment, taking account of the cyber threat landscape; (b)an assessment of the development of cybersecurity capabilities in the public and private sectors across the Union; (c)an assessment of the general level of cybersecurity awareness and cyber hygiene among citizens and entities, including small and medium-sized enterprises; (d)an aggregated assessment of the outcome of the peer reviews referred to in Article 19; (e)an aggregated assessment of the level of maturity of cybersecurity capabilities and resources across the Union, including those at sector level, as well as of the extent to which the Member States' national cybersecurity strategies are aligned.			НП	Обавеза ЕНИСАе.	
18.2.	The report shall include particular policy recommendations, with a view to addressing shortcomings and increasing the level of cybersecurity across the Union, and a summary of the findings for the particular period from the EU Cybersecurity Technical Situation Reports on incidents and cyber threats prepared by ENISA in accordance with Article 7(6) of Regulation (EU) 2019/881.			НП	Обавеза ЕНИСАе	
18.3.	ENISA, in cooperation with the Commission, the Cooperation Group and the CSIRTs network, shall develop the methodology, including the relevant variables, such as quantitative and qualitative			НП	Обавеза ЕНИСАе	

	indicators, of the aggregated assessment referred to in paragraph 1, point (e).					
19.1.	***Peer reviews*** The Cooperation Group shall, on 17 January 2025, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed. The peer reviews shall cover at least one of the following: (a)the level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in Articles 21 and 23; (b)the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities; (c)the operational capabilities of the CSIRTs; (d)the level of implementation of mutual assistance referred to in Article 37; (e)the level of implementation of the cybersecurity information-sharing arrangements referred to in Article 29; (f)specific issues of cross-border or cross-sector nature.			НП	Обавеза ЕНИСАе	

19.2-19.9.	The methodology referred to in paragraph 1 shall include objective, non-discriminatory, fair and transparent criteria on the basis of which the Member States designate cybersecurity experts eligible to carry out the peer reviews. The Commission and ENISA shall participate as observers in the peer reviews. Member States may identify specific issues as referred to in paragraph 1, point (f), for the purposes of a peer review. Before commencing a peer review as referred to in paragraph 1, Member States shall notify the participating Member States of its scope, including the specific issues identified pursuant to paragraph 3. Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts. The Cooperation Group shall, with the assistance of the Commission and ENISA, lay down the methodology for the Member States' self-assessment. Peer reviews shall entail physical or virtual on-site visits and off-site exchanges of information. In line with the principle of good cooperation, the Member State subject to the peer review shall provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security. The Cooperation Group, in cooperation with the Commission and ENISA, shall develop appropriate codes of conduct underpinning the working methods of designated cybersecurity experts. Any information obtained through the peer review shall be used solely for that purpose. The cybersecurity experts participating in the peer review shall not disclose any sensitive or confidential information obtained in the course of			НП	Обавеза ЕНИСАе	

	that peer review to any third parties. Once subject to a peer review, the same aspects reviewed in a Member State shall not be subject to a further peer review in that Member State for two years following the conclusion of the peer review, unless otherwise requested by the Member State or agreed upon after a proposal of the Cooperation Group. Member States shall ensure that any risk of conflict of interest concerning the designated cybersecurity experts is revealed to the other Member States, the Cooperation Group, the Commission and ENISA, before the commencement of the peer review. The Member State subject to the peer review may object to the designation of particular cybersecurity experts on duly substantiated grounds communicated to the designating Member State. Cybersecurity experts participating in peer reviews shall draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments shall be attached to the reports. The reports shall include recommendations to enable improvement on the aspects covered by the peer review. The reports shall be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available.					
20.1.	***Governance*** Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article. The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the	1.3.1.	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;	ПУ		

	liability of public servants and elected or appointed officials.					
20.2.	Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	1.10.3.4.	Мере заштите ИКТ система се односе на: 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, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедношћу, ради обезбеђивања континуиране едукације;	ПУ		
21.1.	***Cybersecurity risk- management measures*** Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	1.10. 1.11. 1.12.	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 примењују се у свим ИКТ системима оператора из става 1. овог члана. Мере заштите ИКТ система се односе на: 1) успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством 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	ПУ		

			информатичких обука за све запослене и ангажована лица која имају приступ ИКТ системима, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедношћу, ради обезбеђивања континуиране едукације; 5) обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу; 6) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система; 7) идентификовање информационих добара и одређивање одговорности за њихову заштиту; 8) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона; 9) заштиту носача података; 10) ограничење приступа подацима и средствима за обраду података; 11) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа; 12) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију; 13) предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података; 14) примена мера заштите ради спречавања отицања података; 15) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему; 16) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем; 17) обезбеђивање исправног и безбедног функционисања средстава за обраду података;			

			18) примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду; 19) праћење ИКТ система у циљу откривања рањивости и претњи; 20) ограничење приступа интернет страницама које могу потенцијално да наруше безбедност ИКТ система; 21) заштиту података и средстава за обраду података од злонамерног софтвера; 22) заштиту од губитка података редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за размену података; 23) чување података о догађајима који могу бити од значаја за безбедност ИКТ система; 24) обезбеђивање интегритета софтвера и оперативних система; 25) заштиту од злоупотребе техничких безбедносних слабости ИКТ система; 26) обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања; 27) заштиту података у комуникационим мрежама, укључујући уређаје и водове; 28) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система; 29) испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система; 30) заштиту података који се користе за потребе тестирања ИКТ система односно делова система; 31) процедуре за чување и брисање информација у ИКТ системима, у складу са прописима; 32) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга; 33) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга; 34) 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; 35) мере које обезбеђују континуитет обављања посла у ванредним околностима које се дефинишу Планом континуитета обављања посла; 36) усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите; 37) употребу мултифакторске аутентикације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система 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 орган, односно организација у којој се обављају послови Националног ЦЕРТ-а. 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 ИКТ система од посебног значаја заснива се на Акту о процени ризика из члана 11. овог закона. Примена мера заштите ИКТ система мора бити у складу са процењеним ризицима, како би се обезбедила адекватна заштита система и минимизирао утицај потенцијалних инцидената. Акт о безбедности мора да буде усклађен с променама у окружењу и у самом ИКТ систему. Оператор 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 ближе уређује садржај акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери, као и достављање извештаја надлежном органу, доноси Влада на предлог Министарства.			
21.2. (a)	The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: (a)policies on risk analysis and information system security;	1.11. 1.12.	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	ПУ		

			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 орган, односно организација у којој се обављају послови Националног ЦЕРТ-а. 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 ИКТ система од посебног значаја заснива се на Акту о процени ризика из члана 11. овог закона. Примена мера заштите ИКТ система мора бити у складу са процењеним ризицима, како би се обезбедила адекватна заштита система и минимизирао утицај потенцијалних инцидената. Акт о безбедности мора да буде усклађен с променама у окружењу и у самом ИКТ систему. Оператор 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 ближе уређује садржај			

			акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери, као и достављање извештаја надлежном органу, доноси Влада на предлог Министарства.			
21.2. (b)	(b)incident handling;	1.10.34. 1.10.35.	Мере заштите ИКТ система се односе на: 34) 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; 35) мере које обезбеђују континуитет обављања посла у ванредним околностима које се дефинишу Планом континуитета обављања посла.			
21.2. (c)	(c)business continuity, such as backup management and disaster recovery, and crisis management;	1.10.22. 1.10.35.	Мере заштите ИКТ система се односе на: 22) заштиту од губитка података редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за размену података; 35) мере које обезбеђују континуитет обављања посла у ванредним околностима које се дефинишу Планом континуитета обављања посла.			
21.2. (d)	(d)supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	1.10.32. 1.10.33.	Мере заштите ИКТ система се односе на: 32) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга; 33) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;			
21.2. (e)	(e)security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	1.10.18. 1.10.24. 1.10.25. 1.10.26.	Мере заштите ИКТ система се односе на: 18) примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду; 24) обезбеђивање интегритета софтвера и оперативних система; 25) заштиту од злоупотребе техничких безбедносних слабости ИКТ система; 26) обезбеђивање заштите ИКТ система	ПУ		

			приликом спровођења ревизорског тестирања;			
21.2. (f)	(f)policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	1.10.36.	36) усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите.	ПУ		
21.2. (g)	(g)basic cyber hygiene practices and cybersecurity training;	1.10.4. 1.10.7.	Мере заштите ИКТ система се односе на: 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, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедношћу, ради обезбеђивања континуиране едукације; 7) идентификовање информационих добара и одређивање одговорности за њихову заштиту;	ПУ		
21.2. (h)	(h)policies and procedures regarding the use of cryptography and, where appropriate, encryption;	1.10.13.	Мере заштите ИКТ система се односе на: 13) предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података;	ПУ		
21.2. (i)	(i)human resources security, access control policies and asset management;	1.10.1. 1.10.6. 1.10.7. 1.10.10. 1.10.12.	Мере заштите ИКТ система се односе на: 1) успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система; 6) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система; 7) идентификовање информационих добара и одређивање одговорности за њихову заштиту; 10) ограничење приступа подацима и средствима за обраду података;	ПУ		

			12) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију.			
21.2. (j)	(j)the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	1.10.37.	Мере заштите ИКТ система се односе на: 37) употребу мултифакторске аутентикације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система			
21.3.	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).	1.47. 1.48. 1.49.	Инспекција за информациону безбедност Члан 47. 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 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 48. 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, конфигурацију и пенетрационо тестирање ИКТ система у циљу утврђивања евентуалних	ПУ		

			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. Стручни надзор Члан 49. Стручни 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, врши Канцеларија, а у складу са законом којим се уређује инспекцијски надзор. Послове стручног надзора обавља овлашћено лице запослено у Канцеларији (у даљем тексту: овлашћено лице). У поступку стручног надзора овлашћено лице има право и обавезу да контролише: 1) адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај; 2) ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите; 3) одговарајуће спровођење процеса провере усклађености примењених мера ИКТ система са актом о безбедности; 4) примену препорука и мера у случају инцидената који значајно угрожавају информациону безбедност. Ако у вршењу стручног надзора Канцеларија			

			утврди неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, о томе обавештава надзираног субјекта и одређује му рок у коме је дужан да их отклони. Рок из става 4. овог члана не може бити краћи од осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање. Ако Канцеларија утврди да надзирани субјекат није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, подноси пријаву инспекцији. Канцеларија је дужна да по захтеву инспектора за информациону безбедност обави стручни надзор и достави информацију о утврђеном чињеничном стању. Образац легитимације и начин издавања легитимације овлашћеног лица утврђује Канцеларија. Легитимација овлашћеног лица обавезно садржи: грб Републике Србије и назив Канцеларије, име и презиме овлашћеног лица, фотографију овлашћеног лица, службени број легитимације, датум издавања легитимације, печат Канцеларије, потпис директора Канцеларије, као и одштампани текст следеће садржине: „Ималац ове легитимације има овлашћења у складу са одредбама члана 46. ст. 3. и 4. Закона о информационој безбедности.”			
21.4.	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	1.47. 1.48. 1.49.	Инспекција за информациону безбедност Члан 47. 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 преко инспектора за информациону безбедност. У оквиру инспекцијског надзора рада оператора ИКТ система, инспектор за информациону безбедност утврђује да ли су испуњени услови	ПУ		

			прописани овим законом и прописима донетим на основу овог закона. Члан 48. 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, конфигурацију и пенетрационо тестирање 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. Стручни надзор Члан 49. Стручни 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, врши Канцеларија, а у складу са законом којим се уређује инспекцијски надзор. Послове стручног надзора обавља овлашћено лице запослено у Канцеларији (у даљем тексту: овлашћено лице).		

			У поступку стручног надзора овлашћено лице има право и обавезу да контролише: 1) адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај; 2) ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите; 3) одговарајуће спровођење процеса провере усклађености примењених мера ИКТ система са актом о безбедности; 4) примену препорука и мера у случају инцидената који значајно угрожавају информациону безбедност. Ако у вршењу стручног надзора Канцеларија утврди неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, о томе обавештава надзираног субјекта и одређује му рок у коме је дужан да их отклони. Рок из става 4. овог члана не може бити краћи од осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање. Ако Канцеларија утврди да надзирани субјекат није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, подноси пријаву инспекцији. Канцеларија је дужна да по захтеву инспектора за информациону безбедност обави стручни надзор и достави информацију о утврђеном чињеничном стању. Образац легитимације и начин издавања легитимације овлашћеног лица утврђује Канцеларија. Легитимација овлашћеног лица обавезно садржи: грб Републике Србије и назив Канцеларије, име и презиме овлашћеног лица, фотографију овлашћеног лица, службени број легитимације, датум издавања легитимације, печат Канцеларије, потпис директора			

			Канцеларије, као и одштампани текст следеће садржине: „Ималац ове легитимације има овлашћења у складу са одредбама члана 46. ст. 3. и 4. Закона о информационој безбедности.”			
21.5.	By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers. The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph. When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).	1.54.	Члан 54. Рокови за доношење подзаконских аката Подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона. План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности из члана 18. овог закона доноси се у року од 18 месеци од дана ступања на снагу овог закона.	ПУ		
22.1.-22.2.	***Union level coordinated security risk assessments of critical supply chains*** The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products			НП	Група коју оснивају државе чланице ЕУ	

	supply chains, taking into account technical and, where relevant, non-technical risk factors. The Commission, after consulting the Cooperation Group and ENISA, and, where necessary, relevant stakeholders, shall identify the specific critical ICT services, ICT systems or ICT products that may be subject to the coordinated security risk assessment referred to in paragraph 1.					
23.1.	***Reporting obligations*** Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.	1.13.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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	ПУ		

			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 могли довести до околности сличних онима описаним у ставу 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.			
23.2.	Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.	1.13.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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 тешкоћа у вршењу послова и пружању услуга и имају утицај на	ПУ		

			већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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.			
23.3.	An incident shall be considered to be significant if: (a)it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b)it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	1.13.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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;	ПУ		

			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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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.			
23.4.	Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: (a)without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant	1.13. 1.14. 1.15. 1.24.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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.	ПУ		

	incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (b)without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; (c)upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates; (d)a final report not later than one month after the submission of the incident notification under point (b), including the following: (i)a detailed description of the incident, including its severity and impact; (ii)the type of threat or root cause that is likely to have triggered the incident; (iii)applied and ongoing mitigation measures; (iv)where applicable, the cross-border impact of the incident; (e)in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of		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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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.			

	becoming aware of the significant incident.		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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби. 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 Канцеларије; 3) достављају завршни извештај о инциденту у року од 15 дана од дана престанка инцидента, који садржи следеће податке: (1) врсту и детаљан опис инцидента, (2) врсту претње и узрок који је довео до инцидента; (3) време и трајање инцидента, (4) озбиљност и утицај инцидента, односно последице које је инцидент изазвао, (5) информацију о евентуалном прекограничном дејству инцидента, (6) предузете активности ради отклањања последица инцидента и, по потреби, друге информације од значаја за евидентирање инцидента и статистичку обраду. Након завршеног инцидента Канцеларија припрема препоруке и савете за заштиту од потенцијалних ризика, на основу анализе извршеног инцидента.			
23.5.	The CSIRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph 4, point (a), a response to the notifying entity, including initial feedback on the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSIRT. The CSIRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT or the competent authority shall also	1.13 1.14. 1.15. 1.16.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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	ПУ		

	provide guidance on reporting the significant incident to law enforcement authorities.		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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено			

			обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) 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.			
23.6.	Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident. Such information shall include the type of information received in accordance with paragraph 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with Union or national law, preserve the entity's security and commercial interests as well as the confidentiality of the information provided.	1.17. 1.18. 1.19. 1.20. 1.21. 1.22. 1.23.	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. Канцеларија за информациону безбедност утврђује критеријуме за именовање чланова оперативног тима. Канцеларија за информациону безбедност може да, зависно од природе и последица инцидента, затражи укључивање других органа у рад оперативног тима у оквиру њихових надлежности. По потреби, састанцима оперативног тима могу присуствовати и представници посебних ЦЕРТ-ова, као и друга лица. Лица која учествују у раду сталног оперативног тима дужна су да се сертификују за рад са тајним подацима. 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, 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	ПУ		

			нивоа и криза информационе безбедности; 4) активности за унапређење способности реаговања на инциденте, а пре свега планове 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 успоставља се сарадња са органима и правним лицима чије су надлежности, односно послови и делатности повезани са планираним активностима. 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 са тим 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 објављује информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио. Изузетно од става 3. овог члана, Канцеларија за информациону безбедност може објавити информацију о инциденту који се догодио у оператору приоритетног ИКТ система од посебног значаја који обавља делатност у области банкарства и финансијских тржишта из			

			члана 5. став 2. тачка 1) подтачка (3), уз претходно прибављену сагласност Народне банке Србије односно Комисије за хартије од вредности. Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске комуникације и поштанске услуге дужни су да обавештења 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 безбедносне и контраобавештајне послове од значаја за одбрану Републике Србије или органу надлежном за послове националне безбедности, у случају да је инцидент повезан са значајним нарушавањем информационе безбедности које има или може имати за последицу угрожавање одбране Републике Србије или националне безбедности. Приликом управљања инцидентом Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске 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 је дужна да о томе обавести Министарство. Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, припрема препоруке и мере за решавање инцидента. Министарство након пријема обавештења из става 1. овог члана сазива седницу Тела за координацију послова информационе безбедности. Након завршетка инцидента Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, 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 инцидента којем је у складу са класификацијом утврђен ниво опасности „веома висок“ и који представља кризу информационе безбедности, руковођење и координацију спровођења мера и задатака предузима Влада. Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, израђује предлог 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 информационе безбедности; 4) задужење органа за поступање у складу са својим надлежностима; 5) мере за решавање кризе. Предлог за проглашење кризе информационе безбедности упућује се Министарству, које по			

			пријему предлога без одлагања сазива седницу Тела за координацију послова информационе безбедности. Влада на предлог Министарства доноси одлуку о проглашењу кризе информационе безбедности и задужује органе да поступају према предложеним мерама у складу са својим надлежностима. Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, координира решавањем кризе информационе безбедности и најмање једном недељно извештава Министарство и Владу о свим активностима. Предлог за проглашење завршетка кризе информационе 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.			
23.7.	Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.	1.22.	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 је дужна да о томе обавести Министарство. Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, припрема препоруке и мере за решавање инцидента. Министарство након пријема обавештења из става 1. овог члана сазива седницу Тела за координацију послова информационе безбедности. Након завршетка инцидента Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, сачињава завршни извештај који доставља Министарству у року од 30 дана након завршеног инцидента.	ПУ		

23.8.	At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.	1.34.	Међународна сарадња и послови јединствене тачке контакта Члан 34. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија 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	ПУ		

23.9.	The single point of contact shall submit to ENISA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30. In order to contribute to the provision of comparable information, ENISA may adopt technical guidance on the parameters of the information to be included in the summary report. ENISA shall inform the Cooperation Group and the CSIRTs network about its findings on notifications received every six months.			НП	Обавеза држава чланица према ЕНИСАи	
23.10.	The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive (EU) 2022/2557.	1.31.1.	Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система.	ПУ		
23.11.	The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article. By 17 October 2024, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, adopt implementing acts further specifying the cases in which an incident shall be considered to be significant as referred to in paragraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities. The Commission shall exchange advice and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in	1.54.	Члан 54. Рокови за доношење подзаконских аката Подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона. План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности из члана 18. овог закона доноси се у року од 18 месеци од дана ступања на снагу овог закона.	ПУ		

	accordance with Article 14(4), point (e). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).					
24.1.	***Use of European cybersecurity certification schemes*** In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.			НП	Одредба се односи на коришћење сертификационих шема у ЕУ.	
24.2.	The Commission is empowered to adopt delegated acts, in accordance with Article 38, to supplement this Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881. Those delegated acts shall be adopted where insufficient levels of cybersecurity have been identified and shall include an implementation period. Before adopting such delegated acts, the Commission shall carry out an impact assessment and shall carry out consultations in accordance with Article 56 of Regulation (EU) 2019/881.			НП	Овлашћења комисије.	
24.3.	Where no appropriate European cybersecurity certification scheme for the purposes of paragraph 2 of this Article is available, the Commission may, after consulting the Cooperation Group and the European Cybersecurity Certification Group, request ENISA to prepare a candidate scheme pursuant to Article 48(2) of Regulation (EU) 2019/881.			НП	Овлашћења Комисије.	

25.1.	***Standardisation*** In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.			ПУ	Осигурана имплементација применом општих прописа који се односе на стандардизацију.	
25.2.	ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.			НП	Овлашћења ЕНИСА.	
26.1.	***Jurisdiction and territoriality*** Entities falling within the scope of this Directive shall be considered to fall under the jurisdiction of the Member State in which they are established, except in the case of: (a)providers of public electronic communications networks or providers of publicly available electronic communications services, which shall be considered to fall under the jurisdiction of the Member State in which they provide their services; (b)DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms, which shall be considered to fall under the jurisdiction of the Member State in which they have their main establishment in the Union under paragraph 2; (c)public administration entities, which shall be considered to fall under the jurisdiction of the Member State which established them.			НП	Регулише међусобне надлежности држава чланица у случају сукоба јурисдикција.	

26.2.	For the purposes of this Directive, an entity as referred to in paragraph 1, point (b), shall be considered to have its main establishment in the Union in the Member State where the decisions related to the cybersecurity risk-management measures are predominantly taken. If such a Member State cannot be determined or if such decisions are not taken in the Union, the main establishment shall be considered to be in the Member State where cybersecurity operations are carried out. If such a Member State cannot be determined, the main establishment shall be considered to be in the Member State where the entity concerned has the establishment with the highest number of employees in the Union.					
26.3.	If an entity as referred to in paragraph 1, point (b), is not established in the Union, but offers services within the Union, it shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. Such an entity shall be considered to fall under the jurisdiction of the Member State where the representative is established. In the absence of a representative in the Union designated under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for the infringement of this Directive.			НП	Регулише међусобне надлежности држава чланица у случају сукоба јурисдикција.	
26.4.	The designation of a representative by an entity as referred to in paragraph 1, point (b), shall be without prejudice to legal actions, which could be initiated against the entity itself.			НП	Регулише међусобне надлежности држава чланица у случају сукоба јурисдикција.	
26.5.	Member States that have received a request for mutual assistance in relation to an entity as referred to in paragraph 1, point (b), may, within the limits of that request, take appropriate supervisory and enforcement measures in relation to the entity concerned that provides services or which has a network and information system on their territory.			НП	Регулише међусобне надлежности држава чланица у случају сукоба јурисдикција.	
27.1.	***Registry of entities*** ENISA shall create and maintain a registry of DNS service providers, TLD name registries, entities			НП	Обавеза ЕНИСА	

	providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact in accordance with paragraph 4. Upon request, ENISA shall allow the competent authorities access to that registry, while ensuring that the confidentiality of information is protected where applicable.					
27.2.	Member States shall require entities referred to in paragraph 1 to submit the following information to the competent authorities by 17 January 2025: (a)the name of the entity; (b)the relevant sector, subsector and type of entity referred to in Annex I or II, where applicable; (c)the address of the entity's main establishment and its other legal establishments in the Union or, if not established in the Union, of its representative designated pursuant to Article 26(3); (d)up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative designated pursuant to Article 26(3); (e)the Member States where the entity provides services; and (f)the entity's IP ranges.	1.9.	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.	ПУ		

			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 става 1. тач. 4), 5), 6) и 8) 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 ст. 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 законом којим се уређује заштита података о личности и чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 5. овог члана. Министарство ставља на располагање ажурну Евиденцију Канцеларији за информациону безбедност ради извршења одредби овог закона у погледу прикупљања и размене информација о претњама, рањивостима и инцидентима и пружања подршке, упозоравања и саветовања лица која управљају ИКТ системима. Евиденција представља тајни податак у смислу закона којим се уређује тајност података.			
27.3.	Member States shall ensure that the entities referred to in paragraph 1 notify the competent authority	1.9.	Евиденција оператора ИКТ система од посебног значаја	ПУ		

	about any changes to the information they submitted under paragraph 2 without delay and in any event within three months of the date of the change.		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 става 1. тач. 4), 5), 6) и 8) 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 ст. 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 законом којим се уређује заштита података о личности и чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 5. овог члана. Министарство ставља на располагање ажурну Евиденцију Канцеларији за информациону безбедност ради извршења одредби овог закона у погледу прикупљања и размене информација о претњама, рањивостима и инцидентима и пружања подршке, упозоравања и саветовања лица која управљају ИКТ системима. Евиденција представља тајни податак у смислу закона којим се уређује тајност података.			
27.4.	Upon receipt of the information referred to in paragraphs 2 and 3, except for that referred to in paragraph 2, point (f), the single point of contact of the Member State concerned shall, without undue delay, forward it to ENISA.			НП	Обавеза према ЕНИСА	
27.5.	Where applicable, the information referred to in paragraphs 2 and 3 of this Article shall be submitted through the national mechanism referred to in Article 3(4), fourth subparagraph.			НП	Обавеза према ЕНИСА	
28.1.	***Database of domain name registration data*** For the purpose of contributing to the security, stability and resilience of the DNS, Member States shall require TLD name registries and entities providing domain name registration services to collect and maintain accurate and complete domain	1.35.1.	Организације које су овлашћене за управљање регистром домена највишег нивоа и пружање услуга ДНС-а обавезне су да прикупљају, чувају и одржавају тачне и потпуне податке о регистрацији домена у посебној бази података,	ПУ		

	name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.		уз дужну пажњу и у складу са прописима о заштити података о личности.			
28.2.	For the purposes of paragraph 1, Member States shall require the database of domain name registration data to contain the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include: (a)the domain name; (b)the date of registration; (c)the registrant's name, contact email address and telephone number; (d)the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.	1.37.2.	База података из става 1 овог члана мора да садржи најмање следеће податке: 1) назив домена; 2) датум регистрације домена; 3) име, контакт адресу електронске поште и број телефона регистранта; 4) контакт адресу електронске поште и број телефона лица задуженог за администрацију домена, уколико се разликују од података регистранта.	ПУ		
28.3.	Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available.	1.37.3.	Организације из става 1. овог члана дужне су да усвоје и примене акте и процедуре за верификацију тачности и потпуности података у бази података. Ове процедуре морају бити јавно доступне.	ПУ		
28.4.	Member States shall require the TLD name registries and the entities providing domain name registration services to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.	1.37.4.	Организације из става 1. овог члана дужне су да обезбеде јавну доступност података који нису лични одмах по регистрацији домена, а у складу са правилима и условима регистрације назива националних интернет домена.	ПУ		
28.5.	Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection	1.37.5. 1.37.6.	Организације из става 1. овог члана обавезне су да омогуће приступ специфичним подацима о регистрацији домена на основу законитих и образложених захтева овлашћених лица или органа, у складу са овлашћењима додељеним прописима који уређују делокруг њиховог рада.	ПУ		

	law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.	1.37.7.	Одговор на захтев из става 5. овог члана мора бити достављен без одлагања, а најкасније у року од 72 сата од пријема захтева. Акти и процедуре за откривање података на основу ових захтева морају бити јавно доступни.			
28.6.	Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.	1.37.8.	У складу са овим чланом, прикупљање података о регистрацији домена не сме довести до дуплирања података. Организације из става 1. овог члана дужне су да сарађују ради избегавања дуплирања и осигурања усклађености са законом.	ПУ		
29.1.	***Cybersecurity information-sharing arrangements*** Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing: (a)aims to prevent, detect, respond to or recover from incidents or to mitigate their impact; (b)enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.	1.33. 1.34.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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. Канцеларија остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и	ПУ		

			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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
29.2.	Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information	1.33. 1.34.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима	ПУ		

	shared.		самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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. Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду			

			усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
29.3.	Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).	1.33. 1.34.	Сарадња на националном нивоу Члан 33. Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система. Канцеларија 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 Канцеларија је дужна 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.	ПУ		

			Канцеларија 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 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система. Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације. Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија 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. Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.			
29.4.	Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in	1.47.	Инспекција за информациону безбедност Члан 47. Инспекција за информациону безбедност врши инспекцијски надзор над применом овог закона	ПУ		

	paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.		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 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.			
29.5.	ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.			НП	Обавеза ЕНИСА	
30.1.	***Voluntary notification of relevant information*** Member States shall ensure that, in addition to the notification obligation provided for in Article 23, notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by: (a)essential and important entities with regard to incidents, cyber threats and near misses; (b)entities other than those referred to in point (a), regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses.			ПУ	Проистиче из одредби чланова 13-15 о обавештавању о инцидентима.	
30.2.	Member States shall process the notifications referred to in paragraph 1 of this Article in accordance with the procedure laid down in Article 23. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Where necessary, the CSIRTs and, where applicable, the competent authorities shall provide the single points of contact with the information about notifications received pursuant to this Article, while ensuring the confidentiality and appropriate	1.13. 1.14. 1.15.	Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност Члан 13. Оператори ИКТ система од посебног значаја дужни су да доставе обавештење 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	ПУ		

	protection of the information provided by the notifying entity. Without prejudice to the prevention, investigation, detection and prosecution of criminal offences, voluntary reporting shall not result in the imposition of any additional obligations upon the notifying entity to which it would not have been subject had it not submitted the notification.		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 тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије; 5) инциденти који доводе до неовлашћеног приступа 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 могли довести до околности сличних онима описаним у ставу 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 путем веб странице Министарства или Канцеларије 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) дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности. Оператори приоритетних ИКТ система од посебног значаја који обављају делатности електронских комуникација из члана 5. став 2. тачка 1) подтачка (9) алинеја трећа и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 2. тачка 1) алинеја прва, 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 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 ИКТ система од посебног значаја из става 2. и 3. овог члана обавештавају кориснике о инцидентима 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 министарствима надлежним за секторе критичне инфраструктуре. Органи из ст. 1–3. овог закона, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података. 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, односно сазнања о инциденту 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) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидената, као и мере које су том приликом предузете; 9) друге релевантне информације, по потреби.			
31.1.	***General aspects concerning supervision and enforcement*** Member States shall ensure that their competent authorities effectively supervise and take the measures necessary to ensure compliance with this Directive.	1.47. 1.49.	Инспекција за информациону безбедност Члан 47. 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 преко	ПУ		

			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. Стручни надзор Члан 49. Стручни 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, врши Канцеларија, а у складу са законом којим се уређује инспекцијски надзор. Послове стручног надзора обавља овлашћено лице запослено у Канцеларији (у даљем тексту: овлашћено лице). У поступку стручног надзора овлашћено лице има право и обавезу да контролише: 1) адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај; 2) ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите; 3) одговарајуће спровођење процеса провере усклађености примењених мера ИКТ система са актом о безбедности; 4) примену препорука и мера у случају инцидената који значајно угрожавају информациону безбедност. Ако у вршењу стручног надзора Канцеларија утврди неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, о томе обавештава надзираног субјекта и одређује му рок у коме је дужан да их отклони. Рок из става 4. овог члана не може бити краћи од			

			осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање. Ако Канцеларија утврди да надзирани субјекат није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, подноси пријаву инспекцији. Канцеларија је дужна да по захтеву инспектора за информациону безбедност обави стручни надзор и достави информацију о утврђеном чињеничном стању. Образац легитимације и начин издавања легитимације овлашћеног лица утврђује Канцеларија. Легитимација овлашћеног лица обавезно садржи: грб Републике Србије и назив Канцеларије, име и презиме овлашћеног лица, фотографију овлашћеног лица, службени број легитимације, датум издавања легитимације, печат Канцеларије, потпис директора Канцеларије, као и одштампани текст следеће садржине: „Ималац ове легитимације има овлашћења у складу са одредбама члана 46. ст. 3. и 4. Закона о информационој безбедности.”			
31.2.	Member States may allow their competent authorities to prioritise supervisory tasks. Such prioritisation shall be based on a risk-based approach. To that end, when exercising their supervisory tasks provided for in Articles 32 and 33, the competent authorities may establish supervisory methodologies allowing for a prioritisation of such tasks following a risk-based approach.	3.9.	Процена ризика Члан 9. Инспекцијски надзор заснива се на процени ризика и сразмеран је процењеном ризику, тако да се ризиком делотворно управља. Процена ризика је део процеса анализе ризика, који обухвата и управљање ризиком и обавештавање о ризику. Ризик, према степену, може бити незнатан, низак, средњи, висок и критичан. Инспекција није дужна да врши инспекцијски надзор када је процењени ризик незнатан. Ризик се процењује у току припреме плана инспекцијског надзора и пре и у току инспекцијског надзора. Када се у току реализације годишњег плана инспекцијског надзора промене околности на основу којих је процењен ризик и сачињен план, инспекција усклађује процену ризика и план инспекцијског надзора са новонасталим околностима. Процена ризика у току припреме плана	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			инспекцијског надзора врши се тако што инспекција у праћењу и анализи стања у области инспекцијског надзора која је у њеном делокругу идентификује ризике по законом и другим прописом заштићена добра, права и интересе, који могу настати из пословања или поступања надзираног субјекта и, према одговарајућим критеријумима, процењује тежину штетних последица и вероватноћу њиховог настанка, тако да се добије процењени степен ризика. Тежина штетних последица процењује се полазећи од: 1) природе штетних последица, која произлази из врсте делатности или активности надзираног субјекта, односно карактеристика робе или производа кога надзирани субјекат ставља у промет или услуга које надзирани субјекат пружа, или радњи које предузима, односно овлашћења која врши у склопу свог пословања или поступања, а у односу на законом и другим прописом заштићена добра, права и интересе, и 2) обима штетних последица, пре свега круга лица који користе робу, производ или услуге, односно круга лица која остварују одређена права у надзираном субјекту или у вези са надзираним субјектом, односно опсега законом и другим прописом заштићених добара, права и интереса на које се односи делатност или активност надзираног субјекта или на које она утиче. Вероватноћа настанка штетних последица процењује се полазећи нарочито од претходног пословања и поступања надзираног субјекта, укључујући последње утврђено стање законитости и безбедности његовог пословања и поступања. Вероватноћа настанка штетних последица процењује се полазећи и од: српских стандарда и правила добре праксе које надзирани субјекат примењује; система управљања и унутрашњег надзора над законитошћу, правилношћу и безбедношћу пословања и поступања код надзираног субјекта, узимајући у обзир политику управљања ризицима и различите облике унутрашњег надзора код надзираног субјекта, као и ревизију			

			финансијских извештаја надзираног субјекта; стања у области у којој се његова делатност или активност врши и предвиђања будућих кретања у њој; унутрашњих и спољних стручних, техничких, технолошких и финансијских капацитета надзираног субјекта. Поред процене ризика за надзиране субјекте, ризик се, према посебно прописаним критеријумима, може проценити и за поједина територијална подручја и друге територијалне и сличне целине (нпр. територијалне јединице, области и подобласти, деонице и др), објекте и групе објеката, у складу са делокругом инспекције и потребама вршења инспекцијског надзора. Заједничке елементе процене ризика у инспекцијском надзору прописује Влада. Посебне елементе процене ризика и учесталост вршења инспекцијског надзора на основу процене ризика, као и посебне критеријуме из става 8. овог члана прописује министар надлежан за одговарајућу област инспекцијског надзора, односно ималац јавног овлашћења који врши инспекцијски надзор у одређеној области. Посебне елементе процене ризика и учесталост вршења инспекцијског надзора на основу процене ризика из изворне надлежности аутономне покрајине и јединице локалне самоуправе прописује надлежни орган аутономне покрајине и јединице локалне самоуправе.			
31.3.	The competent authorities shall work in close cooperation with supervisory authorities under Regulation (EU) 2016/679 when addressing incidents resulting in personal data breaches, without prejudice to the competence and tasks of the supervisory authorities under that Regulation.	3.5.	Сарадња са другим органима, имаоцима јавних овлашћења и правним и физичким лицима Члан 5. Сарадња надлежне инспекције са другим органима државне управе, органима аутономне покрајине и јединице локалне самоуправе, правосудним и другим државним органима и другим заинтересованим органима и организацијама остварује се у складу са надлежностима инспекције и облицима сарадње утврђеним прописима о државној управи и посебним законима. Сарадња, нарочито, обухвата међусобно обавештавање, размену података, пружање	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			помоћи и заједничке мере и радње од значаја за инспекцијски надзор. Надлежна инспекција у обављању послова из свог делокруга усклађује планове инспекцијског надзора и свог рада, размењује податке, предлаже предузимање заједничких мера и активности од значаја за обављање послова инспекцијског надзора и на други начин сарађује са другим инспекцијама и субјектима са јавним овлашћењима који врше посебне облике надзора и контроле – ради обављања обухватнијег и делотворнијег инспекцијског надзора и нарочито ради сузбијања делатности или активности нерегистрованих субјеката. Државни органи, органи аутономне покрајине и јединице локалне самоуправе и имаоци јавних овлашћења дужни су, на захтев инспектора, да му у року од 15 дана од пријема захтева доставе тражене податке и обавештења који су значајни за инспекцијски надзор. Надлежна инспекција, у складу са законом, сарађује са физичким и правним лицима, нарочито у циљу превентивног деловања, као и унапређења узајамне одговорности физичких и правних лица и инспекција у процесу примене и надзора над применом прописа. У том циљу, инспекција може одржавати информативне и едукативне трибине и консултативне састанке са представницима приватног сектора и другим заинтересованим странама. Физичка и правна лица могу инспекцији подносити представке и захтеве, и од ње тражити податке и обавештења, у складу са законом. Ако се у вези са вршењем инспекцијског надзора основано очекује да надзирани субјекат пружи отпор или се он пружи и инспектору онемогућава или битно отежава вршење инспекцијског надзора, инспектор може да захтева помоћ полиције и комуналне полиције. Полиција и комунална полиција пружају помоћ према законима којима се уређују полиција и комунална полиција.			

31.4.	Without prejudice to national legislative and institutional frameworks, Member States shall ensure that, in the supervision of compliance of public administration entities with this Directive and the imposition of enforcement measures with regard to infringements of this Directive, the competent authorities have appropriate powers to carry out such tasks with operational independence vis-à-vis the public administration entities supervised. Member States may decide on the imposition of appropriate, proportionate and effective supervisory and enforcement measures in relation to those entities in accordance with the national legislative and institutional frameworks.	3.49.	Самосталност у раду Члан 49. Инспектор је самосталан у раду у границама овлашћења утврђених законом и другим прописом и за свој рад лично је одговоран. Нико не сме искоришћавањем службеног положаја или овлашћења, прекорачењем граница својих овлашћења, невршењем своје дужности или на други начин онемогућавати или ометати инспектора, односно службеника овлашћеног за вршење инспекцијског надзора у обављању инспекцијског надзора и предузимању мера и радњи на које је овлашћен.	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	
	Supervisory and enforcement measures in relation to essential entities Member States shall ensure that the supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case. Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to:		Овлашћења инспектора за информациону безбедност Члан 48. 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, конфигурацију и пенетрационо тестирање 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.			

32.1. 32.2.	(a)on-site inspections and off-site supervision, including random checks conducted by trained professionals; (b)regular and targeted security audits carried out by an independent body or a competent authority; (c)ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity; (d)security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned; (e)requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27; (f)requests to access data, documents and information necessary to carry out their supervisory tasks; (g)requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information.	1.48. 3.6. 3.7. 3.20. 3.21.	Врсте инспекцијског надзора Члан 6. Инспекцијски надзор, према врсти, може бити редован, ванредан, мешовити, контролни и допунски. Редован инспекцијски надзор врши се према плану инспекцијског надзора. Инспекцијски надзор на државној граници, који се обавља редовно, уподобљава се редовном инспекцијском надзору и на њега се сходно примењују одредбе овог закона, ако овим или посебним законом није другачије одређено, односно када то проистиче из потврђеног међународног уговора или правних тековина Европске уније. Ванредан инспекцијски надзор врши се: када је неопходно да се, сагласно делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину, права и интересе запослених и радно ангажованих лица, привреду, животну средину, биљни или животињски свет, јавне приходе, несметан рад органа и организација, комунални ред или безбедност; када се после доношења годишњег	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	
	The results of any targeted security audit shall be made available to the competent authority. The		плана инспекцијског надзора процени да је ризик висок или критичан или промене			

	costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.		околности; када такав надзор захтева надзирани субјекат; ради спречавања обављања делатности и вршења активности нерегистрованих субјеката; по захтеву јавног тужиоца; када се поступа по представци правног или физичког лица; када другостепени орган преко инспекције допуњава поступак или понавља цео поступак или његов део, а нису испуњени услови за допунски инспекцијски надзор. Ванредан инспекцијски надзор по захтеву надзираног субјекта може бити утврђујући, који се врши када је потребно утврдити испуњеност прописаних услова након чијег испуњења надзирани субјекат стиче право за почетак рада или обављања делатности, вршења активности или остваривање одређеног права, у складу са посебним законом, или потврђујући, који се врши када надзирани субјекат поднесе захтев да се потврди законитост и безбедност поступања у вршењу одређеног права или извршењу одређене обавезе, односно у његовом пословању. Мешовити инспекцијски надзор врши се истовремено као редован и ванредан надзор код истог надзираног субјекта, када се предмет редовног и ванредног инспекцијског надзора делимично или у целости поклапају или су повезани. Контролни инспекцијски надзор врши се ради утврђивања извршења мера које су предложене или наложене надзираном субјекту у оквиру редовног или ванредног инспекцијског надзора. Допунски инспекцијски надзор врши се по службеној дужности или поводом захтева надзираног субјекта, ради утврђивања чињеница које су од значаја за инспекцијски надзор, а које нису утврђене у редовном, ванредном, мешовитом или контролном инспекцијском надзору, с тим да се може извршити само један допунски инспекцијски надзор, у року који не може бити дужи од 30 дана од окончања редовног, ванредног или контролног инспекцијског надзора. Облици инспекцијског надзора			

			Члан 7. Инспекцијски надзор, према облику, може бити теренски и канцеларијски. Теренски инспекцијски надзор врши се изван службених просторија инспекције, на лицу места и састоји се од непосредног увида у земљиште, објекте, постројења, уређаје, просторије, возила и друга наменска превозна средства, предмете, робу и друге предмете, акте и документацију надзираног субјекта. Канцеларијски инспекцијски надзор врши се у службеним просторијама инспекције, увидом у акте, податке и документацију надзираног субјекта. Права и дужности надзираног субјекта Члан 20. Надзирани субјекти имају једнака права и обавезе у инспекцијском надзору, што укључује и право да инспекција једнако поступа у истим или битно сличним ситуацијама према свим надзираним субјектима. Надзирани субјекат у поступку инспекцијског надзора има право: да буде упознат са предметом и трајањем поступка, налогом за инспекцијски надзор и другим актима донетим у поступку; да буде упознат са правима и дужностима које има у вези са инспекцијским надзором; да се изјасни о чињеницама битним за потпуно и правилно утврђивање чињеничног стања и понуђеним доказима; да учествује у извођењу доказа, поставља питања сведоцима и вештацима, износи чињенице које су од значаја за инспекцијски надзор; да предлаже доказе и износи правне тврдње; да захтева превентивно деловање; да упозори инспектора на тајност информација које му чини доступним; да укаже на незаконитости у поступку и да захтева да се оне отклоне; да захтева накнаду штете која му је проузрокована незаконитим инспекцијским надзором. Ако више инспекција врши заједнички надзор, надзирани субјекат има право да инспектору ускрати давање података и изјава које је дао једном од инспектора у том надзору.			

			Надзирани субјекат има право да инспектору ускрати давање података и изјава о предмету раније извршеног надзора, осим ако су се ти подаци у међувремену променили, као и када је давање података неопходно ради предузимања хитних мера ради спречавања или отклањања опасности по живот или здравље људи, животну средину или биљни или животињски свет. Када је уредно обавештен о предстојећем инспекцијском надзору, надзирани субјекат дужан је да буде присутан на месту вршења надзора, осим ако постоје нарочито оправдане околности које га у томе спречавају, о чему је дужан да благовремено на подесан начин обавести инспекцију. Ако надзирани субјекат који је уредно обавештен о предстојећем инспекцијском надзору не буде присутан на месту вршења надзора, а не постоје околности из става 5. овог члана, инспекцијски надзор се врши у присуству службеног или другог лица које се затекне на месту вршења инспекцијског надзора. Надзирани субјекат дужан је да инспектору који му предочи службену легитимацију и уручи налог за инспекцијски надзор, када је он издат, односно који поступи у складу са чланом 18. ст. 8. и 9. овог закона, омогући несметан инспекцијски надзор, што подразумева нарочито да: стави на располагање одговарајући радни простор за теренски надзор; обезбеди увид у пословне књиге, опште и појединачне акте, евиденције, извештаје, уговоре, приватне исправе и другу документацију надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их поседује и чува; омогући приступ локацији, земљишту, објектима, пословном и другом нестамбеном простору, постројењима, уређајима, опреми, прибору, возилима и другим наменским превозним средствима, другим средствима рада, производима, предметима који се стављају у промет, роби у промету и другим предметима којима обавља делатност или врши активност, као и другим предметима од значаја за инспекцијски надзор; благовремено пружи			

			потпуне и тачне податке који су му доступни, а ако нешто од тога не може – да разлоге за то писано образложи инспектору. Надзирани субјекат дужан је да се на захтев инспектора усмено или писано изјасни о предмету надзора. Надзирани субјекат дужан је да поштује интегритет и службено својство инспектора. Надзирани субјекат има и друга права и обавезе утврђене овим и другим законом. Овлашћења инспектора ради утврђивања чињеница Члан 21. Инспектор је овлашћен да ради утврђивања чињеница: 1) изврши увид у јавне исправе и податке из регистара и евиденција које воде надлежни државни органи, органи аутономне покрајине и органи јединице локалне самоуправе и други имаоци јавних овлашћења ако су неопходни за инспекцијски надзор, а није могао да их прибави по службеној дужности, и да их копира, у складу са законом; 2) изврши увид у личну или другу јавну исправу са фотографијом која је подобна да се идентификују овлашћена лица у надзираном субјекту, друга запослена или радно ангажована лица, физичка лица која су надзирани субјекти, сведоци, службена лица и заинтересована лица, као и физичка лица затечена на месту надзора; 3) узима писане и усмене изјаве надзираних субјеката – физичких лица и заступника, односно овлашћених лица у надзираном субјекту – правном лицу и других запослених или радно ангажованих лица, сведока, службених лица и заинтересованих лица, и да их позива да дају изјаве о питањима од значаја за инспекцијски надзор; 4) наложи да му се у одређеном року ставе на увид пословне књиге, општи и појединачни акти, евиденције, уговори и друга документација надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их надзирани субјекат поседује и чува;			

			5) врши увиђај, односно прегледа и проверава локацију, земљиште, објекте, пословни и други нестамбени простор, постројења, уређаје, опрему, прибор, возила и друга наменска превозна средства, друга средства рада, производе, предмете који се стављају у промет, робу у промету и друге предмете којима обавља делатност или врши активност, као и друге предмете од значаја за инспекцијски надзор; 6) узме потребне узорке ради њиховог испитивања и утврђивања чињеничног стања, у складу са посебним законом и прописима донетим на основу закона; 7) фотографише и сними простор у коме се врши инспекцијски надзор и друге ствари које су предмет надзора; 7а) обезбеди доказе; 8) предузме друге радње ради утврђивања чињеничног стања према овом и посебном закону. Ако надзирани субјекат обавља делатност преко организационих јединица у свом саставу које се налазе на различитим адресама, инспекцијски надзор у погледу заједничких елемената пословања или поступања и унутрашњих правила, општих аката и процеса надзираног субјекта врши инспекција надлежна према месту седишта тог надзираног субјекта. У вршењу инспекцијског надзора према организационој јединици надзираног субјекта из става 2. овог члана, инспекција надлежна за инспекцијски надзор над пословањем организационе јединице дужна је да прибави податке и информације о заједничким елементима пословања или поступања, унутрашњим правилима, општим актима и процесима овог субјекта од инспекције надлежне према месту седишта тог надзираног субјекта. У случају неуједначеног поступања инспекције или више инспекција у вршењу инспекцијског надзора према организационим јединицама надзираног субјекта из става 2. овог члана, овај субјекат, односно инспекција може да затражи акт о примени прописа од надлежног органа или		

			организације. Инспектор се стара о томе да вршењем својих овлашћења не омета редован процес рада, односно обављања делатности и вршења активности надзираног субјекта. Истоветност копија и оригинала документације надзираног субјекта потврђује надзирани субјекат својим печатом и потписом. Министар надлежан за одговарајућу област инспекцијског надзора, односно ималац јавних овлашћења који врши инспекцијски надзор у одређеној области, овлашћен је да ближе уреди услове и начин узимања и испитивања узорака.			
32.3.	When exercising their powers under paragraph 2, point (e), (f) or (g), the competent authorities shall state the purpose of the request and specify the information requested.	3.16.1. 3.16.2.	Налог за инспекцијски надзор Члан 16. Руководилац инспекције или лице које он овласти издаје писани налог за инспекцијски надзор. Налог за инспекцијски надзор садржи: податке о инспекцији; податке о инспектору или инспекторима који врше инспекцијски надзор са бројевима службених легитимација; податке о надзираном субјекту или субјектима ако су познати, а ако ти подаци нису познати, односно ако није могуће утврдити надзиране субјекте или је њихов број превелик – одговарајуће познате информације од значаја за одређење субјекта, односно субјеката код којих ће се вршити надзор (нпр.: врста делатности или активности, територијално подручје, локација објекта, врста робе или производа, односно услуга итд.); правни основ инспекцијског надзора; навођење и кратко објашњење врсте и облика инспекцијског надзора; процењени ризик; прецизан и јасан опис предмета инспекцијског надзора; планирано трајање инспекцијског надзора (дан почетка и окончања надзора); разлоге за изостављање обавештења, ако постоје; број, време и место издавања; потпис издаваоца налога; печат, када је то потребно према обележјима предмета инспекцијског надзора.	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	
32.4.	Member States shall ensure that their competent authorities, when exercising their enforcement powers in relation to essential entities, have the	1.48.	Члан 48. Овлашћења инспектора за информациону безбедност	ПУ	Имплементација ових одредби је осигурана	

	power at least to: (a)issue warnings about infringements of this Directive by the entities concerned; (b)adopt binding instructions, including with regard to measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring the entities concerned to remedy the deficiencies identified or the infringements of this Directive; (c)order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct; (d)order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period; (e)order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat; (f)order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline; (g)designate a monitoring officer with well-defined tasks for a determined period of time to oversee the compliance of the entities concerned with Articles 21 and 23; (h)order the entities concerned to make public aspects of infringements of this Directive in a specified manner; (i)impose, or request the imposition by the relevant	3.25. 3.26. 3.27. 3.28.	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, конфигурацију и пенетрационо тестирање 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. Мере управљене према надзираном субјекту и њихова сразмерност Члан 25. Надзираном субјекту инспектор може изрећи управну меру, и то превентивну меру, меру за отклањање незаконитости, посебну меру наредбе, забране или заплене или меру за заштиту права трећих лица. Инспектор изриче оне мере које су сразмерне процењеном ризику и откривеним, односно вероватним незаконитостима и штетним последицама, тако да се ризиком делотворно управља, и којима се најповољније по надзираног субјекта постижу циљ и сврха закона и другог прописа. Инспектор се обавезно стара о томе да мере из става 2. овог члана буду сразмерне економској снази надзираног субјекта, да се њихове штетне		применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

	bodies, courts or tribunals, in accordance with national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (h) of this paragraph.		последице сведу на најмању меру и настави одрживо пословање и развој надзираног субјекта. Превентивне мере Члан 26. Инспектор у записнику одређује одговарајуће превентивне мере, ако је то потребно да би се спречио настанак незаконитости и штетних последица. Ако надзирани субјекат не поступи по превентивним мерама одређеним у записнику, инспектор изриче те мере решењем. Превентивне мере јесу: 1) упозоравање надзираног субјекта о његовим обавезама из закона и других прописа, као и о прописаним радњама и мерама управљеним према надзираном субјекту и санкцијама за поступања супротна тим обавезама; 2) указивање надзираном субјекту на могућност наступања штетних последица његовог пословања или поступања; 3) налагање надзираном субјекту предузимања или уздржавања од одређених радњи ради отклањања узрока вероватних штетних последица, као и одговарајућих мера предострожности у циљу спречавања настанка могућих штетних последица; 4) друге мере којима се постиже превентивна улога инспекцијског надзора. Превентивне мере могу се изрећи и непознатом субјекту инспекцијског надзора. Нерегистрованом субјекту се не може изрећи превентивна мера. Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору.			

			Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости. Посебне мере наредбе, забране и заплене Члан 28. Ако надзирани субјекат не отклони незаконитост у остављеном року, инспектор је овлашћен да донесе решење и изрекне меру којом, до отклањања незаконитости, надзираном субјекту забрањује обављање делатности или вршење активности или заплењује документацију, робу и		

			друге предмете који су надзираном субјекту послужили за повреду прописа или су тиме настали. Инспектор је овлашћен да, без остављања рока за отклањање незаконитости, изрекне меру забране обављања делатности или вршења активности или заплене предмета или документације ако је неопходно да се, сагласно делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину веће вредности, права и интересе запослених и радно ангажованих лица, привреду, животну средину, биљни или животињски свет, јавне приходе веће вредности, несметан рад органа и организација, комунални ред или безбедност. Инспектор који забрани обављање делатности или вршење активности има право да нареди да се надзираном субјекту запечате пословне и производне просторије, објекти и други простор у коме обавља делатност или врши активност или који томе служи, постројења, уређаји, опрема, прибор, средства рада и други предмети којима обавља делатност или врши активност. Инспектор може изрећи и другу посебну меру наредбе, забране или заплене (нпр. мера повлачења или опозивања производа, мере ограничења, мера уништавања предмета, мера уклањања објекта и др), кад је то одређено посебним законом.			
32.5.	Where enforcement measures adopted pursuant to paragraph 4, points (a) to (d) and (f), are ineffective, Member States shall ensure that their competent authorities have the power to establish a deadline by which the essential entity is requested to take the necessary action to remedy the deficiencies or to comply with the requirements of those authorities. If the requested action is not taken within the deadline set, Member States shall ensure that their competent authorities have the power to: (a)suspend temporarily, or request a certification or authorisation body, or a court or tribunal, in accordance with national law, to suspend	1.48. 3.27.	Члан 48. 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,	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

	temporarily a certification or authorisation concerning part or all of the relevant services provided or activities carried out by the essential entity; (b)request that the relevant bodies, courts or tribunals, in accordance with national law, prohibit temporarily any natural person who is responsible for discharging managerial responsibilities at chief executive officer or legal representative level in the essential entity from exercising managerial functions in that entity. Temporary suspensions or prohibitions imposed pursuant to this paragraph shall be applied only until the entity concerned takes the necessary action to remedy the deficiencies or comply with the requirements of the competent authority for which such enforcement measures were applied. The imposition of such temporary suspensions or prohibitions shall be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence. The enforcement measures provided for in this paragraph shall not be applicable to public administration entities that are subject to this Directive.		конфигурацију и пенетрационо тестирање 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. Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне			

			последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости.			
32.6.	Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it has the power to ensure its compliance with this Directive. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive. As regards public administration entities, this paragraph shall be without prejudice to national law as regards the liability of public servants and elected or appointed officials.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који	ПУ		

			је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које			

			је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
32.7.	When taking any of the enforcement measures referred to in paragraph 4 or 5, the competent authorities shall comply with the rights of the defence and take account of the circumstances of each individual case and, as a minimum, take due account of: (a)the seriousness of the infringement and the importance of the provisions breached, the following, inter alia, constituting serious infringement in any event: (i)repeated violations; (ii)a failure to notify or remedy significant incidents; (iii)a failure to remedy deficiencies following binding instructions from competent authorities; (iv)the obstruction of audits or monitoring activities ordered by the competent authority following the finding of an infringement; (v)providing false or grossly inaccurate information in relation to cybersecurity risk-management measures or reporting obligations laid down in Articles 21 and 23; (b)the duration of the infringement; (c)any relevant previous infringements by the entity concerned; (d)any material or non-material damage caused, including any financial or economic loss, effects on other services and the number of users affected; (e)any intent or negligence on the part of the perpetrator of the infringement; (f)any measures taken by the entity to prevent or	3.27. 4.42. 4.43.	Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

	mitigate the material or non-material damage; (g)any adherence to approved codes of conduct or approved certification mechanisms; (h)the level of cooperation of the natural or legal persons held responsible with the competent authorities.		отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости. Одмеравање казне Члан 42. Казна за прекршаје одмерава се у границама које су за тај прекршај прописане, а при томе се узимају у обзир све околности које утичу да казна буде већа или мања, а нарочито: тежина и последице прекршаја, околности под којима је прекршај учињен, степен одговорности учиниоца, ранија осуђиваност, личне прилике учиниоца и држање учиниоца после учињеног прекршаја. Не може се узети у обзир као отежавајућа околност раније изречена прекршајна санкција учиниоцу ако је од дана правноснажности одлуке до дана доношења нове протекло више од четири године. При одмеравању висине новчане казне узеће се у обзир и имовно стање учиниоца. Ублажавање казне Члан 43. Ако се приликом одмеравања казне утврди да прекршајем нису проузроковане теже последице, а постоје олакшавајуће околности које указују да се и блажом казном може постићи сврха кажњавања, прописана казна се може ублажити тако што се може: 1) изрећи казна испод најмање мере казне која је прописана за тај прекршај али не испод најмање законске мере те врсте казне; 2) уместо прописане казне затвора изрећи новчана казна или рад у јавном интересу, али не испод најмање законске мере те врсте казне; 3) уместо прописане казне затвора и новчане казне изрећи само једна од тих казни.			
32.8.	The competent authorities shall set out a detailed reasoning for their enforcement measures. Before	3.35.	Записник о инспекцијском надзору Члан 35.	ПУ	Имплементација ових	

	adopting such measures, the competent authorities shall notify the entities concerned of their preliminary findings. They shall also allow a reasonable time for those entities to submit observations, except in duly substantiated cases where immediate action to prevent or respond to incidents would otherwise be impeded.	3.36.	Инспектор сачињава записник о инспекцијском надзору. У записник се уносе: подаци из налога за инспекцијски надзор ако је издат; време и место инспекцијског надзора, а нарочито навођење основа и образложење разлога који су условили да се инспекцијски надзор врши ван радног времена надзираног субјекта у смислу члана 19. став 2. овог закона; опис предузетих радњи и попис преузетих докумената; подаци о броју узетих узорака и предлозима које у вези са узимањем узорака даје овлашћено лице надзираног субјекта; изјаве које су дате; опис других изведених доказа; захтеви за изузеће који су поднети; утврђено чињенично стање; констатација законитог пословања и поступања надзираног субјекта; опис откривених незаконитости, са навођењем доказа на основу којег је одређена чињеница утврђена и правног основа за утврђивање незаконитости; мере које се изричу са навођењем правног основа на коме су засноване и роком за поступање по њима; одговарајућа образложења; обавеза надзираног субјекта да обавештава инспектора о поступању по мерама и рок за то обавештавање; подаци о поднетим кривичним пријавама, пријавама за привредни преступ и захтевима за покретање прекршајног поступка, ако су поднете, односно издатим прекршајним налозима, ако су издати, односно, у складу са чланом 42. став 3. овог закона, неподношење захтева за покретање прекршајног поступка, односно неиздавање прекршајног налога; подаци о другим мерама и радњама на које је инспектор овлашћен, ако су предузете; рок за давање примедаба на записник; навођење да је записник са или без примедаба прочитан лицу које присуствује надзору; други подаци и наводи од значаја за инспекцијски надзор. Контролна листа и анализа одговарајуће стручне институције, односно акредитованог тела чине саставни део записника. Овлашћено лице надзираног субјекта може да одбије да прими записник, што инспектор констатује у писаном облику и у записнику		одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			наводи разлоге због којих је пријем записника одбијен. Записник се доставља надзираном субјекту у року од осам дана од завршетка инспекцијског надзора. Општи образац записника о инспекцијском надзору прописује министар надлежан за послове државне управе. Општи образац записника о инспекцијском надзору за инспекцијски надзор из изворне надлежности аутономне покрајине и јединице локалне самоуправе прописује надлежни орган аутономне покрајине или јединице локалне самоуправе. Примедбе на записник Члан 36. Надзирани субјекат има право да у писаном облику стави примедбе на записник о инспекцијском надзору, у року од пет радних дана од његовог пријема. Инспектор оцењује примедбе, све заједно и сваку засебно, и у међусобној вези. Инспектор може после тога да изврши допунски инспекцијски надзор, да би утврдио чињенице на које се примедбе односе. Ако су у примедбама на записник изнете нове чињенице и нови докази, због којих треба изменити чињенично стање које је утврђено у записнику или друкчије правне и друге оцене, инспектор о томе саставља допуну записника, на коју се не може ставити примедба. Поступајући по примедбама на записник, инспектор може да измени предложену или наложену, односно изречену меру или да одустане од ње.			
32.9.	Member States shall ensure that their competent authorities under this Directive inform the relevant competent authorities within the same Member State under Directive (EU) 2022/2557 when exercising their supervisory and enforcement powers aiming to ensure compliance of an entity identified as a critical entity under Directive (EU) 2022/2557 with this Directive. Where appropriate,	3.5.	Сарадња са другим органима, имаоцима јавних овлашћења и правним и физичким лицима Члан 5. Сарадња надлежне инспекције са другим органима државне управе, органима аутономне покрајине и јединице локалне самоуправе, правосудним и другим државним органима и другим заинтересованим органима и	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

	the competent authorities under Directive (EU) 2022/2557 may request the competent authorities under this Directive to exercise their supervisory and enforcement powers in relation to an entity that is identified as a critical entity under Directive (EU) 2022/2557.		организацијама остварује се у складу са надлежностима инспекције и облицима сарадње утврђеним прописима о државној управи и посебним законима. Сарадња, нарочито, обухвата међусобно обавештавање, размену података, пружање помоћи и заједничке мере и радње од значаја за инспекцијски надзор. Надлежна инспекција у обављању послова из свог делокруга усклађује планове инспекцијског надзора и свог рада, размењује податке, предлаже предузимање заједничких мера и активности од значаја за обављање послова инспекцијског надзора и на други начин сарађује са другим инспекцијама и субјектима са јавним овлашћењима који врше посебне облике надзора и контроле – ради обављања обухватнијег и делотворнијег инспекцијског надзора и нарочито ради сузбијања делатности или активности нерегистрованих субјеката. Државни органи, органи аутономне покрајине и јединице локалне самоуправе и имаоци јавних овлашћења дужни су, на захтев инспектора, да му у року од 15 дана од пријема захтева доставе тражене податке и обавештења који су значајни за инспекцијски надзор. Надлежна инспекција, у складу са законом, сарађује са физичким и правним лицима, нарочито у циљу превентивног деловања, као и унапређења узајамне одговорности физичких и правних лица и инспекција у процесу примене и надзора над применом прописа. У том циљу, инспекција може одржавати информативне и едукативне трибине и консултативне састанке са представницима приватног сектора и другим заинтересованим странама. Физичка и правна лица могу инспекцији подносити представке и захтеве, и од ње тражити податке и обавештења, у складу са законом. Ако се у вези са вршењем инспекцијског надзора основано очекује да надзирани субјекат пружи отпор или се он пружи и инспектору онемогућава или битно отежава вршење инспекцијског надзора, инспектор може да			

			захтева помоћ полиције и комуналне полиције. Полиција и комунална полиција пружају помоћ према законима којима се уређују полиција и комунална полиција.			
32.10.	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an essential entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.	3.5.	Сарадња са другим органима, имаоцима јавних овлашћења и правним и физичким лицима Члан 5. Сарадња надлежне инспекције са другим органима државне управе, органима аутономне покрајине и јединице локалне самоуправе, правосудним и другим државним органима и другим заинтересованим органима и организацијама остварује се у складу са надлежностима инспекције и облицима сарадње утврђеним прописима о државној управи и посебним законима. Сарадња, нарочито, обухвата међусобно обавештавање, размену података, пружање помоћи и заједничке мере и радње од значаја за инспекцијски надзор. Надлежна инспекција у обављању послова из свог делокруга усклађује планове инспекцијског надзора и свог рада, размењује податке, предлаже предузимање заједничких мера и активности од значаја за обављање послова инспекцијског надзора и на други начин сарађује са другим инспекцијама и субјектима са јавним овлашћењима који врше посебне облике надзора и контроле – ради обављања обухватнијег и делотворнијег инспекцијског надзора и нарочито ради сузбијања делатности или активности нерегистрованих субјеката. Државни органи, органи аутономне покрајине и јединице локалне самоуправе и имаоци јавних овлашћења дужни су, на захтев инспектора, да му у року од 15 дана од пријема захтева доставе тражене податке и обавештења који су значајни за инспекцијски надзор. Надлежна инспекција, у складу са законом, сарађује са физичким и правним лицима, нарочито у циљу превентивног деловања, као и унапређења узајамне одговорности физичких и правних лица и инспекција у процесу примене и надзора над применом прописа. У том циљу, инспекција може одржавати информативне и	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			едукативне трибине и консултативне састанке са представницима приватног сектора и другим заинтересованим странама. Физичка и правна лица могу инспекцији подносити представке и захтеве, и од ње тражити податке и обавештења, у складу са законом. Ако се у вези са вршењем инспекцијског надзора основано очекује да надзирани субјекат пружи отпор или се он пружи и инспектору онемогућава или битно отежава вршење инспекцијског надзора, инспектор може да захтева помоћ полиције и комуналне полиције. Полиција и комунална полиција пружају помоћ према законима којима се уређују полиција и комунална полиција.			
33.1.	***Supervisory and enforcement measures in relation to important entities*** When provided with evidence, indication or information that an important entity allegedly does not comply with this Directive, in particular Articles 21 and 23 thereof, Member States shall ensure that the competent authorities take action, where necessary, through ex post supervisory measures. Member States shall ensure that those measures are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	1.48. 3.6. 3.7. 3.20. 3.21.	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, конфигурацију и пенетрационо тестирање 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.	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			Врсте инспекцијског надзора Члан 6. Инспекцијски надзор, према врсти, може бити редован, ванредан, мешовити, контролни и допунски. Редован инспекцијски надзор врши се према плану инспекцијског надзора. Инспекцијски надзор на државној граници, који се обавља редовно, уподобљава се редовном инспекцијском надзору и на њега се сходно примењују одредбе овог закона, ако овим или посебним законом није другачије одређено, односно када то проистиче из потврђеног међународног уговора или правних тековина Европске уније. Ванредан инспекцијски надзор врши се: када је неопходно да се, сагласно делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину, права и интересе запослених и радно ангажованих лица, привреду, животну средину, биљни или животињски свет, јавне приходе, несметан рад органа и организација, комунални ред или безбедност; када се после доношења годишњег плана инспекцијског надзора процени да је ризик висок или критичан или промене околности; када такав надзор захтева надзирани субјекат; ради спречавања обављања делатности и вршења активности нерегистрованих субјеката; по захтеву јавног тужиоца; када се поступа по представци правног или физичког лица; када другостепени орган преко инспекције допуњава поступак или понавља цео поступак или његов део, а нису испуњени услови за допунски инспекцијски надзор. Ванредан инспекцијски надзор по захтеву надзираног субјекта може бити утврђујући, који се врши када је потребно утврдити испуњеност прописаних услова након чијег испуњења надзирани субјекат стиче право за почетак рада или обављања делатности, вршења активности или остваривање одређеног права, у складу са посебним законом, или потврђујући, који се врши када надзирани субјекат поднесе захтев да			

			се потврди законитост и безбедност поступања у вршењу одређеног права или извршењу одређене обавезе, односно у његовом пословању. Мешовити инспекцијски надзор врши се истовремено као редован и ванредан надзор код истог надзираног субјекта, када се предмет редовног и ванредног инспекцијског надзора делимично или у целости поклапају или су повезани. Контролни инспекцијски надзор врши се ради утврђивања извршења мера које су предложене или наложене надзираном субјекту у оквиру редовног или ванредног инспекцијског надзора. Допунски инспекцијски надзор врши се по службеној дужности или поводом захтева надзираног субјекта, ради утврђивања чињеница које су од значаја за инспекцијски надзор, а које нису утврђене у редовном, ванредном, мешовитом или контролном инспекцијском надзору, с тим да се може извршити само један допунски инспекцијски надзор, у року који не може бити дужи од 30 дана од окончања редовног, ванредног или контролног инспекцијског надзора. Облици инспекцијског надзора Члан 7. Инспекцијски надзор, према облику, може бити теренски и канцеларијски. Теренски инспекцијски надзор врши се изван службених просторија инспекције, на лицу места и састоји се од непосредног увида у земљиште, објекте, постројења, уређаје, просторије, возила и друга наменска превозна средства, предмете, робу и друге предмете, акте и документацију надзираног субјекта. Канцеларијски инспекцијски надзор врши се у службеним просторијама инспекције, увидом у акте, податке и документацију надзираног субјекта. Права и дужности надзираног субјекта Члан 20. Надзирани субјекти имају једнака права и		

			обавезе у инспекцијском надзору, што укључује и право да инспекција једнако поступа у истим или битно сличним ситуацијама према свим надзираним субјектима. Надзирани субјекат у поступку инспекцијског надзора има право: да буде упознат са предметом и трајањем поступка, налогом за инспекцијски надзор и другим актима донетим у поступку; да буде упознат са правима и дужностима које има у вези са инспекцијским надзором; да се изјасни о чињеницама битним за потпуно и правилно утврђивање чињеничног стања и понуђеним доказима; да учествује у извођењу доказа, поставља питања сведоцима и вештацима, износи чињенице које су од значаја за инспекцијски надзор; да предлаже доказе и износи правне тврдње; да захтева превентивно деловање; да упозори инспектора на тајност информација које му чини доступним; да укаже на незаконитости у поступку и да захтева да се оне отклоне; да захтева накнаду штете која му је проузрокована незаконитим инспекцијским надзором. Ако више инспекција врши заједнички надзор, надзирани субјекат има право да инспектору ускрати давање података и изјава које је дао једном од инспектора у том надзору. Надзирани субјекат има право да инспектору ускрати давање података и изјава о предмету раније извршеног надзора, осим ако су се ти подаци у међувремену променили, као и када је давање података неопходно ради предузимања хитних мера ради спречавања или отклањања опасности по живот или здравље људи, животну средину или биљни или животињски свет. Када је уредно обавештен о предстојећем инспекцијском надзору, надзирани субјекат дужан је да буде присутан на месту вршења надзора, осим ако постоје нарочито оправдане околности које га у томе спречавају, о чему је дужан да благовремено на подесан начин обавести инспекцију. Ако надзирани субјекат који је уредно обавештен о предстојећем инспекцијском надзору не буде присутан на месту вршења			

			надзора, а не постоје околности из става 5. овог члана, инспекцијски надзор се врши у присуству службеног или другог лица које се затекне на месту вршења инспекцијског надзора. Надзирани субјекат дужан је да инспектору који му предочи службену легитимацију и уручи налог за инспекцијски надзор, када је он издат, односно који поступи у складу са чланом 18. ст. 8. и 9. овог закона, омогући несметан инспекцијски надзор, што подразумева нарочито да: стави на располагање одговарајући радни простор за теренски надзор; обезбеди увид у пословне књиге, опште и појединачне акте, евиденције, извештаје, уговоре, приватне исправе и другу документацију надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их поседује и чува; омогући приступ локацији, земљишту, објектима, пословном и другом нестамбеном простору, постројењима, уређајима, опреми, прибору, возилима и другим наменским превозним средствима, другим средствима рада, производима, предметима који се стављају у промет, роби у промету и другим предметима којима обавља делатност или врши активност, као и другим предметима од значаја за инспекцијски надзор; благовремено пружи потпуне и тачне податке који су му доступни, а ако нешто од тога не може – да разлоге за то писано образложи инспектору. Надзирани субјекат дужан је да се на захтев инспектора усмено или писано изјасни о предмету надзора. Надзирани субјекат дужан је да поштује интегритет и службено својство инспектора. Надзирани субјекат има и друга права и обавезе утврђене овим и другим законом. Овлашћења инспектора ради утврђивања чињеница Члан 21. Инспектор је овлашћен да ради утврђивања чињеница: 1) изврши увид у јавне исправе и податке из регистара и евиденција које воде надлежни		

			државни органи, органи аутономне покрајине и органи јединице локалне самоуправе и други имаоци јавних овлашћења ако су неопходни за инспекцијски надзор, а није могао да их прибави по службеној дужности, и да их копира, у складу са законом; 2) изврши увид у личну или другу јавну исправу са фотографијом која је подобна да се идентификују овлашћена лица у надзираном субјекту, друга запослена или радно ангажована лица, физичка лица која су надзирани субјекти, сведоци, службена лица и заинтересована лица, као и физичка лица затечена на месту надзора; 3) узима писане и усмене изјаве надзираних субјеката – физичких лица и заступника, односно овлашћених лица у надзираном субјекту – правном лицу и других запослених или радно ангажованих лица, сведока, службених лица и заинтересованих лица, и да их позива да дају изјаве о питањима од значаја за инспекцијски надзор; 4) наложи да му се у одређеном року ставе на увид пословне књиге, општи и појединачни акти, евиденције, уговори и друга документација надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их надзирани субјекат поседује и чува; 5) врши увиђај, односно прегледа и проверава локацију, земљиште, објекте, пословни и други нестамбени простор, постројења, уређаје, опрему, прибор, возила и друга наменска превозна средства, друга средства рада, производе, предмете који се стављају у промет, робу у промету и друге предмете којима обавља делатност или врши активност, као и друге предмете од значаја за инспекцијски надзор; 6) узме потребне узорке ради њиховог испитивања и утврђивања чињеничног стања, у складу са посебним законом и прописима донетим на основу закона; 7) фотографише и сними простор у коме се врши инспекцијски надзор и друге ствари које су предмет надзора; 7а) обезбеди доказе; 8) предузме друге радње ради утврђивања			

			чињеничног стања према овом и посебном закону. Ако надзирани субјекат обавља делатност преко организационих јединица у свом саставу које се налазе на различитим адресама, инспекцијски надзор у погледу заједничких елемената пословања или поступања и унутрашњих правила, општих аката и процеса надзираног субјекта врши инспекција надлежна према месту седишта тог надзираног субјекта. У вршењу инспекцијског надзора према организационој јединици надзираног субјекта из става 2. овог члана, инспекција надлежна за инспекцијски надзор над пословањем организационе јединице дужна је да прибави податке и информације о заједничким елементима пословања или поступања, унутрашњим правилима, општим актима и процесима овог субјекта од инспекције надлежне према месту седишта тог надзираног субјекта. У случају неуједначеног поступања инспекције или више инспекција у вршењу инспекцијског надзора према организационим јединицима надзираног субјекта из става 2. овог члана, овај субјекат, односно инспекција може да затражи акт о примени прописа од надлежног органа или организације. Инспектор се стара о томе да вршењем својих овлашћења не омета редован процес рада, односно обављања делатности и вршења активности надзираног субјекта. Истоветност копија и оригинала документације надзираног субјекта потврђује надзирани субјекат својим печатом и потписом. Министар надлежан за одговарајућу област инспекцијског надзора, односно ималац јавних овлашћења који врши инспекцијски надзор у одређеној области, овлашћен је да ближе уреди услове и начин узимања и испитивања узорака.			
33.2.	Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to important entities, have the power to subject those entities at least to:	1.48. 3.6.	Овлашћења инспектора за информациону безбедност Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора,	ПУ	Имплементација ових одредби је осигурана применом инспекторских	

	(a)on-site inspections and off-site ex post supervision conducted by trained professionals; (b)targeted security audits carried out by an independent body or a competent authority; (c)security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the cooperation of the entity concerned; (d)requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to Article 27; (e)requests to access data, documents and information necessary to carry out their supervisory tasks; (f)requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence. The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information. The results of any targeted security audit shall be made available to the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited entity, except in duly substantiated cases when the competent authority decides otherwise.	3.7. 3.20. 3.21.	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, конфигурацију и пенетрационо тестирање 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. Врсте инспекцијског надзора Члан 6. Инспекцијски надзор, према врсти, може бити редован, ванредан, мешовити, контролни и допунски. Редован инспекцијски надзор врши се према плану инспекцијског надзора. Инспекцијски надзор на државној граници, који се обавља редовно, уподобљава се редовном инспекцијском надзору и на њега се сходно примењују одредбе овог закона, ако овим или посебним законом није другачије одређено, односно када то проистиче из потврђеног међународног уговора или правних тековина Европске уније. Ванредан инспекцијски надзор врши се: када је неопходно да се, сагласно делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину, права и интересе		овлашћења на основу Закона о инспекцијском надзору.	

			запослених и радно ангажованих лица, привреду, животну средину, бильни или животињски свет, јавне приходе, несметан рад органа и организација, комунални ред или безбедност; када се после доношења годишњег плана инспекцијског надзора процени да је ризик висок или критичан или промене околности; када такав надзор захтева надзирани субјекат; ради спречавања обављања делатности и вршења активности нерегистрованих субјеката; по захтеву јавног тужиоца; када се поступа по представци правног или физичког лица; када другостепени орган преко инспекције допуњава поступак или понавља цео поступак или његов део, а нису испуњени услови за допунски инспекцијски надзор. Ванредан инспекцијски надзор по захтеву надзираног субјекта може бити утврђујући, који се врши када је потребно утврдити испуњеност прописаних услова након чијег испуњења надзирани субјекат стиче право за почетак рада или обављања делатности, вршења активности или остваривање одређеног права, у складу са посебним законом, или потврђујући, који се врши када надзирани субјекат поднесе захтев да се потврди законитост и безбедност поступања у вршењу одређеног права или извршењу одређене обавезе, односно у његовом пословању. Мешовити инспекцијски надзор врши се истовремено као редован и ванредан надзор код истог надзираног субјекта, када се предмет редовног и ванредног инспекцијског надзора делимично или у целости поклапају или су повезани. Контролни инспекцијски надзор врши се ради утврђивања извршења мера које су предложене или наложене надзираном субјекту у оквиру редовног или ванредног инспекцијског надзора. Допунски инспекцијски надзор врши се по службеној дужности или поводом захтева надзираног субјекта, ради утврђивања чињеница које су од значаја за инспекцијски надзор, а које нису утврђене у редовном, ванредном, мешовитом или контролном инспекцијском		

			надзору, с тим да се може извршити само један допунски инспекцијски надзор, у року који не може бити дужи од 30 дана од окончања редовног, ванредног или контролног инспекцијског надзора. Облици инспекцијског надзора Члан 7. Инспекцијски надзор, према облику, може бити теренски и канцеларијски. Теренски инспекцијски надзор врши се изван службених просторија инспекције, на лицу места и састоји се од непосредног увида у земљиште, објекте, постројења, уређаје, просторије, возила и друга наменска превозна средства, предмете, робу и друге предмете, акте и документацију надзираног субјекта. Канцеларијски инспекцијски надзор врши се у службеним просторијама инспекције, увидом у акте, податке и документацију надзираног субјекта. Права и дужности надзираног субјекта Члан 20. Надзирани субјекти имају једнака права и обавезе у инспекцијском надзору, што укључује и право да инспекција једнако поступа у истим или битно сличним ситуацијама према свим надзираним субјектима. Надзирани субјекат у поступку инспекцијског надзора има право: да буде упознат са предметом и трајањем поступка, налогом за инспекцијски надзор и другим актима донетим у поступку; да буде упознат са правима и дужностима које има у вези са инспекцијским надзором; да се изјасни о чињеницама битним за потпуно и правилно утврђивање чињеничног стања и понуђеним доказима; да учествује у извођењу доказа, поставља питања сведоцима и вештацима, износи чињенице које су од значаја за инспекцијски надзор; да предлаже доказе и износи правне тврдње; да захтева превентивно деловање; да упозори инспектора на тајност информација које му чини доступним; да укаже на незаконитости у поступку и да захтева да се			

			оне отклоне; да захтева накнаду штете која му је проузрокована незаконитим инспекцијским надзором. Ако више инспекција врши заједнички надзор, надзирани субјекат има право да инспектору ускрати давање података и изјава које је дао једном од инспектора у том надзору. Надзирани субјекат има право да инспектору ускрати давање података и изјава о предмету раније извршеног надзора, осим ако су се ти подаци у међувремену променили, као и када је давање података неопходно ради предузимања хитних мера ради спречавања или отклањања опасности по живот или здравље људи, животну средину или биљни или животињски свет. Када је уредно обавештен о предстојећем инспекцијском надзору, надзирани субјекат дужан је да буде присутан на месту вршења надзора, осим ако постоје нарочито оправдане околности које га у томе спречавају, о чему је дужан да благовремено на подесан начин обавести инспекцију. Ако надзирани субјекат који је уредно обавештен о предстојећем инспекцијском надзору не буде присутан на месту вршења надзора, а не постоје околности из става 5. овог члана, инспекцијски надзор се врши у присуству службеног или другог лица које се затекне на месту вршења инспекцијског надзора. Надзирани субјекат дужан је да инспектору који му предочи службену легитимацију и уручи налог за инспекцијски надзор, када је он издат, односно који поступи у складу са чланом 18. ст. 8. и 9. овог закона, омогући несметан инспекцијски надзор, што подразумева нарочито да: стави на располагање одговарајући радни простор за теренски надзор; обезбеди увид у пословне књиге, опште и појединачне акте, евиденције, извештаје, уговоре, приватне исправе и другу документацију надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их поседује и чува; омогући приступ локацији, земљишту, објектима, пословном и другом нестамбеном простору, постројењима, уређајима, опреми, прибору,			

			возилима и другим наменским превозним средствима, другим средствима рада, производима, предметима који се стављају у промет, роби у промету и другим предметима којима обавља делатност или врши активност, као и другим предметима од значаја за инспекцијски надзор; благовремено пружи потпуне и тачне податке који су му доступни, а ако нешто од тога не може – да разлоге за то писано образложи инспектору. Надзирани субјекат дужан је да се на захтев инспектора усмено или писано изјасни о предмету надзора. Надзирани субјекат дужан је да поштује интегритет и службено својство инспектора. Надзирани субјекат има и друга права и обавезе утврђене овим и другим законом. Овлашћења инспектора ради утврђивања чињеница Члан 21. Инспектор је овлашћен да ради утврђивања чињеница: 1) изврши увид у јавне исправе и податке из регистара и евиденција које воде надлежни државни органи, органи аутономне покрајине и органи јединице локалне самоуправе и други имаоци јавних овлашћења ако су неопходни за инспекцијски надзор, а није могао да их прибави по службеној дужности, и да их копира, у складу са законом; 2) изврши увид у личну или другу јавну исправу са фотографијом која је подобна да се идентификују овлашћена лица у надзираном субјекту, друга запослена или радно ангажована лица, физичка лица која су надзирани субјекти, сведоци, службена лица и заинтересована лица, као и физичка лица затечена на месту надзора; 3) узима писане и усмене изјаве надзираних субјеката – физичких лица и заступника, односно овлашћених лица у надзираном субјекту – правном лицу и других запослених или радно ангажованих лица, сведока, службених лица и заинтересованих лица, и да их позива да дају изјаве о питањима од значаја за инспекцијски		

			надзор; 4) наложи да му се у одређеном року ставе на увид пословне књиге, општи и појединачни акти, евиденције, уговори и друга документација надзираног субјекта од значаја за инспекцијски надзор, а у облику у којем их надзирани субјекат поседује и чува; 5) врши увиђај, односно прегледа и проверава локацију, земљиште, објекте, пословни и други нестамбени простор, постројења, уређаје, опрему, прибор, возила и друга наменска превозна средства, друга средства рада, производе, предмете који се стављају у промет, робу у промету и друге предмете којима обавља делатност или врши активност, као и друге предмете од значаја за инспекцијски надзор; 6) узме потребне узорке ради њиховог испитивања и утврђивања чињеничног стања, у складу са посебним законом и прописима донетим на основу закона; 7) фотографише и сними простор у коме се врши инспекцијски надзор и друге ствари које су предмет надзора; 7а) обезбеди доказе; 8) предузме друге радње ради утврђивања чињеничног стања према овом и посебном закону. Ако надзирани субјекат обавља делатност преко организационих јединица у свом саставу које се налазе на различитим адресама, инспекцијски надзор у погледу заједничких елемената пословања или поступања и унутрашњих правила, општих аката и процеса надзираног субјекта врши инспекција надлежна према месту седишта тог надзираног субјекта. У вршењу инспекцијског надзора према организационој јединици надзираног субјекта из става 2. овог члана, инспекција надлежна за инспекцијски надзор над пословањем организационе јединице дужна је да прибави податке и информације о заједничким елементима пословања или поступања, унутрашњим правилима, општим актима и процесима овог субјекта од инспекције надлежне према месту седишта тог надзираног			

			субјекта. У случају неуједначеног поступања инспекције или више инспекција у вршењу инспекцијског надзора према организационим јединицима надзираног субјекта из става 2. овог члана, овај субјекат, односно инспекција може да затражи акт о примени прописа од надлежног органа или организације. Инспектор се стара о томе да вршењем својих овлашћења не омета редован процес рада, односно обављања делатности и вршења активности надзираног субјекта. Истоветност копија и оригинала документације надзираног субјекта потврђује надзирани субјекат својим печатом и потписом. Министар надлежан за одговарајућу област инспекцијског надзора, односно ималац јавних овлашћења који врши инспекцијски надзор у одређеној области, овлашћен је да ближе уреди услове и начин узимања и испитивања узорака.			
33.3.	When exercising their powers under paragraph 2, point (d), (e) or (f), the competent authorities shall state the purpose of the request and specify the information requested.	3.16.1. 3.16.2.	Налог за инспекцијски надзор Члан 16. Руководилац инспекције или лице које он овласти издаје писани налог за инспекцијски надзор. Налог за инспекцијски надзор садржи: податке о инспекцији; податке о инспектору или инспекторима који врше инспекцијски надзор са бројевима службених легитимација; податке о надзираном субјекту или субјектима ако су познати, а ако ти подаци нису познати, односно ако није могуће утврдити надзиране субјекте или је њихов број превелик – одговарајуће познате информације од значаја за одређење субјекта, односно субјеката код којих ће се вршити надзор (нпр.: врста делатности или активности, територијално подручје, локација објекта, врста робе или производа, односно услуга итд.); правни основ инспекцијског надзора; навођење и кратко објашњење врсте и облика инспекцијског надзора; процењени ризик; прецизан и јасан опис предмета инспекцијског надзора; планирано трајање инспекцијског надзора (дан	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			почетка и окончања надзора); разлоге за изостављање обавештења, ако постоје; број, време и место издавања; потпис издаваоца налога; печат, када је то потребно према обележјима предмета инспекцијског надзора.			
33.4.	Member States shall ensure that the competent authorities, when exercising their enforcement powers in relation to important entities, have the power at least to: (a)issue warnings about infringements of this Directive by the entities concerned; (b)adopt binding instructions or an order requiring the entities concerned to remedy the deficiencies identified or the infringement of this Directive; (c)order the entities concerned to cease conduct that infringes this Directive and desist from repeating that conduct; (d)order the entities concerned to ensure that their cybersecurity risk-management measures comply with Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period; (e)order the entities concerned to inform the natural or legal persons with regard to which they provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat; (f)order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline; (g)order the entities concerned to make public aspects of infringements of this Directive in a specified manner; (h)impose, or request the imposition by the relevant bodies, courts or tribunals, in accordance with	1.48. 3.25. 3.26. 3.27. 3.28.	Овлашћења инспектора за информациону безбедност Члан 48. 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, конфигурацију и пенетрационо тестирање 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. Мере управљене према надзираном субјекту и њихова сразмерност Члан 25. Надзираном субјекту инспектор може изрећи управну меру, и то превентивну меру, меру за отклањање незаконитости, посебну меру наредбе, забране или заплене или меру за заштиту права трећих лица. Инспектор изриче оне мере које су сразмерне процењеном ризику и откривеним, односно	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

	national law, of an administrative fine pursuant to Article 34 in addition to any of the measures referred to in points (a) to (g) of this paragraph.		вероватним незаконитостима и штетним последицама, тако да се ризиком делотворно управља, и којима се најповољније по надзираног субјекта постижу циљ и сврха закона и другог прописа. Инспектор се обавезно стара о томе да мере из става 2. овог члана буду сразмерне економској снази надзираног субјекта, да се њихове штетне последице сведу на најмању меру и настави одрживо пословање и развој надзираног субјекта. Превентивне мере Члан 26. Инспектор у записнику одређује одговарајуће превентивне мере, ако је то потребно да би се спречио настанак незаконитости и штетних последица. Ако надзирани субјекат не поступи по превентивним мерама одређеним у записнику, инспектор изриче те мере решењем. Превентивне мере јесу: 1) упозоравање надзираног субјекта о његовим обавезама из закона и других прописа, као и о прописаним радњама и мерама управљеним према надзираном субјекту и санкцијама за поступања супротна тим обавезама; 2) указивање надзираном субјекту на могућност наступања штетних последица његовог пословања или поступања; 3) налагање надзираном субјекту предузимања или уздржавања од одређених радњи ради отклањања узрока вероватних штетних последица, као и одговарајућих мера предострожности у циљу спречавања настанка могућих штетних последица; 4) друге мере којима се постиже превентивна улога инспекцијског надзора. Превентивне мере могу се изрећи и непознатом субјекту инспекцијског надзора. Нерегистрованом субјекту се не може изрећи превентивна мера. Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или		

			поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости.			

			Посебне мере наредбе, забране и заплене Члан 28. Ако надзирани субјекат не отклони незаконитост у остављеном року, инспектор је овлашћен да донесе решење и изрекне меру којом, до отклањања незаконитости, надзираном субјекту забрањује обављање делатности или вршење активности или заплењује документацију, робу и друге предмете који су надзираном субјекту послужили за повреду прописа или су тиме настали. Инспектор је овлашћен да, без остављања рока за отклањање незаконитости, изрекне меру забране обављања делатности или вршења активности или заплене предмета или документације ако је неопходно да се, сагласно делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину веће вредности, права и интересе запослених и радно ангажованих лица, привреду, животну средину, биљни или животињски свет, јавне приходе веће вредности, несметан рад органа и организација, комунални ред или безбедност. Инспектор који забрани обављање делатности или вршење активности има право да нареди да се надзираном субјекту запечате пословне и производне просторије, објекти и други простор у коме обавља делатност или врши активност или који томе служи, постројења, уређаји, опрема, прибор, средства рада и други предмети којима обавља делатност или врши активност. Инспектор може изрећи и другу посебну меру наредбе, забране или заплене (нпр. мера повлачења или опозивања производа, мере ограничења, мера уништавања предмета, мера уклањања објекта и др), кад је то одређено посебним законом.			
33.5.	Article 32(6), (7) and (8) shall apply mutatis mutandis to the supervisory and enforcement measures provided for in this Article for important entities.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. овог закона;	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

		3.27. 3.35 3.36. 4.42. 4.43.	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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона.			

			За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до		

			500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и			

			прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости. Записник о инспекцијском надзору Члан 35. Инспектор сачињава записник о инспекцијском надзору. У записник се уносе: подаци из налога за инспекцијски надзор ако је издат; време и место инспекцијског надзора, а нарочито навођење основа и образложење разлога који су условили да се инспекцијски надзор врши ван радног времена надзираног субјекта у смислу члана 19. став 2. овог закона; опис предузетих радњи и попис преузетих докумената; подаци о броју узетих узорака и предлозима које у вези са узимањем узорака даје овлашћено лице надзираног субјекта; изјаве које су дате; опис других изведених доказа; захтеви за изузеће који су поднети; утврђено чињенично стање; констатација законитог пословања и поступања			

			надзираног субјекта; опис откривених незаконитости, са навођењем доказа на основу којег је одређена чињеница утврђена и правног основа за утврђивање незаконитости; мере које се изричу са навођењем правног основа на коме су засноване и роком за поступање по њима; одговарајућа образложења; обавеза надзираног субјекта да обавештава инспектора о поступању по мерама и рок за то обавештавање; подаци о поднетим кривичним пријавама, пријавама за привредни преступ и захтевима за покретање прекршајног поступка, ако су поднете, односно издатим прекршајним налозима, ако су издати, односно, у складу са чланом 42. став 3. овог закона, неподношење захтева за покретање прекршајног поступка, односно неиздавање прекршајног налога; подаци о другим мерама и радњама на које је инспектор овлашћен, ако су предузете; рок за давање примедаба на записник; навођење да је записник са или без примедаба прочитан лицу које присуствује надзору; други подаци и наводи од значаја за инспекцијски надзор. Контролна листа и анализа одговарајуће стручне институције, односно акредитованог тела чине саставни део записника. Овлашћено лице надзираног субјекта може да одбије да прими записник, што инспектор констатује у писаном облику и у записнику наводи разлоге због којих је пријем записника одбијен. Записник се доставља надзираном субјекту у року од осам дана од завршетка инспекцијског надзора. Општи образац записника о инспекцијском надзору прописује министар надлежан за послове државне управе. Општи образац записника о инспекцијском надзору за инспекцијски надзор из изворне надлежности аутономне покрајине и јединице локалне самоуправе прописује надлежни орган аутономне покрајине или јединице локалне самоуправе. Примедбе на записник			

			Члан 36. Надзирани субјекат има право да у писаном облику стави примедбе на записник о инспекцијском надзору, у року од пет радних дана од његовог пријема. Инспектор оцењује примедбе, све заједно и сваку засебно, и у међусобној вези. Инспектор може после тога да изврши допунски инспекцијски надзор, да би утврдио чињенице на које се примедбе односе. Ако су у примедбама на записник изнете нове чињенице и нови докази, због којих треба изменити чињенично стање које је утврђено у записнику или друкчије правне и друге оцене, инспектор о томе саставља допуну записника, на коју се не може ставити примедба. Поступајући по примедбама на записник, инспектор може да измени предложену или наложену, односно изречену меру или да одустане од ње. Одмеравање казне Члан 42. Казна за прекршаје одмерава се у границама које су за тај прекршај прописане, а при томе се узимају у обзир све околности које утичу да казна буде већа или мања, а нарочито: тежина и последице прекршаја, околности под којима је прекршај учињен, степен одговорности учиниоца, ранија осуђиваност, личне прилике учиниоца и држање учиниоца после учињеног прекршаја. Не може се узети у обзир као отежавајућа околност раније изречена прекршајна санкција учиниоцу ако је од дана правноснажности одлуке до дана доношења нове протекло више од четири године. При одмеравању висине новчане казне узеће се у обзир и имовно стање учиниоца. Ублажавање казне Члан 43. Ако се приликом одмеравања казне утврди да прекршајем нису проузроковане теже последице,		

			а постоје олакшавајуће околности које указују да се и блажом казном може постићи сврха кажњавања, прописана казна се може ублажити тако што се може: 1) изрећи казна испод најмање мере казне која је прописана за тај прекршај али не испод најмање законске мере те врсте казне; 2) уместо прописане казне затвора изрећи новчана казна или рад у јавном интересу, али не испод најмање законске мере те врсте казне; 3) уместо прописане казне затвора и новчане казне изрећи само једна од тих казни.			
33.6.	Member States shall ensure that their competent authorities under this Directive cooperate with the relevant competent authorities of the Member State concerned under Regulation (EU) 2022/2554. In particular, Member States shall ensure that their competent authorities under this Directive inform the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 when exercising their supervisory and enforcement powers aimed at ensuring compliance of an important entity that is designated as a critical ICT third-party service provider pursuant to Article 31 of Regulation (EU) 2022/2554. with this Directive.	3.5.	Сарадња са другим органима, имаоцима јавних овлашћења и правним и физичким лицима Члан 5. Сарадња надлежне инспекције са другим органима државне управе, органима аутономне покрајине и јединице локалне самоуправе, правосудним и другим државним органима и другим заинтересованим органима и организацијама остварује се у складу са надлежностима инспекције и облицима сарадње утврђеним прописима о државној управи и посебним законима. Сарадња, нарочито, обухвата међусобно обавештавање, размену података, пружање помоћи и заједничке мере и радње од значаја за инспекцијски надзор. Надлежна инспекција у обављању послова из свог делокруга усклађује планове инспекцијског надзора и свог рада, размењује податке, предлаже предузимање заједничких мера и активности од значаја за обављање послова инспекцијског надзора и на други начин сарађује са другим инспекцијама и субјектима са јавним овлашћењима који врше посебне облике надзора и контроле – ради обављања обухватнијег и делотворнијег инспекцијског надзора и нарочито ради сузбијања делатности или активности нерегистрованих субјеката. Државни органи, органи аутономне покрајине и јединице локалне самоуправе и имаоци јавних овлашћења дужни су, на захтев инспектора, да му у року од 15 дана од пријема захтева доставе тражене податке и обавештења који су значајни	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			за инспекцијски надзор. Надлежна инспекција, у складу са законом, сарађује са физичким и правним лицима, нарочито у циљу превентивног деловања, као и унапређења узајамне одговорности физичких и правних лица и инспекција у процесу примене и надзора над применом прописа. У том циљу, инспекција може одржавати информативне и едукативне трибине и консултативне састанке са представницима приватног сектора и другим заинтересованим странама. Физичка и правна лица могу инспекцији подносити представке и захтеве, и од ње тражити податке и обавештења, у складу са законом. Ако се у вези са вршењем инспекцијског надзора основано очекује да надзирани субјекат пружи отпор или се он пружи и инспектору онемогућава или битно отежава вршење инспекцијског надзора, инспектор може да захтева помоћ полиције и комуналне полиције. Полиција и комунална полиција пружају помоћ према законима којима се уређују полиција и комунална полиција.			
34.1.	***General conditions for imposing administrative fines on essential and important entities*** Member States shall ensure that the administrative fines imposed on essential and important entities pursuant to this Article in respect of infringements of this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case.	3.27.	Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости.			
34.2.	Administrative fines shall be imposed in addition to any of the measures referred to in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g).	3.27. 3.28.	Мере за отклањање незаконитости Члан 27. Ако открије незаконитост у пословању или поступању надзираног субјекта, инспектор му указује на незаконитост и опомиње га због тога, у складу са овлашћењима прописаним у посебном закону налаже или предлаже мере и оставља примерен рок за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, и то уноси у записник о инспекцијском надзору. Надзирани субјекат дужан је да писано обавести инспектора о томе да ли је у остављеном року предузео мере које су му наложене, односно предложене, отклонио незаконитост и штетне последице и испунио прописане обавезе, и ако јесте – инспектор окончава поступак у складу са чланом 37. став 2. овог закона. Ради утврђивања да ли су благовремено	ПУ	Имплементација ових одредби је осигурана применом инспекторских овлашћења на основу Закона о инспекцијском надзору.	

			предузете наложене, односно предложене мере, незаконитост и штетне последице отклоњене и прописане обавезе испуњене, инспектор је овлашћен да од надзираног субјекта тражи да уз обавештење из става 2. овог члана приложи документацију, односно други материјал (фотографије и др) из кога је видљиво да су утврђена незаконитост и њене штетне последице отклоњене, а прописане обавезе испуњене. Ако надзирани субјекат у остављеном року не предузме мере које су му наложене, односно предложене, не отклони незаконитост и штетне последице и не испуни прописане обавезе, инспектор доноси решење којим изриче мере за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза. Инспектор може без одлагања донети решење којим изриче мере за отклањање незаконитости, без претходног указивања на незаконитост и остављања рока за отклањање незаконитости и штетних последица и испуњавање прописаних обавеза, ако то налаже неопходност предузимања хитних мера ради спречавања или отклањања непосредне опасности по живот или здравље људи, животну средину или биљни или животињски свет. Инспектор може истовремено изрећи више мера за отклањање незаконитости. Посебне мере наредбе, забране и заплене Члан 28. Ако надзирани субјекат не отклони незаконитост у остављеном року, инспектор је овлашћен да донесе решење и изрекне меру којом, до отклањања незаконитости, надзираном субјекту забрањује обављање делатности или вршење активности или заплењује документацију, робу и друге предмете који су надзираном субјекту послужили за повреду прописа или су тиме настали. Инспектор је овлашћен да, без остављања рока за отклањање незаконитости, изрекне меру забране обављања делатности или вршења активности или заплене предмета или документације ако је неопходно да се, сагласно		

			делокругу инспекције, предузму хитне мере ради спречавања или отклањања непосредне опасности по живот или здравље људи, имовину веће вредности, права и интересе запослених и радно ангажованих лица, привреду, животну средину, биљни или животињски свет, јавне приходе веће вредности, несметан рад органа и организација, комунални ред или безбедност. Инспектор који забрани обављање делатности или вршење активности има право да нареди да се надзираном субјекту запечате пословне и производне просторије, објекти и други простор у коме обавља делатност или врши активност или који томе служи, постројења, уређаји, опрема, прибор, средства рада и други предмети којима обавља делатност или врши активност. Инспектор може изрећи и другу посебну меру наредбе, забране или заплене (нпр. мера повлачења или опозивања производа, мере ограничења, мера уништавања предмета, мера уклањања објекта и др), кад је то одређено посебним законом.			
34.3.	When deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in Article 32(7).	4.42. 4.43.	Одмеравање казне Члан 42. Казна за прекршаје одмерава се у границама које су за тај прекршај прописане, а при томе се узимају у обзир све околности које утичу да казна буде већа или мања, а нарочито: тежина и последице прекршаја, околности под којима је прекршај учињен, степен одговорности учиниоца, ранија осуђиваност, личне прилике учиниоца и држање учиниоца после учињеног прекршаја. Не може се узети у обзир као отежавајућа околност раније изречена прекршајна санкција учиниоцу ако је од дана правноснажности одлуке до дана доношења нове протекло више од четири године. При одмеравању висине новчане казне узеће се у обзир и имовно стање учиниоца. Ублажавање казне Члан 43. Ако се приликом одмеравања казне утврди да	ПУ		

			прекршајем нису проузроковане теже последице, а постоје олакшавајуће околности које указују да се и блажом казном може постићи сврха кажњавања, прописана казна се може ублажити тако што се може: 1) изрећи казна испод најмање мере казне која је прописана за тај прекршај али не испод најмање законске мере те врсте казне; 2) уместо прописане казне затвора изрећи новчана казна или рад у јавном интересу, али не испод најмање законске мере те врсте казне; 3) уместо прописане казне затвора и новчане казне изрећи само једна од тих казни.			
34.4.	Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51.	ДУ	Овакав начин обрачуна није могућ према општим прописима о прекршајима, укључујући и максималне казне које се смеју прописати правним и физичким лицима посебним законима.	

			Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог			

			закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			

34.5.	Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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	ДУ	Овакав начин обрачуна није могућ према општим прописима о прекршајима, укључујући и максималне казне које се смеју прописати правним и физичким лицима посебним законима.	

			5) не изврши проверу усклађености примењених мера из члана 12. став 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
34.6.	Member States may provide for the power to impose periodic penalty payments in order to compel an essential or important entity to cease an infringement of this Directive in accordance with a prior decision of the competent authority.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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;	ПУ		

			5) не изврши проверу усклађености примењених мера из члана 12. став 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који			

			је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
34.7.	Without prejudice to the powers of the competent authorities pursuant to Articles 32 and 33, each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public administration entities.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који	ПУ		

			је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које			

			је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
34.8.	Where the legal system of a Member State does not provide for administrative fines, that Member State shall ensure that this Article is applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts or tribunals, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by the competent authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. The Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by 17 October 2024 and, without delay, any subsequent amendment law or amendment affecting them.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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;	ПУ		

			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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од		

			5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
35.1.	***Infringements entailing a personal data breach*** Where the competent authorities become aware in the course of supervision or enforcement that the infringement by an essential or important entity of the obligations laid down in Articles 21 and 23 of this Directive can entail a personal data breach, as defined in Article 4, point (12), of Regulation (EU) 2016/679 which is to be notified pursuant to Article 33 of that Regulation, they shall, without undue delay, inform the supervisory authorities as referred	5.52. 5.53.	Обавештавање Повереника о повреди података о личности Члан 52. Руковалац је дужан да о повреди података о личности која може да произведе ризик по права и слободе физичких лица обавести Повереника без непотребног одлагања, или, ако је то могуће, у року од 72 часа од сазнања за повреду. Ако руковалац не поступи у року од 72 часа од сазнања за повреду, дужан је да образложи разлоге због којих није поступио у том року.	ПУ	Применом режима заштите података о личности и прописивањм начина и сврхе обраде података о личности овим законом.	

	to in Article 55 or 56 of that Regulation.		Обрађивач је дужан да, после сазнања за повреду података о личности, без непотребног одлагања обавести руковаоца о тој повреди. Обавештење из става 1. овог члана мора да садржи најмање следеће информације: 1) опис природе повреде података о личности, укључујући врсте података и приближан број лица на која се подаци те врсте односе, као и приближан број података о личности чија је безбедност повређена; 2) име и контакт податке лица за заштиту података о личности или информације о другом начину на који се могу добити подаци о повреди; 3) опис могућих последица повреде; 4) опис мера које је руковалац предузео или чије је предузимање предложено у вези са повредом, укључујући и мере које су предузете у циљу умањења штетних последица. Ако се све информације из става 4. овог члана не могу доставити истовремено, руковалац без непотребног одлагања поступно доставља доступне информације. Руковалац је дужан да документује сваку повреду података о личности, укључујући и чињенице о повреди, њеним последицама и предузетим мерама за њихово отклањање. Документација из става 6. овог члана мора омогућити Повереник да утврди да ли је руковалац поступио у складу са одредбама овог члана. Ако се ради о повреди података о личности које обрађују надлежни органи у посебне сврхе, а који су пренети руковаоцу у другој држави или међународној организацији, руковалац је дужан да без непотребног одлагања достави информације из става 4. овог члана руковаоцу у тој другој држави или међународној организацији, у складу са међународним споразумом. Повереник прописује образац обавештења из става 1. овог члана и ближе уређује начин обавештавања. Обавештавање лица о повреди података о		

			личности Члан 53. Ако повреда података о личности може да произведе висок ризик по права и слободе физичких лица, руковалац је дужан да без непотребног одлагања о повреди обавести лице на које се подаци односе. У обавештењу из става 1. овог члана руковалац је дужан да на јасан и разумљив начин опише природу повреде података и наведе најмање информације из члана 52. став 4. тач. 2) до 4) овог закона. Руковалац није дужан да обавести лице из става 1. овог члана ако: 1) је предузео одговарајуће техничке, организационе и кадровске мере заштите у односу на податке о личности чија је безбедност повређена, а посебно ако је криптозаштитом или другим мерама онемогућио разумљивост података свим лицима која нису овлашћена за приступ овим подацима; 2) је накнадно предузео мере којима је обезбедио да повреда података о личности са високим ризиком за права и слободе лица на које се подаци односе више не може да произведе последице за то лице; 3) би обавештавање лица на које се подаци односе представљало несразмеран утрошак времена и средстава. У том случају, руковалац је дужан да путем јавног обавештавања или на други делотворан начин обезбеди пружање обавештења лицу на које се подаци односе. Ако руковалац није обавестио лице на које се подаци односе о повреди података о личности, Повереник може, узимајући у обзир могућност да повреда података произведе висок ризик, да наложи руковаоцу да то учини или може да утврди да су испуњени услови из става 3. овог члана. Ако се ради о повреди података о личности које обрађују надлежни органи у посебне сврхе, руковалац може одложити или ограничити обавештавање лица на које се подаци односе, у складу са условима и на основу разлога из члана 25. став 3. овог закона.			

35.2.	Where the supervisory authorities as referred to in Article 55 or 56 of Regulation (EU) 2016/679 impose an administrative fine pursuant to Article 58(2), point (i), of that Regulation, the competent authorities shall not impose an administrative fine pursuant to Article 34 of this Directive for an infringement referred to in paragraph 1 of this Article arising from the same conduct as that which was the subject of the administrative fine under Article 58(2), point (i), of Regulation (EU) 2016/679. The competent authorities may, however, impose the enforcement measures provided for in Article 32(4), points (a) to (h), Article 32(5) and Article 33(4), points (a) to (g), of this Directive.	4.8.	Забрана поновног суђења у истој ствари Члан 8. Никоме се не може поново судити нити му може поново бити изречена прекршајна санкција за прекршај о коме је правноснажно одлучено у складу са законом. Забрана из става 1. овог члана не спречава понављање прекршајног поступка у складу са овим законом. Против учиниоца прекршаја који је у кривичном поступку правноснажно оглашен кривим за кривично дело које обухвата и обележја прекршаја не може се за тај прекршај покренути поступак, а ако је покренут или је у току, не може се наставити и довршити. Против учиниоца прекршаја који је у поступку по привредном преступу правноснажно оглашен одговорним за привредни преступ који обухвата и обележја прекршаја не може се за тај прекршај покренути поступак, а ако је покренут или је у току, не може се наставити и довршити.	ПУ		
35.3.	Where the supervisory authority competent pursuant to Regulation (EU) 2016/679 is established in another Member State than the competent authority, the competent authority shall inform the supervisory authority established in its own Member State of the potential data breach referred to in paragraph 1.	5.72.	Међународна сарадња у вези са заштитом података о личности Члан 72. Повереник предузима одговарајуће мере у односима са органима надлежним за заштиту података о личности у другим државама и међународним организацијама у циљу: 1) развоја механизама међународне сарадње за олакшавање делотворне примене закона који се односе на заштиту података о личности; 2) обезбеђивања међународне узајамне помоћи у примени закона који се односе на заштиту података о личности, укључујући и обавештавање, упућивање на поступке заштите и правне помоћи у вршењу надзора, као и размену информација, под условом да су предузете одговарајуће мере заштите података о личности и основних права и слобода; 3) ангажовања заинтересованих страна у расправама и активностима које су усмерене на развој међународне сарадње у примени закона који се односе на заштиту података о личности; 4) подстицања и унапређивања размене	ПУ		

			информација о законодавству које се односи на заштиту података о личности и његовој примени, укључујући и питања сукоба надлежности са другим државама у овој области.			
36.1.	***Penalties*** Member States shall lay down rules on penalties applicable to infringements of national measures adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 17 January 2025, notify the Commission of those rules and of those measures and shall notify it, without delay of any subsequent amendment affecting them.	1.50. 1.51. 1.52. 1.53.	Члан 50. Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. 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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 51. Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система од посебног значаја ако: 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. овог закона; 2) не донесе Акт о процени ризика из члана 11. став 1. овог закона;	ДУ	Казне су прописане у складу са ограничењима која су успостављена општим прописима о прекршајима.	

			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 5. 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 48. став 1. тачка 1) овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Члан 52. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног 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 инцидента из члана 24. овог закона; За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 500.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који			

			је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст. 1 - 3. 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 53. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног 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 инцидента из члана 24 овог закона. За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система од посебног значаја новчаном казном у износу од 10.000,00 до 250.000,00 динара. За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.			
37.1.- 37.2.	***Mutual assistance*** Where an entity provides services in more than one Member State, or provides services in one or more Member States and its network and information systems are located in one or more other Member States, the competent authorities of the Member States concerned shall cooperate with and assist each other as necessary. That cooperation shall			НП	Обавезе држава чланица	

	entail, at least, that: (a)the competent authorities applying supervisory or enforcement measures in a Member State shall, via the single point of contact, inform and consult the competent authorities in the other Member States concerned on the supervisory and enforcement measures taken; (b)a competent authority may request another competent authority to take supervisory or enforcement measures; (c)a competent authority shall, upon receipt of a substantiated request from another competent authority, provide the other competent authority with mutual assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner. The mutual assistance referred to in the first subparagraph, point (c), may cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits. A competent authority to which a request for assistance is addressed shall not refuse that request unless it is established that it does not have the competence to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authority, or the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of the Member State's national security, public security or defence. Before refusing such a request, the competent authority shall consult the other competent authorities concerned as well as, upon the request of one of the Member States concerned, the Commission and ENISA. Where appropriate and with common agreement, the competent authorities of various Member States may carry out joint supervisory actions.					

38.1.-38.6.	***Exercise of the delegation*** The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. The power to adopt delegated acts referred to in Article 24(2) shall be conferred on the Commission for a period of five years from 16 January 2023. The delegation of power referred to in Article 24(2) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council. A delegated act adopted pursuant to Article 24(2) shall enter into force only if no objection has been expressed either by the European Parliament or by the Council within a period of two months of notification of that act to the European Parliament and to the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.			НП	Прелазне и завршне одредбе	
39.1.-39.3.	***Committee procedure*** The Commission shall be assisted by a committee. That committee shall be a committee within the			НП	Прелазне и завршне одредбе	

	meaning of Regulation (EU) No 182/2011. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. Where the opinion of the committee is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a committee member so requests.					
40.1.	***Review*** By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council. The report shall in particular assess the relevance of the size of the entities concerned, and the sectors, subsectors and types of entity referred to in Annexes I and II for the functioning of the economy and society in relation to cybersecurity. To that end and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. The report shall be accompanied, where necessary, by a legislative proposal.			НП	Прелазне и завршне одредбе	
41.1- 41.2.	***Transposition*** By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 18 October 2024. When Member States adopt the measures referred to in paragraph 1, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.			НП	Прелазне и завршне одредбе	

42.-46.	***Amendment of Regulation (EU) No 910/2014*** In Regulation (EU) No 910/2014, Article 19 is deleted with effect from 18 October 2024. ***Amendment of Directive (EU) 2018/1972*** In Directive (EU) 2018/1972, Articles 40 and 41 are deleted with effect from 18 October 2024. ***Repeal*** Directive (EU) 2016/1148 is repealed with effect from 18 October 2024. References to the repealed Directive shall be construed as references to this Directive and shall be read in accordance with the correlation table set out in Annex III. ***Entry into force*** This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. ***Addressees*** This Directive is addressed to the Member States.			НП	Прелазне и завршне одредбе	
ANNEX I	SECTORS OF HIGH CRITICALITY	1.5.	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:	ПУ		

			(1) Енергетика - производња електричне енергије, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - комбинована производња електричне и топлотне енергије; - снабдевање електричном енергијом; - пренос електричне енергије и управљање преносним системом; - дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом; - складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика; - 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 и производња нафте и природног гаса; - производња деривата нафте; - складиштење нафте и деривата нафте; - транспорт и управљање транспортним системом за природни гас; - складиштење и управљање складиштем природног гаса; - дистрибуција и управљање дистрибутивним системом за природни гас; - снабдевање и јавно снабдевање природним гасом; - производња и прерада угља; - 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; - сервис за управљање бродским саобраћајем (VTS); - речни информациони сервиси (RIS); - управљање путном инфраструктуром; - управљање интелигентним транспортним системима (ИТС). (3) Банкарство и финансијска тржишта - послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно 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 односно салдирања 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 фармацеутских лекова и препарата намењених за здравствену употребу; - производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја 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; - пружање услуга мреже за испоруку садржаја; - 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.			
ANNEX II	OTHER CRITICAL SECTORS	1.6.	Оператори важних ИКТ система од посебног значаја Члан 6. Оператори важних ИКТ система од посебног	ПУ		

			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; - управљање амбалажним отпадом, у смислу закона којим се уређује управљање амбалажним отпадом; - производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије; - производња, прерада 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 послове информационе безбедности. Министарства у чијим надлежностима су области у којима оператори приоритетних и важних ИКТ система од посебног значаја обављају делатности, 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.			
ANNEX III	CORRELATION TABLE			НП		