**ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖИ И ИНФОРМАЦИСКИ СИСТЕМИ**

## **Предмет**

## **Член 1**

(1) Со овој закон се определуваат мерките за безбедност на мрежи и информациски системи, безбедносните услови и известувања за инциденти на мрежи и информациски системи кои треба да бидат исполнети како услови од страна на операторите на суштинските услуги и од давателите на дигитални услуги.

(2) Со овој закон се уредува стратешката соработка и размената на информации, координацијата на тимовите за одговор на компјутерски инциденти, како и обврските на единствената точка за контакт и на тимовите за одговор на компјутерски безбедносни инциденти.

(3) Со овој закон се основа мрежата за одговор на компјутерски инциденти и Дигиталната агенција на Република Северна Македонија.

(4) Со овој закон се определува начинот на управување со Националната транспортна оптичка мрежа, начинот на управување со податочниот центар, како и начинот на обезбедување и управување со услугите во облак за потребите на државните органи.

## **Цел**

## **Член 2**

(1) Целта на овој закон е обезбедување високо заедничко ниво на безбедност и заштита на мрежи и информациски системи заради непрекинато функционирање на внатрешниот пазар, превенција на сајбер безбедносни инциденти или кризи, како и развој на брза и ефективна оперативна соработка за заштита на мрежи и информациски системи.

(2) Целта на овој закон е идентификување на секторите кои обезбедуваат суштински услуги и дигитални услуги, заради заштита на нивните мрежи и информациски системи.

(3) Целта на овој закон е обезбедување на сигурност при користењето на транспортната оптичка мрежа, високо ниво на безбедност на податоците создадени од државните органи, како и обезбедување на услови за безбедно користење на услуги за обработка во облак за потребите на државните органи.

## **Примена на законот**

## **Член 3**

(1) Одредбите на овој закон се применуваат на работата на органите на државната управа и единиците на локалната самоуправа, судовите, јавните обвинителства и државното правобранителство и правни лица на кои со закон им е доверено да вршат јавни овластувања.

(2) Одредбите на овој закон се применуваат и на работата на правни лица кои обезбедуваат услуги од секторите:

- енергетика,

- транспорт,

- банкарство,

- финансиски пазар,

- здравство,

- снабдување на вода за пиење и дистрибуција,

- дигитална инфраструктура.

(3) Овој закон не се применува на операторите на јавна електронска комуникациска мрежа определени со Законот за електронските комуникации и давателите на доверливи услуги определени со Законот за електронски документи, електронска идентификација и доверливи услуги.

(4) Директорот на Дигиталната агенција утврдува листа на потсектори кои се опфатени во рамки на секторите утврдени со ставот (2) на овој член.

## **Обработка на лични податоци и размена на класифицирани информации**

## **Член 4**

(1) Обработката и користењето на личните податоци се врши согласно прописите од областа на заштитата на личните податоци.

(2) Класифицираните информации се разменуваат со надлежните домашни и меѓународни органи единствено кога таквата размена е неопходна за примената на овој закон.

(3) Во случаите од ставот (2) на овој член, се смета дека обемот на размената на класифицираните информации е ограничен и пропорционален на целта заради којашто се врши размената.

(4) Разменетите класифицирани информации го задржуваат степенот на доверливоста, а надлежните органи се должни да преземат мерки со кои ќе ги заштитат безбедносните и комерцијалните интереси на операторите на суштинските услуги и на давателите на дигитални услуги.

## **Дефиниции**

## **Член 5**

Изразите употребени во овој закон го имаат следното значење:

1) **„мрежен и информациски систем“** е:

(a) електронска комуникациска мрежа определена согласно одредбите од Законот за електронските комуникации;

(б) секој уред или група уреди меѓусебно поврзани или сродни уреди, од кои еден или повеќе од тие уреди вршат автоматска обработка на дигитални податоци со користење на одредена програма или

(в) дигитални податоци складирани, обработени, преземени или пренесени од елементи опфатени под точките (а) и (б) за целите на нивното работење, употреба, заштита и одржување,

2) **„безбедност на мрежи и информациски системи“** значи способност на мрежните и информациските системи, на одредено ниво на доверба, да се спротивстават на какво било дејство кое ја компромитира достапноста, автентичноста, интегритетот или доверливоста на складираните или пренесените или обработените податоци или поврзаните услуги што ги нудат или се достапни преку тие мрежи и информациски системи,

3) **„Национална стратегија за безбедност на мрежите и информациските системи“** значи рамка која обезбедува стратешки цели и приоритети за безбедност на мрежите и информациските системи на национално ниво,

4) **„оператор на суштински услуги“** значи јавен или приватен субјект, кој ги исполнува критериумите утврдени во член 6 став (2) од овој закон,

5) **„дигитална услуга“** е секоја услуга на информатичкото општество, односно секоја услуга што вообичаено се обезбедува за надомест, на далечина, со користење на електронски средства и на индивидуално барање на корисникот на услугата,

6) **„давател на дигитални услуги“** е секое правно лице кое обезбедува дигитална услуга,

7) **„инцидент“** е настан кој може да предизвика реален негативен ефект врз безбедноста на мрежите и информациските системи,

8) **„справување со инциденти“** се сите постапки и мерки за поддршка на откривање, анализа на инцидент и ограничување на неговото влијание, како и одговор на инцидент,

9) **„ризик“** е секоја разумно идентификувана околност или настан што може да има потенцијален негативен ефект врз безбедноста на мрежните и информациските системи,

10) **„претставник“** е секое физичко или правно лице од Република Северна Македонија или од земја членка на Европската Унија, експлицитно назначено да дејствува во име на давател на дигитални услуги кој не е основан во Република Северна Македонија или во земја членка на Европската Унија, на кое може да му се обрати надлежен орган или надлежен тим за одговор на компјутерски безбедносни инциденти наместо на давателот на дигитални услуги во однос на обврските на што тој давател на дигитални услуги треба да ги исполни, во согласност со овој закон или со Директивата (ЕУ) 2016/1148 во однос на мерки за високо заедничко ниво на безбедност на мрежите и информациските системи низ Унијата,

11) **„спецификациjа“** е документ што пропишува технички услови што треба да ги исполни производ, процес, услуга или систем и кој утврдува едно или повеќе од следниве:

(а) потребните карактеристики на производот, вклучително и нивоа на квалитет, перформанси, интероперабилност, заштита на животната средина, здравје, безбедност или димензии и вклучување на барањата што се применуваат на производот во врска со името под кое се продава производот, терминологија, симболи, тестирање и тест постапки, пакување, обележување или обележување и процедури за проценка на сообразност;

(б) методите и процесите на производство што се користат во однос на земјоделските производи, производи наменети за исхрана на луѓето и животните и медицинските производи, како и методите и процесите на производство што се однесуваат на други производи, кога тие влијаат на нивните карактеристики;

(в) потребните карактеристики на услугата, вклучително и нивоа на квалитет, перформанси, интероперабилност, заштита на животната средина, здравје или безбедност и вклучување на барањата што се применуваат за давателот на услуги во врска со информациите што му се ставаат на располагање на корисникот;

(г) методите и критериумите за проценка на перформансите на градежните производи, во однос на нивните основни карактеристики;

12) **„точка за размена на интернет“** е мрежна структура која овозможува поврзување на повеќе од два независни автономни системи, првенствено заради олеснување на размената на интернет сообраќај или точка која обезбедува интерконекција само за автономни системи. За точката за размена на интернет не е потребно интернет-сообраќајот што поминува помеѓу кој било пар на автономни системи што учествуваат, да помине низ кој било трет автономен систем, ниту пак го менува или на друг начин го попречува таквиот сообраќај (во натамошниот текст: IXP),

13) **„домен“** е дел од хиерархиски систем на имиња на адреси на интернет што споделуваат заеднички суфикс и се под контрола на одредена организација;

14) **„систем за имиња на домени“** е хиерархиски дистрибуиран систем за определување на имиња на домени во мрежа (во натамошниот текст: DNS),

15) **„давател на DNS-услуги“** e субјект кој обезбедува DNS-услуги на интернет,

16) **„регистар на имиња на домени од највисоко ниво“** е субјект кој управува и раководи со регистрацијата на имиња на интернет-домени под одреден домен од највисоко ниво (во натамошниот текст: TLD),

17) **„он-лајн пазар“** значи дигитална услуга што им овозможува на потрошувачите и/или трговците, да склучуваат он-лајн договори за продажба или за услуги со трговци, преку веб-страницата на он-лајн пазарот или преку веб-страницата на трговецот што користи компјутерски услуги кои ги нуди на он-лајн пазарот,

18) **„он-лајн пребарувач“** е вид на дигитална услуга која на корисниците им овозможува да вршат пребарување на било која тема на сите веб-страници или на веб-страници на одреден јазик, врз основа на клучен збор, фраза или друг внес, при што враќа линкови во кои може да се најдат информации поврзани со бараната содржина,

19) **„услуга за обработка во облак“** е дигитална услуга која овозможува пристап до надградлив и флексибилен збир на разменливи компјутерски ресурси,

20) **„тим за одговор на компјутерски безбедносни инциденти“** е посебна организациска единица формирана во рамки на надлежен орган за секторите определени во член 3 став (2) на овој закон надлежна за преземање на соодветни постапки и мерки за поддршка на откривање, анализа на инцидент и ограничување на неговото влијание, како и одговор на инцидент кој би можел да настане во рамки на конкретниот сектор (во натамошниот текст: CSIRT),

21) **„****Национален центар за одговор на компјутерски инциденти“** е посебна организациска единица формирана во рамки на Дигиталната агенција на Република Северна Македонија, заради:

- координација на секторските CSIRT и мерките во нивна надлежност при справување со безбедносни инциденти на мрежите и информациските системи кои би можеле да имаат влијание врз мрежите и информациските системи на два или повеќе сектори и

- национален центар за контакт и одговор на безбедносни инциденти и ризици на мрежите и информациските системи во државата (во натамошниот текст: MKD-CSIRT).

22) **сајбер безбедност** е систем на активности и мерки потребни за заштита на мрежни и информациски системи, корисниците на таквите системи и други лица погодени од закани преку компјутерски мрежи;

23) **сајбер закана** е секоја потенцијална околност, настан или активност што може да оштети, наруши или на друг начин негативно влијание врз мрежата и информациските системи, корисниците на таквите системи и други лица;

24) **Национална транспортна оптичка мрежа** во смисла на овој закон е електронска комуникациска мрежа составена од физичка инфраструктура и активна опрема и други придружни средства

преку кои се овозможува поставување на оптичка инфраструктура на која по претходно одбрение од Дигиталната агенција се приклучени државните органи.

а) активна опрема и други придружни средства се компоненти со која се овозможува емитирање, прием или обработка на сигнали преку оптичките влакна.

25) **Податочен центар** е централизиран физички простор во кој се поставени компјутерски сервери и компјутерски компоненти, а кои се користат за далечинско складирање, обработка или дистрибуција на податоци и документи.

**Оператори на суштински услуги**

**Член 6**

(1) Тимовите за одговор на компјутерски безбедносни инциденти се одговорни за идентификување на операторите на суштински услуги во рамки на секторот за кој се надлежни, согласно член 11 став (2) од овој закон.

(2) Критериуми за идентификување на операторите на суштински услуги се:

- правно лице кое обезбедува услуга што е неопходна за одржување на критични општествени или економски активности;

- услугата што ја обезбедува да зависи од мрежни и информациски системи и

- доколку настане инцидент истиот може да предизвика значителни подривачки ефекти врз обезбедувањето на услугата од страна на правното лице.

(3) Тимовите за одговор на компјутерски безбедносни инциденти за секторот за кој се надлежни воспоставуваат листа на оператори на суштински услуги, во која се содржани и услугите кои ги обезбедуваат.

(4) Тимовите за одговор на компјутерски безбедносни инциденти листата од ставот (3) на овој член се должни редовно да ја ажурираат, а најмалку еднаш на секои две години.

(5) Тимовите за одговор на компјутерски безбедносни инциденти при секое ажурирање на листата од ставот (3) на овој член, а најмалку еднаш на секои две години до Националниот центар за одговор на компјутерски инциденти доставуваат Извештај за идентификација на оператори на суштински услуги, кој содржи:

- мерки за идентификација на операторите на суштинските услуги;

- компаративни портфолија за операторите на суштински услуги запишани во листата ставот (3) на овој член;

- бројот на оператори на суштински услуги идентификувани во секторот и индикација за нивното значење во однос на тој сектор;

- прагови преку кои може да се утврди релевантното ниво на корисници на услугата со наведување на бројот на корисници на услугата или индикации за важноста на секој оператор на суштински услуги.

**Даватели на дигитални услуги**

**Член 7**

(1) Даватели на дигитални услуги се правни лица кои обезбедуваат дигитални услуги и тоа:

- он-лајн пазар,

- он-лајн пребарувач,

- услуги за обработка во облак.

(2) Микро и мали претпријатија не се сметаат за даватели на дигитални услуги.

(3) Надлежен тим за одговор на компјутерски безбедносни инциденти (CSIRT) за давателите на дигитални услуги е тимот за одговор на компјутерски безбедносни инциденти (CSIRT) за секторот дигитална инфраструктура, односно организациската единица формирана во Дигиталната агенција.

**Значителен подривачки ефект**

**Член 8**

(1) При утврдување на значењето на нарушувањето на безбедноста, односно при утврдување на значителен подривачки ефект, задолжително се утврдува и влијанието на следните фактори:

- бројот на корисници кои ја користат услугата што ја обезбедува засегнатиот оператор на суштински услуги;

- зависноста и поврзаноста со другите сектори со секторот во кој засегнатиот оператор на суштински услуги ја обезбедува услугата;

- влијанието што потенцијалниот инцидент може да го има, односно степен и времетраење на инцидентот и неговото влијание врз економските или општествените активности или врз јавната безбедност;

- пазарниот удел на операторот на суштинска услуга;

- географската распространетост во однос на подрачјето што би можело да биде зафатено од потенцијалниот инцидент;

- значењето на операторот на суштинската услуга во однос на обезбедување на доволно ниво на услугата, земајќи ја предвид достапноста на алтернативни средства за обезбедување на таа услуга.

(2) Со цел да се утврди дали одреден инцидент може да предизвика значителен подривачки ефект, задолжително се земаат во предвид и специфичните фактори за секторот во кој се обезбедува суштинската услуга во која може да настане инцидентот.

**Национална стратегија за безбедност на мрежи и информациски системи**

**Член 9**

(1) Владата на Република Северна Македонија на предлог на Дигиталната агенција донесува Национална стратегија за безбедност на мрежи и информациски системи, односно Национална стратегија за сајбер безбедност, на секои две години.

(2) Со националната стратегија од ставот (1) на овој член се дефинираат стратешките цели и соодветни политики и регулаторни мерки со цел да се постигне и одржи високо ниво на безбедност на мрежните и информациските системи и мерки за обезбедување на сигурност во секторите во кои се обезбедуваат суштински услуги.

(3) Националната стратегија од ставот (1) на овој член ги опфаќа особено:

- целите и приоритетите за безбедност на мрежните и информациските системи;

- управувувачка рамка за постигнување на целите и приоритетите на националната стратегија за безбедност на мрежните и информациските системи, вклучувајќи ги улогите и одговорностите на надлежните органи и другите засегнати страни;

- идентификација на мерки поврзани со подготвеност, одговор и закрепнување од инциденти, вклучувајќи соработка помеѓу јавниот и приватниот сектор;

- наведување програми за едукација и програми за подигнување на јавната свест и обука, кои се однесуваат на стратегијата;

- планови за истражување и развој на безбедност на мрежните и информациските системи;

- план за проценка на ризици со идентификација на ризиците;

- листа на различни засегнати страни вклучени во спроведувањето на стратегијата.

(4) Владата на Република Северна Македонија е должна да ја достави Националната стратегија за безбедност на мрежи и информациски системи до Европската Комисија, најдоцна во рок од три месеци од нејзиното донесување.

(5) При доставата на Националната стратегија за безбедност на мрежи и информациски системи во Европската Комисија, Владата може да ги исклучи елементите од стратегијата што се однесуваат на националната безбедност.

**Единствена точка за контакт**

**Член 10**

(1) Функцијата на единствена точка за контакт за безбедност на мрежни и информациски системи ја врши Дигиталната агенција.

(2) Единствената точка за контакт е надлежна за прекугранична соработка од областа на сајбер безбедноста.

(3) Единствената точка за контакт обезбедува прекугранична соработка со надлежните телата на земјите членки на Европската унија, со надлежните органи на унијата и со Групата за соработка, во согласност со член 13 и член 14 од овој закон.

(4) Единствената точка за контакт е должна при воспоставување и обезбедување на меѓународна соработка да се консултира и да соработува со органите надлежни за спроведување на овој закон и со надлежните органи за заштита на податоци.

(5) Владата на Република Северна Македонија е должна да ја извести Европската Комисија за надлежностите на единствената точка за контакт, како и за секоја промена во однос на надлежниот орган за вршење на функцијата единствена точка за контакт или за надлежностите на единствената точка за контакт.

**Тимови за одговор на компјутерски безбедносни инциденти (CSIRT)**

**Член 11**

(1) Тим за одговор на компјутерски безбедносни инциденти(CSIRT)е посебна организациска единица формирана во рамки на надлежен орган за секторите:

- енергетика,

- транспорт,

- банкарство,

- финансиски пазар,

- здравство,

- снабдување на вода за пиење и дистрибуција,

- дигитална инфраструктура.

(2) Надлежни органи во кои се формираат тимови за одговор на компјутерски безбедносни инциденти се:

- Агенција за енергетика-за секторот енергетика;

- Акционерското друштво за контрола на летање М-НАВ- за секторот транспорт, за воздушен транспорт;

- Агенцијата за железнички систем- за секторот транспорт, за железнички транспорт и

- Министерството за транспорт и врски- за секторот транспорт, за воден и копнен транспорт;

- Народна банка на Република Северна Македонија- за секторот банкарство;

- Министерството за финансии- за секторот финансиски пазар;

- Управата за електронско здравство- за секторот здравство;

- Акционерското друштво „Водостопанство“ на Република Северна Македонија- за секторот снабдување на вода за пиење и дистрибуција;

- Дигиталната агенција- за секторот дигитална инфраструктура и за давателите на дигитални услуги.

(3) Тимовите за одговор на компјутерски безбедносни инциденти треба да имаат пристап до соодветна, безбедна и флексибилна комуникациска и информациска инфраструктура на национално ниво.

(4) Владата на Република Северна Македонија е должна да ја информира Европската комисија за надлежностите, како и за главните елементи на процесот на справување со инциденти на секторските тимови за одговор на компјутерски безбедносни инциденти.

(5) Во Дигиталната агенција се формира посебна организациска единица за Национален центар за одговор на компјутерски инциденти (MKD CSIRT) и посебна организациска единица за Тим за одговор на компјутерски безбедносни инциденти на Владата на Република Северна Македонија (во натамошниот текст: G CSIRT).

**Надлежности на тимовите за одговор на компјутерски безбедносни инциденти (CSIRT)**

**Член 12**

(1) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) се надлежни за:

1) следење на инциденти на национално ниво во рамки на секторот за кој се надлежни;

2) рано предупредување, известувања, соопштенија и пренос на информации до засегнатите страни од ризиците и инцидентите;

3) одговор на инциденти;

4) обезбедување динамична анализа на ризик и инциденти и ситуациона свест.

(2) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) се должни да учествуваат во мрежата на CSIRTови.

(3) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) се должни да воспостават односи на соработка со приватниот сектор.

(4) Заради олеснување на соработката, CSIRTовите го промовираат усвојувањето и користењето заеднички или стандардизирани практики за:

- постапки за справување со инциденти и ризици;

- шеми за класификација на инциденти, ризици и информации.

(5) Условите за работа на тимовите за одговор на компјутерски безбедносни инциденти ги пропишува министерот за информатичко општество и администрација.

**Обврска за соработка на тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) и Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT)**

**Член 13**

(1) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) и Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT) се должни да соработуваат во однос на исполнувањето на обврските утврдени во овој закон.

(2) Во случај кога тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) не добиле известување за компјутерски инцидент, а истиот е настанат, тогаш надлежниот тим за одговор на компјутерски безбедносни инциденти (CSIRT) добива пристап до податоци за инциденти за кои известиле операторите на суштинските услуги, во согласност со член 15 став (4) и став (5) или давателите на дигитални услуги, во согласност со член 17 став (4) и став (5) од овој закон, до степен што е неопходен за исполнување на своите надлежности.

(3) Надлежниот тим за одговор на компјутерски безбедносни инциденти (CSIRT)

е должен да го информира Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) за известувањата за инциденти добиени или прибавени во согласност со одредбите од овој закон.

**Надлежност на Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT)**

**Член 14**

(1) Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT) е посебна организациска единица во рамки на Дигиталната агенција која е надлежна за:

- координација на секторските CSIRT-ови и мерките во нивна надлежност при справување со безбедносни инциденти на мрежите и информациските системи кои би можеле да имаат влијание врз мрежите и информациските системи на два или повеќе сектори,

- одговор на безбедносни инциденти и ризици на мрежите и информациските системи на државата и

- донесување на имплементациски акти за оценување на дополнителните елементи наведени во член 17 став (2) и параметрите наведени во член 17 став (6) од овој член.

(2) Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT) подготвува годишен извештај најдоцна до 1 март во тековната година за претходната година за добиените известувања, вклучувајќи го бројот на известувања и природата на пријавените инциденти и активностите преземени во согласност со член 15 став (4) и став (5) и член 17 став (4) и став (6) од овој закон.

(3) Извештајот од ставот (2) на овој член Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT) го доставува до директорот на Дигиталната агенција и до министерот за информатичко општество и администрација најдоцна до 31 март секоја година.

(4) Извештајот од ставот (2) на овој член Националниот центар за одговор на компјутерски инциденти (MKD-CSIRT) го доставува и до Групата за соработка.

**Безбедност на мрежи и информациски системи на операторите на суштински услуги**

**Член 15**

(1) Операторите на суштинските услуги се должни да преземат соодветни и пропорционални технички и организациски мерки за управување со ризиците по безбедноста на мрежите и информациските системи кои ги користат во нивното работење.

(2) Мерките од ставот (1) на овој член задолжително треба да обезбедат ниво на сигурност на мрежните и информациските системи соодветни на потенцијалниот ризик.

(3) Операторите на суштинските услуги се должни да преземат соодветни мерки за спречување и минимизирање на влијанието на инцидентите кои влијаат на безбедноста на мрежите и на информациските системи што се користат за обезбедување вакви суштински услуги, заради обезбедување на континуитет на услугите.

(4) Операторите на суштинските услуги се должни да го известат надлежниот CSIRT за инцидентите кои би можеле значително влијаат врз континуитетот на суштинските услуги што ги обезбедуваат, веднаш, а најдоцна во рок од 24 часа од моментот на откривање на инцидентот.

(5) Известувањето од ставот (4) на овој член содржи информации што му овозможуваат на надлежнот CSIRT да утврди евентуално меѓусекторско или прекугранично влијание на инцидентот.

(6) При утврдување на влијанието на инцидентот, операторот на суштинските услуги треба да ги земе предвид следниве параметри:

- бројот на корисници погодени од нарушувањето на суштинската услуга;

- времетраењето на инцидентот;

- географската распространетост во однос на областа погодена од инцидентот.

(6) Надлежниот CSIRT му доставува релевантни информации на операторот на суштинските услуги кој известил за инцидентот во однос на следењето на неговото известување, како и информации кои би можеле да го поддржат ефективното справување со инцидентот.

(7) По претходна консултација со операторот на суштински услуги кој известил за инцидентот, надлежниот CSIRT може да ја информира јавноста за поединечни инциденти, кога тоа е потребно подигнување на јавната свест за да се спречи настанување на инцидент или да се справи со тековен инцидент.

(8) Доколку инцидентот има значително влијание врз континуитетот во обезбедување на суштински услуги на земја членка на Европската унија, надлежниот CSIRT е должен да го извести Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), заради информирање на засегнатата земја членка.

(9) Во случаите определени со ставот (8) од овој член, MKD-CSIRT ги зачувува безбедносните и комерцијалните интереси на операторот на суштинските услуги, како и доверливоста на информациите што се дадени во неговото известување.

**Спроведување на мерките за безбедност на мрежи и информациски системи на оператори на суштински услуги**

**Член 16**

(1) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) се должни да ги преземат сите мерки и средства за да оценат дали операторите на суштинските услуги ги почитуваат нивните обврски за безбедност на мрежите и информациски системи наведени во член 15 од овој закон, како и влијанието на нивната безбедност врз безбедноста на мрежите и информациските системи.

(2) Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) имаат овластување да бараат од операторите на суштинските услуги да обезбедат:

- информации потребни за да се оцени безбедноста на нивните мрежни и информациски системи, вклучувајќи документирани безбедносни политики;

- доказ за ефективно спроведување на безбедносните политики, како што се резултати од безбедносна ревизија извршена од страна на надлежен орган или овластен ревизор, а доколку безбедносната ревизија е извршена од страна на овластен ревизор, резултатите од ревизијата, вклучувајќи ги и основните докази, да ги направат достапни за надлежниот CSIRT.

(3) Кога надлежниот CSIRT ги бара информациите или доказите определени со став (2) од овој член, ја наведува целта на барањето и специфицира кои информации се потребни.

(4) По проценката на информациите или резултатите од безбедносните ревизии наведени во став (2) алинеја 2 од овој член, а во случај на констатирани недостатоци, надлежниот CSIRT може да издаде обврзувачки упатства до операторите на суштинските услуги за да ги отстранат утврдените недостатоци.

(5) Надлежниот CSIRT соработува со органот надлежен за заштита на личните податоците, при решавањето на инцидентите што резултираат со загрозување на безбедноста на личните податоци.

**Безбедност на мрежите и информациските системи на давателите на дигитални услуги**

**Член 17**

(1) Давателите на дигитални услуги се должни да преземат соодветни и пропорционални технички и организациски мерки за управување со ризици што би ја загрозиле безбедноста на мрежите и информациските системи кои тие ги користат во контекст на обезбедување на дигиталните услуги.

(2) Мерките од ставот (1) на овој член задолжително треба да обезбедат ниво на сигурност на мрежите и информациските системи соодветни на потенцијалниот ризик и ги земаат предвид следните елементи:

- безбедноста на системите и објектите;

- управување со инциденти;

- управување со континуитет на бизнисот;

- мониторинг, ревизија и тестирање;

- усогласеност со меѓународните стандарди.

(3) Давателите на дигитални услуги се должни да ги преземат мерките согласно став (1) од овој член заради обезбедување на континуитет на дигиталните услуги што ги обезбедуваат.

(4) Давателите на дигитални услуги се должни да го известат надлежниот CSIRT за инциденти кои би можеле значително влијаат врз континуитетот на дигиталните услуги што ги обезбедуваат, веднаш, а најдоцна во рок од 24 часа од моментот на откривање на инцидентот.

(5) Известувањето од ставот (4) на овој член содржи информации што му овозможуваат на надлежнот орган CSIRT да утврди евентуално прекугранично влијание на инцидентот.

(6) При утврдување на влијанието на инцидентот, давателот на дигитални услуги треба да ги земе предвид следниве параметри:

- бројот на корисници погодени од инцидентот, особено корисниците кои ја користат услугата при обезбедување на сопствени услуги;

- времетраење на инцидентот;

- географската распространетост во однос на областа погодена од инцидентот;

- степенот на нарушување на функционирањето на услугата;

- степенот на влијанието врз економските и општествените активности.

(7) Обврската за пријавување инцидент настанува само ако давателот на дигитални услуги има пристап до информациите потребни за да се оцени влијанието на инцидент врз параметрите наведени во став (6) од овој член.

(8) Кога оператор на суштински услуги користи услуги од давател на дигитални услуги заради обезбедување на услуга која е од суштинско значење за одржување на критичните општествени и економски активности, давателот на дигиталните услуги е должен да го извести операторот на суштинската услуга за секој инцидент кој влијае на давателот на дигитални услуги, а има и значајно влијание врз континуитетот на суштинските услуги.

(9) Доколку инцидентот има значително влијание врз две или повеќе земји членки на Европската унија, надлежниот CSIRT е должен да го извести Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), заради информирање на засегнатите земји членки на унијата.

(10) Во случаите определени со ставот (9) од овој член, MKD-CSIRT се грижи за безбедносните и комерцијалните интереси на давателот на дигитални услуги, како и доверливоста на информациите што се дадени во неговото известување.

(11) По претходна консултација со давателот на дигитални услуги кој известил за инцидентот, надлежниот CSIRT може да ја информира јавноста за поединечни инциденти или да побара од давателот на дигитални услуги да го стори тоа, ако е неопходно јавно информирање за да се спречи потенцијален инцидент или за да се справи со тековен инцидент, или кога откривањето на инцидентот е од јавен интерес.

(12) Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) на предлог на надлежниот CSIRT донесува имплементациски акти за оценување на дополнителните елементи наведени во став (2) и параметрите наведени во став (6) од овој член.

**Спроведување на мерките за безбедност на мрежи и информациски системи на даватели на дигитални услуги**

**Член 18**

(1) Надлежниот CSIRT за давателите на дигитални услуги е должен да ги преземе сите мерки и средства, а доколку е потребно и ревизорски мерки, за да оцени дали давателите на дигитални услуги ги почитуваат нивните обврски за безбедност на мрежите и информациски системи наведени во член 17 од овој закон.

(2) Надлежниот CSIRT може да ги прибави потребните докази и од надлежен орган на земја членка на Европската унија во која се обезбедува дигиталната услуга.

(3) Надлежниот CSIRT има право да бара од давателите на дигитални услуги да обезбедат:

- информации потребни за да се оцени безбедноста на нивните мрежи и информациски системи, вклучувајќи документирани безбедносни политики;

- отстранување на секое неисполнување на услувите утврдени со членот 17 од овој закон.

(4) Доколку давателот на дигитални услуги има свое седиште или претставник во земја членка на Европската унија, но неговите мрежи и информациски системи се лоцирани во една или повеќе други земји членки на унијата, надлежниот орган на земјата-членка во која е регистрирано седиштето или претставникот на давателот на дигиталната услуга и надлежните органи на другите засегнати земји членки на унијата ќе соработуваат и ќе си помагаат меѓусебно.

(5) Соработката определена со став (4) од овој член може да опфаќа размена на информации помеѓу засегнатите надлежни органи и барања за преземање на супервизорските мерки во смисла на став (2) од овој член.

**Јурисдикција над даватели на дигитални услуги**

**Член 19**

(1) Давател на дигитални услуги се смета дека е под јурисдикција на земја членка на Европската унија во која има регистрирано седиште.

(2) Давателот на дигитални услуги се смета дека има седиште во земја членка на Европската унија во која се наоѓа неговата главна деловна единица.

(3) Давател на дигитални услуги кој не е основан во Европската унијата, а нуди дигитални услуги во Република Северна Македонија, должен е да назначи свој претставник во Република Северна Македонија.

(4) Давателот на дигитални услуги се смета дека е под јурисдикција на земјата членка на Унијата во која е регистриран претставникот.

**Стандардизација**

**Член 20**

(1) Заради обезбедување на примена на унифицирани мерки за безбедност на мрежите и информациските системи на операторите на суштински услуги и на мрежите и информациските системи на давателите на дигитални услуги надлежните органи треба да имплементираат меѓународно прифатени стандарди и спецификации релевантни за безбедноста на мрежите и информациските системи.

(2) Дигиталната агенција изготвува совети и упатства во однос на техничките области од ставот (1) на овој член, како и во однос на веќе постојните меѓународни и национални стандарди.

**Доброволно известување**

**Член 21**

(1) Правните лица кои не се идентификувани како оператори на суштински услуги и не се даватели на дигитални услуги можат доброволно да ги пријават инцидентите кои имаат значително влијание врз континуитетот на услугите што ги обезбедуваат.

(2) При обработка на известувањата за инциденти приоритет имаат задолжителни известувања примени од операторите на суштински услуги и од давателите на дигитални услуги пред обработката на доброволните известувања примени од правните лица определени со став (1) на овој член.

(3) Доброволните известувања се обработуваат само кога таквата обработка не претставува диспропорционално или непотребно оптоварување за надлежните тимови за одговор на компјутерски безбедносни инциденти (CSIRT).

(4) Доброволното известување не резултира со наметнување какви било обврски за правното лице што известува, кои не би ги имало доколку не е дадено тоа известување.

**Дигитална агенција**

**Член 22**

(1) Дигиталната агенција е самостојна во вршењето на работите утврдени со овој закон и има својство на правно лице.

(2) Дигиталната агенција е надлежна за работите од областа на:

- безбедноста на мрежите и информациските системи;

- управувањето со Националната транспортна оптичка мрежа и

-управувањето и безбедноста на податочниот центар и на дигиталните услуги обезбедени од институциите од јавниот сектор.

**Надлежности на Дигиталната агенција од областа на сајбер безбедноста**

**Член 23**

(1) Дигиталната агенција е надлежна за следните работи од областа на сајбер безбедноста:

1) подготовка на предлог Национална стратегија за безбедност на мрежи и информациски системи, односно Национална стратегија за сајбер безбедност, на секои две години,

2) воспоставување на контакти за обезбедување на прекугранична соработка од областа на безбедност на мрежи и информациски системи, односно вршење на функција на Единствена точка за контакт, по претходни консултации со надлежните органи за спроведување на овој закон и со надлежниот орган за заштита на личните податоци,

3) координација на секторските CSIRT-ови и мерките во нивна надлежност при справување со безбедносни инциденти на мрежите и информациските системи кои би можеле да имаат влијание врз мрежите и информациските системи на два или повеќе сектори,

4) националниот центар за контакт и одговор на безбедносни инциденти и ризици на мрежите и информациските системи на државата,

5) креирање на политики и мерки за постигнување на високо ниво на безбедност на мрежи и информациски системи во Република Северна Македонија,

6) обезбедување на совети и експертиза за компјутерска безбедност на институциите од јавниот и приватниот сектор,

7) обезбедување стратешки насоки за активностите на Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT);

8) совети за имплементација на најдобрите практики за разменување на информации поврзани со известување за инциденти, согласно член 15 став (4) и став (5) и член 17 став (4) и став (5) од овој закон;

9) помош на надлежните органи во кои се формирани секторски CSIRT-ови во градењето капацитети за да се обезбеди сигурност на мрежите и информациските системи;

10) размена на информации и најдобри практики со секторските CSIRT-ови за подигнување на свеста и обуки за безбедност на мрежи и информациски системи;

11) размена на информации и податоци за истражување и развој со секторските CSIRT-ови во однос на безбедноста на мрежите и информациските системи;

12) размена на искуства за прашања поврзани со безбедноста на мрежите и информациските системи со органите од јавниот сектор и со правни лица кои вршат дејност во секторите определени во член 3 став (2) од овој закон;

13) поддршка при истражување и развој на стандарди преку:

- помош при воведување и преземање европски и меѓународни стандарди за управување со ризикот и безбедноста на мрежите и информациските системи во соработка со надлежниот орган за стандардизација;

- советување на секторските CSIRT-ови за потребата од истражување во областа на мрежната и информациската безбедност со цел да се обезбеди одговор на тековните и новите ризици и закани за мрежната и информациската безбедност;

14) анализа и обработка на информации за најдобрите практики за справување ризици и одговор на инциденти;

15) анализа и обработка на податоци содржани во годишните извештаи од надлежните CSIRT-ови, доставени согласно член 13 став (?) од овој закон;

16) подготовка на програми за обука и симулација на вежби поврзани со безбедноста на мрежите и информациските системи;

17) советодавна помош на секторските CSIRT-ови во однос на идентификацијата на операторите на суштинските услуги, вклучувајќи однос на прекуграничните меѓузависни врски, во однос на ризиците и инцидентите;

18) утврдување на модалитетите за пријавување и известувања за инциденти, согласно член 15 и член 17 од овој закон,

19) соработка со надлежни органи на други држави во областа на безбедноста на мрежите и информациските системи, а особено со Агенцијата за безбедност на мрежи и информациски системи на Европската унија ( во натамошниот текст: ENISA),

20) пропишува спецификации на безбедност на информатичко-комуникациски производи,

21) обезбедува поддршка на развој на политики и регулатива од областа на безбедноста на мрежите и информациските системи преку:

- поддршка и совети за сите прашања поврзани со политиката и регулативата на Република Северна Македонија и Европската унија за мрежна и информациска безбедност;

- обезбедување подготвителна работа, совети и анализи во врска со развојот и ажурирањето на политиката и регулативата на Република Северна Македонија и Европската унија за мрежна и информациска безбедност;

- анализа на јавно достапни стратегии за мрежна и информациска безбедност и

22) соработка со надлежните органи од областа на сајбер криминал и заштита на личните податоци, заради решавање на прашања од заеднички интерес преку:

- размена на знаења и искуства и најдобри практики;

- обезбедување совети за релевантните аспекти на мрежната и информациската безбедност.

(2) Дигиталната агенција е надлежен CSIRT и за:

- операторите на суштински услуги од секторот дигитална инфраструктура и

- давателите на дигитални услуги.

**Надлежности на Дигиталната агенција од областа на управувањето со Националната транспортна оптичка мрежа**

**Член 24**

Дигиталната агенција е надлежна за следните работи од областа на управувањето со Националната транспортна оптичка мрежа:

1) координација на пристапот до капацитетите, идниот развој на бродбенд поврзувањето на институциите од јавниот сектор на Националната транспортна оптичка мрежа (НТОМ),

2) спроведување на политиката и на пропишаните правила за поврзување на јавните институции во затворените мрежи изградени со јавни средства,

3) спроведување на политиката и на пропишаните правила за поврзување на јавните институции до јавниот интернет,

4) поврзување помеѓу затворените мрежи на различни јавни институции,

5) издавање на одобренија за приклучување на институциите од јавниот сектор на Националната транспортна општичка мрежа,

6) набавка, одржување, поставување и управување со активната опрема и другите придружни средства на Националната транспортна оптичка мрежа,

7) дава мислења и предлози на Јавното претпријатие Македонска радиодифузија во однос на плановите и програмите за изградба на физичката инфраструктура на Националната транспортна оптичка мрежа,

8) управува и спроведува постапки за давање на користење на изградената физичка инфраструктура, односно користење на слободните оптички влакна на операторите, со надомест,

9) врши оптимизација и консолидација на оптичката инфраструктура изградена со буџетски средства,

10) врши контрола врз начинот на користње на Националната транспортна мрежа.

**Надлежности на Дигиталната агенција од областа на управувањето и безбедноста на податочниот центар и на дигиталните услуги обезбедени од институциите од јавниот сектор**

**Член 25**

Дигиталната агенција е надлежна за следните работи од областа на управувањето и безбедноста на податочниот центар и на дигиталните услуги обезбедени од институциите од јавниот сектор:

1) развој и одржување на хардвер и софтвер за потребите на органите на државната управа,

2) обезбедува техничка поддршка за развој и одржување на хардвер и софтвер за потребите на институциите од јавниот сектор,

3) спроведува набавки на мрежни и информациски системи за потребите на органите на државната управа,

4) дава согласност на институциите од јавниот сектор за спроведување на постапки за јавни набавки на информациска и мрежна опрема,

5) го воспоставува, управува и одржува државниот податочен центар,

6) врши координација и издава насоки за начинот на користење на државниот податочен центар,

7) имплементира мерки и процедури за обезбедување на безбедноста на државниот податочен центар,

8) имплементира мерки и процедури за безбедност и сигурност на дигиталните услуги кои ги даваат институциите од јавниот сектор,

9) врши координација на планирањето и имплементацијата на проектите од областа на информатичкото општество помеѓу органите на државната управа и институциите од јавниот сектор,

10) имплементира стандарди за безбедност и развој на информациските системи на органите на државната управа,

11) го воспоставува и води Регистарот на информациско-комуникациска опрема во сопственост на органите на државната управа,

12) управува со Националната платформа за интероперабилност, Системот за единствена најава, Националниот портал за електронски услуги, Каталогот на услуги и Централниот регистар на население и

13) обезбедува услуги за обработка во облак за потребите на органите на државната управа,

**Мрежа на CSIRT-ови**

**Член 26**

(1) Во Дигиталната агенција како посебна организациска единица се воспоставува и Мрежа на CSIRT-ови, заради обезбедување на брза и ефективна оперативна соработка помеѓу секторските CSIRT-ови.

(2) Мрежата на CSIRT-ови е надлежна за:

1) размена на информации за услугите, операциите и начините за соработка на секторските CSIRT-ови;

2) на барање на надлежен секторски CSIRT што е потенцијално погоден од инцидент, разменува и дискутира за некомерцијално чувствителни информации поврзани со тој инцидент и поврзани ризици;

3) доброволна размена и ставање на располагање недоверливи информации во врска со поединечни инциденти;

4) на барање на надлежен секторски CSIRT определува мерки за координиран одговор на инцидент кој е идентификуван во секторот, но може да има и подривачки ефект и во други сектори;

5) обезбедува поддршка при справување и одговор на меѓусекторски инциденти;

6) определува мерки за оперативна соработка меѓу секторските CSIRT-ови, вклучително и во врска со:

- категории на ризици и инциденти;

- рани предупредувања;

- заемна помош;

- принципи и модалитети за координација;

7) евалуација на резултати од спроведени вежби кои се однесуваат на безбедноста на мрежите и информациските системи;

8) на барање на поединечен CSIRT, спроведува анализа на оперативните способности и подготвеност за одговор на инциденти на тој CSIRT;

9) издава упатства за воедначена примена на оперативните практики при спроведувањето на овој закон.

(3) Мрежата на CSIRT-ови е должна да соработува со ENISA.

**Органи на Дигиталната агенција**

**Член 27**

Органи на Дигиталната агенција се Управен одбор и директор.

**Управен одбор**

**Член 28**

(1) Управниот одбор се состои од пет члена кои ги именува и разрешува Владата на Република Северна Македонија.

(2) По еден член во Управниот одбор на Дигиталната агенција предлагаат министрите надлежни за работите од областа на:

- одбраната,

- внатрешните работи и

- информатичкото општество и администрација.

(3) За именување на останатите два члена на Управниот одбор се објавува јавен оглас во најмалку три дневни весници кои се издаваат на целата територија на Република Македонија од кои еден од весниците кој се издава на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

(4) Управниот одбор од редот на своите членови избира и разрешува претседател и заменик на претседателот на одборот на начин и постапка утврдени во Деловникот за работа на Управниот одбор.

(5) Заменик претседателот по службена должност го заменува претседателот ако тој не е во можност да ги извршува своите должности.

(6) Членовите на Управниот одбор се именуваат со мандат од пет години.

(7) Членовите на Управниот одбор не можат да бидат именувани повеќе од два последователни мандата.

(8) Членовите на Управниот одбор се именуваат не подоцна од 30 дена пред истекот на мандатот на нивните претходници. Претседателот е должен да ја извести Владата на Република Северна Македонија за истекот на мандатот на членовите на Управниот одбор не подоцна од 60 дена пред истекот на истиот.

(9) Ако постапката за именување не е завршена пред истекот на мандатот на членовите на Управниот одбор, членовите на Управниот одбор чиј мандат е истечен ќе продолжат да ја вршат својата функција, но не подолго од шест месеци.

(10) Доколку членовите на Управниот одбор донесат одлука од својата надлежност со која ќе ги повредат интересите на Агенцијата, одговараат неограничено и солидарно за штетата настаната со таквата одлука. Нема да се смета за одговорен оној член на Управниот одбор кој укажал дека предложената одлука е спротивна на овој закон и се спротивставил на донесувањето на одлуката, на начин што го издвоил своето мислење во записникот од седницата и гласал “против“ одлуката.

**Услови за именување на членови на Управниот одбор**

**Член 29**

(1) За член на Управниот одбор може да биде именувано лице кое:

- е државјанин на Република Северна Македонија,

- во моментот на именувањето со правосилна судска пресуда не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност;

- активно го користи македонскиот јазик,

- има стекнати најмалку 240 кредити според ЕКТС или завршен VII/1 степен образование од областа на информатиката, телекомуникациите, правото или економијата и

- има најмалку пет години соодветно работно искуство и посебни знаења од областа на електронските комуникации.

(2) За член на Управен одбор може да биде именувано лице вработено во друго правно лице, освен во друго правно лице кое може да бидат во конфликт на интересите, согласно со овој закон.

(3) Во текот на времетраењето на својот мандат членовите на Управниот одбор не можат да бидат пратеници во Собранието на Република Северна Македонија, членови на Владата на Република Северна Македонија, како и лица кои извршуваат должности во органите и телата на политички партии.

**Предвремено разрешување на член на Управниот одбор**

**Член 30**

(1) Владата на Република Северна Македонија, може да разреши член на Управниот одбор пред истекот на мандатот:

- на негово барање,

- настапила некоја од пречките за членство во Управниот одбор предвидени во членот 25 став (3) од овој закон,

- ако е правосилно осуден за кривично дело за кое е предвидена казна затвор во траење подолго од шест месеци или му е изречена мерка на безбедност забрана за вршење на професија, дејност или должност во траење подолго од шест месеци,

- ако не е во можност да ја извршува должноста повеќе од шест месеци во континуитет,

- ако неоправдано отсуствувал од три состаноци на Управниот одбор едно по друго или вкупно од пет состаноци за време од една година,

- ако се утврди дека членот на Управниот одбор во постапката за негово именување дал невистинити податоци или пропуштил да изнесе некои информации кои се важни за неговото именување,

(2) За исполнување на условите за предвремено разрешување на член на Управниот одбор, предвидени во ставот (1) на овој член претседателот, односно заменикот на претседателот е должен да ја извести Владата на Република Северна Македонија во рок од пет дена од денот на исполнувањето на условите од ставот (1) на овој член.

**Надлежности на Управниот одбор**

**Член 28**

(1) Управниот одбор е орган на управување на Дигиталната агенција, кој го утврдува општото насочување на активностите на Дигиталната агенција и обезбедува услови за извршување на надлежностите на Агенцијата определени со овој закон.

(2) Управниот одбор ги има следниве надлежности:

- донесува Статут на Дигиталната агенција,

- донесува Деловник за својата работа во согласност со овој закон и Статутот на Дигиталната агенција, кој задолжително содржи одредби за донесување на брзи одлуки по писмена постапка или далечинска конференција,

- донесува одлука за усвојување на годишниот извештај за работа на Дигиталната агенција за претходната година,

- донесува одлука за усвојување на годишната програма за работа на Дигиталната агенција за наредната година,

- донесува одлука за именување и разрешување на директорот на Дигиталната агенција во согласност со овој закон и по постапка утврдена во Статутот на Дигиталната агенција,

- го следи спроведувањето на годишната програма за работа на Дигиталната агенција преку кварталните извештаи доставени од директорот на Дигиталната агенција,

- донесува одлука за користење на нереализираните средства од финансискиот план на Дигиталната агенција од претходната година, на предлог на директорот,

- соработува со други државни органи и институции, органи на единиците на локалната самоуправа, академската заедница и со приватни правни лица и здруженија на граѓани и фондации во Република Северна Македонија,

- дава мислења, препораки и предлози до Владата на Република Северна Македонија и други државни органи и институции од областа на безбедност на мрежи и информациски системи,

- усвојува општи акти за работењето на Дигиталната агенција утврдени во Статутот на Дигиталната агенција, а по предлог на директорот,

- дава мислење на Националната стратегија за безбедност на мрежи и информациски системи, односно Националната стратегија за сајбер безбедност пред нејзиното донесување од страна на Владата на Република Северна Македонија,

- го усвојува годишниот извештај на националниот центар за контакт и одговор на безбедносни инциденти и ризици на мрежите и информациските системи на државата најдоцна до 1 март во тековната година за претходната и истиот го доставува до министерот за информатичко општество и администрација најдоцна во рок од 30 дена сметано од денот на неговото усвојување,

- усвојува политики и мерки за постигнување на високо ниво на безбедност на мрежи и информациски системи во Република Северна Македонија,

- донесува стратешки насоки за активностите на Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT) и

- усвојува годишна програма за обука и симулација на вежби поврзани со безбедноста на мрежите и информациските системи.

(2) Управниот одбор донесува годишна и тригодишната програма за работа на Дигиталната агенција на предлог на директорот најдоцна до 30 октомври во тековната година за следната година и ја доставува до Владата на Република Северна Македонија за усвојување.

(3) Управниот одбор донесува годишен извештај за активностите на Дигиталната агенција до 1 март во тековната година за претходната година на предлог на директорот и го доставува до Владата на Република Северна Македонија најдоцна до 31 март за негово усвојување.

(4) Годишниот извештај содржи преглед на финансиската состојба, наративен дел и евиденција на примени известувања за инциденти од надлежните CSIRT-ови.

(5) Управниот одбор донесува Насоки за борба против измама кои се пропорционални на ризиците од измама, земајќи ја предвид анализата на трошоци и придобивки од мерките кои ќе се спроведат.

(6) Насоките од ставот (5) на овој член се должни да ги почитуваат сите вработени во Дигиталната агенција и во секторските CSIRT-ови.

**Начин на работа и одлучување на Управниот одбор**

**Член 29**

(1) Управниот одбор се состанува најмалку четири пати годишно.

(2) Одлуките на Управниот одбор се донесуваат со мнозинство гласови од вкупниот број членови.

(3) Претседателот на Управниот одбор ги свикува состаноците на Управниот одбор по писмен предлог на директорот на Дигиталната агенција или по писмен предлог на тројца членови на Управниот одбор.

(4) Директорот има право да присуствува и учествува на состаноците на Управниот одбор, без право на глас.

(5) На состаноците на Управниот одбор, без право на одлучување, можат да присуствуваат вработени од стручната служба на Дигиталната агенција, како и вработени во секторските CSIRT-ови на покана на Управниот одбор, а заради давање на информации, појаснувања и стручни образложенија за прашања што се на дневен ред на состанокот, а во согласност со Деловникот за работа на Управниот одбор.

(6) Материјалите за состаноците на Управниот одбор ги подготвува стручната служба на Дигиталната агенција и истите се доставуваат до сите членови на Управниот одбор, на начин и во рок утврден во Деловникот за работа на Управниот одбор.

(7) Дневниот ред, записниците од состаноците на Управниот одбор, донесените одлуки и акти се објавуваат на веб страницата на Дигиталната агенција во рок од седум дена од денот на одржувањето на состанокот.

**Надоместоци на членовите на Управниот одбор**

**Член 30**

(1) Членовите на Управниот одбор имаат право на:

- месечен надоместок во висина до две просечни месечни плати во Република Северна Македонија според податоците објавени од Државниот завод за статистика и

- надоместок за патни трошоци за оние членови на Управниот одбор кои живеат надвор од Скопје кога присуствуваат на состаноците на Управниот одбор и надоместок за патни трошоци, сместување и дневници за службено патување, согласно со Законот за платата и другите надоместоци на избрани и именувани лица во Република Македонија.

(2) Средствата за месечниот надоместок и на другите трошоци на членовите на Управниот одбор се обезбедуваат од средствата на Дигиталната агенција утврдени со финансискиот план.

**Надлежности на директорот на Дигиталната агенција**

**Член 31**

(1) Орган на раководење на Дигиталната агенција е директорот кој е независен во извршувањето на своите должности.

(2) Директорот е надлежен за:

1) тековното работење на Дигиталната агенција;

2) спроведување на одлуките донесени од Управниот одбор;

3) подготовка на годишната програма за работа и на тригодишната програма за работа и нивно доставување до Управниот одбор;

4) спроведување на годишната програма за работа и тригодишната програма за работа и достава на извештаи до Управниот одбор за нивното спроведување;

5) подготвка на годишен извештај за активностите на Дигиталната агенција и негово доставување до Управниот одбор за одобрување;

6) предлага начин на користење на нереализираните средства од финансискиот план на Дигиталната агенција од претходната година;

7) предлага мислења, препораки и предлози до Управниот одбор за Владата на Република Северна Македонија и други државни органи и институции од областа на безбедност на мрежи и информациски системи;

8) предлага општи акти за работењето на Дигиталната агенција утврдени во Статутот на Дигиталната агенција;

9) го води процесот на подготовка на Националната стратегија за безбедност на мрежи и информациски системи, односно Националната стратегија за сајбер безбедност;

10) предлага годишeн извештај на националниот центар за контакт и одговор на безбедносни инциденти и ризици на мрежите и информациските системи на државата;

11) предлага политики и мерки за постигнување на високо ниво на безбедност на мрежи и информациски системи во Република Северна Македонија;

12) предлага стратешки насоки за активностите на Тимовите за одговор на компјутерски безбедносни инциденти (CSIRT);

13) предлага годишна програма за обука и симулација на вежби поврзани со безбедноста на мрежите и информациските системи

14) управува со Мрежата на CSIRT-ови и се грижи за спроведување на активностите во нејзина надлежност;

15) управува со националниот центар за контакт и одговор на безбедносни инциденти и ризици на мрежите и информациските системи на државата;

16) заштита на финансиските интереси на Дигиталната агенција преку примена на превентивни мерки против измама, корупција и други нелегални активности;

17) предлага Насоки за борба против измама;

18) воспоставува и одржува соработка со бизнис заедницата и организациите на потрошувачи за да се обезбеди редовен дијалог со релевантните засегнати страни;

19) врши и други работи определени со овој закон.

(2) По потреба и во рамките на целите и надлежностите на Дигиталната агенција, директорот може да формира работни групи составени од експерти, вклучително и од органите на државната управа, по претходно одобрение од Управниот одбор.

(3) Постапката за составот, именувањето на експертите и активностите на работните групи се утврдуваат Статутот на Дигиталната агенција.

**Услови за именување на директор**

**Член 32**

(1) Управниот одбор именува директор на Дигиталната агенција по пат на јавен оглас кој се објавува во најмалку три дневни весници кои се издаваат на целата територија на Република Северна Македонија од кои еден од весниците кој се издава на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

(2) За директор на Дигиталната агенција може да биде именувано лице кое:

- е државјанин на Република Македонија;

- во моментот на именувањето со правосилна судска пресуда не му е изречена казна или прекршочна санкција забрана за вршење на професија, дејност или должност;

- активно го користи македонскиот јазик;

- има стекнати најмалку 240 кредити според ЕКТС или завршен VII/1 степен образование од областа на електротехничките науки, информатиката, правото или економијата и

- има најмалку пет години соодветно работно искуство во областа на заштитата на информации и податоци или безбедност на мрежи и информациски системи.

(3) При изборот на директорот на Дигиталната агенција ќе се земе предвид неговото професионално искуство во соодветната област.

(4) Управниот одбор е должен да именува директор на Дигиталната агенција не подоцна од 30 дена пред истекот на мандатот на неговиот претходник.

(5) Директорот на Дигиталната агенција е професионално ангажиран со полно работно време.

(6) Мандатот на директорот на Дигиталната агенција е пет години со можност за уште еден последователен мандат.

(7) Ако мандатот на директорот на Дигиталната агенција е завршен, а постапката за именување на директор не е завршена, директорот на Дигиталната агенција продолжува да ја врши функцијата се додека не се именува директор, но не подолго од шест месеци.

**Програма за работа**

**Член 33**

(1) Дигиталната агенција ја врши својата работа во согласност со својата годишна и тригодишна програма за работа која ги вклучува сите планирани активности.

(2) Програмата за работа вклучува специфични индикатори за оценка на постигнатите резултати во однос на нивото на безбедност на мрежи и информациски системи.

(3) Управниот одбор врши оценка на усогласеност на програмата за работа со поставените стратешки цели и мерки за безбедност на мрежи и информациски системи, како и со законските приоритети од областа на мрежната и информациската безбедност.

+ од претходните одредби за програмата за работа

**Изјава за интереси**

**Член 34**

(1) Членовите на Управниот одбор, директорот и вработените во Дигиталната агенција даваат изјава за преземање обврски и изјава за постоењето или непостоењето на директни или индиректни интереси кои би можеле да влијаат на нивната независност.

(2) Изјавите треба да содржат точни и целосни податоци, кои се даваат при преземање на функцијата член на Управен одбор или директор, односно при стапување во работен однос во Дигиталната агенција, а се ажурираат согласно промените на околностите кои влијаат на содржината на изјавите.

(3) Ставовите (1) и (2) од овој член се однесуваат и на членовите на работните групи формирани во Дигиталната агенција.

**Транспарентност**

**Член 35**

(1) Дигиталната агенција е должна јавно да ги објави следните документи кои произлегуваат од нејзината надлежност:

1) Националната стратегија за безбедност на мрежи и информациски системи, односно Националната стратегија за сајбер безбедност,

2) листа на надлежни органи и тела со кои Дигиталната агенција има воспоставено прекугранична соработка,

3) политиките и мерките за постигнување на високо ниво на безбедност на мрежи и информациски системи во Република Северна Македонија,

4) совети за имплементација на најдобрите практики за разменување на информации поврзани со известување за инциденти, согласно член 15 став (4) и став (5) и член 17 став (4) и став (5) од овој закон;

5) иницијативи за воведување и преземање европски и меѓународни стандарди за управување со ризикот и безбедноста на мрежите и информациските системи во соработка;

6) програмите за обука и симулација на вежби поврзани со безбедноста на мрежите и информациските системи;

7) анализи на јавно достапни стратегии за мрежна и информациска безбедност;

8) годишната и тригодишната програма за работа на Дигиталната агенција;

9) годишниот извештај за работа на Дигиталната агенција.

**Доверливост**

**Член 36**

(1) Дигиталната агенција нема право да открива на други држави информации кои ги обработува или прима, за кои е поднесено основано барање за нивно целосно или делумно третирање како доверливи информации.

(2) Членовите на Управниот одбор, директорот, членовите на работните групи и вработените во Дигиталната агенција, вклучувајќи и службеници кои привремено се упатени од земјите членки, се должни да ги почитуваат барањата за доверливост според член 339 од Договорот за функционирањето на Европската Унијата (ДФЕУ), дури и по завршување на вршењето на своите должности.

(3) Членовите на Управниот одбор, директорот, членовите на работните групи и вработените во Дигиталната агенција при преземањето на мандатот, односно при вработувањето во Дигиталната агенција задолжително потпишуваат изјава за доверливост на информации.

(4) По исклучок и доколку е потребно за извршување на надлежностите на Дигиталната агенција, Управниот одбор донесува одлука за начинот и обемот на обработка, односно размена, обработка и складирање на класифицирани информации.

(5) Во случаите определени со ставот (4) на овој член, Управниот одбор во договор со службите на Комисијата, донесува внатрешни правила за работа со примена на начелата за безбедност утврдени во Одлуката 2001/844/ЕЗ, ЕЗЈЧ, Евроатом на Комисијата од 29 ноември 2001 година за изменување на нејзиниот деловник за работа. Овие правила вклучуваат, меѓу другото, одредби за размена, обработка и складирање на класифицирани информации.

**Финансирање на Дигиталната агенција**

**Член 37**

Средствата за плата, надоместоци и додатоци на плата, за работа, унапредување, модернизација и опремување на Дигиталната агенција, предвидени со годишниот финансиски план на Дигиталната агенција се обезбедуваат од Буџетот на Република Северна Македонија.

**Организација и вработување во Дигиталната агенција**

**Член 38**

(1) Стручните, нормативно-правните, управните, управно-надзорните, материјално финансиските, сметководствените, информатичките и други работи на Дигиталната агенција ги врши стручна служба чија внатрешна организација, делокруг на работа и услови за вработување поблиску се уредуваат со актите за внатрешна организација и систематизација на работите и задачите.

(2) Вработените во стручната служба од ставот (1) на овој член имаат статус на административни службеници, согласно со Законот за административни службеници.

(3) Вработените во Агенцијата, кои вршат помошно-технички работи, имаат статус на помошно-технички персонал, согласно со Законот за вработени во јавниот сектор и општите прописи за работни односи.

(4) Начинот на уредување на основната плата и на додатоците на плата на вработените во Дигиталната агенција, како и висината на коефициентот на основната плата ги пропишува Управниот одбор.