ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАЦИСКИ СИСТЕМИ И ДИГИТАЛНА ТРАНСФОРМАЦИЈА

I. ОПШТИ ОДРЕДБИ

Предмет

Член 1

Со овој закон се утврдува:

- донесување на План за дигитална трансформација на јавниот сектор во Република Северна Македонија,
- донесување на Национална стратегија за сајбер безбедност,
- определување на надлежно тело за безбедност на мрежни и информациски системи и дигитална трансформација на јавниот сектор и утврдување на неговите надлежности,
- управување со сајбер кризи, единствена точка за контакт за безбедност на мрежни и информациски системи, како и национално тело за одговор на компјутерски инциденти,
- мерки за управување со сајбер безбедносни ризици и обврски за известување,
- правила и обврски за размена на информации поврзани со сајбер безбедноста,
- надзор над спроведување на овој закон.

Цели

Член 2

Цели на овој закон се обезбедување на:

I. високо ниво на сајбер безбедност со цел заштита и понатамошен развој на општеството,
II. градење и проширување на ИТ инфраструктурата, односно поефикасна и поефективна дигитална трансформација на јавниот сектор,
III. повисок степен на отвореност со цел да се обезбеди развој на иновативни софтверски решенија,
IV. обуки за сајбер безбедност и дигитални вештини за вработените во јавниот сектор и граѓаните на Република Северна Македонија

Дефиниции

Член 3

Изразите употребени во овој закон го имаат следното значење:

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

а) електронска комуникациска мрежа како што е дефинирана соодредбите од Законот за електронските комуникации,

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

в)дигитални податоци кои се складираат, обработуваат, преземаат или пренесуваат со елементи опишани во точките (а) и (б) за целите на нивното работење, употреба, заштита и одржување;

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

3) **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;

4) **„Национална стратегија за сајбер безбедност“** е кохерентна рамка усвоена од Владата на Република Северна Македонија со која се предвидени стратешки цели и приоритети во областа на сајбер безбедност и управување за постигнување на истите;

5) „**избегнат инцидент**“ значи секој настан што можел да ја загрози достапноста, веродостојноста, интегритетот или доверливоста на складираните, пренесените или обработените податоци или на услугите што ги нудат или до кои може да се пристапи преку мрежните и информациските системи, којшто бил успешно спречен или не се случил;

6)**„инцидент“** е настан штоја загрозува достапноста, веродостојноста, интегритетот или доверливоста на складираните, пренесените или обработените податоци или на услугите што ги нудат или до кои може да се пристапи преку мрежните и информациските системи;

7)**„сајбер безбедносен инцидент од големи размери“ (large-scale cybersecurity incident)** е инцидент што предизвикува ниво на нарушување што го надминува

капацитетот на државата да одговори на него или што има значително влијание на најмалку две држави;

8) **„справување со инциденти“ (incident handling)** се однесува на сите дејства и процедури насочени кон спречување, откривање, анализа и ставање под контрола на инцидент или одговор на инцидентот и опоравување од инцидентот;

9) **„ризик“** е потенцијална загуба или нарушување предизвикано од инцидент и треба да се изрази како комбинација на опсегот на таквата загуба или нарушување и веројатноста за случување на инцидентот;

10)„**сајбер закана“ (cyberthreat**) 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;

11) „**сериозна сајбер закана“ (significant cyberthreat**) е компјутерска закана за којашто, врз основа на нејзините технички карактеристики, може да се претпостави дека може да има сериозно влијание врз мрежните и информациските системи на некој субјект или на корисниците на услугите од субјектот преку предизвикување значителна материјална или нематеријална штета

12) „**ранливост“ (vulnerability**) е слабост, подложност или недостаток на ИКТ-производи или ИКТ-услуги што може да бидат искористени од страна на компјутерска закана

13) **„точка за размена на интернет-сообраќај“ (internet exchange point - IXP**) претставува мрежна инфраструктура што овозможува меѓусебно поврзување на повеќе од две независни мрежи (автономни системи), првенствено наменета за олеснување на размената на интернет-сообраќајот, што обезбедува меѓусебно поврзување само за автономни системи и за којашто не е потребно интернет-сообраќајот што поминува помеѓу кои било два автономни системи да поминува низ трет автономен систем, ниту го менува или на друг начин влијае врз таквиот сообраќај;

14) **„систем за имиња на домени“ (domain name system-DNS)** значи хиерархиски распореден систем за именување што овозможува идентификација на интернет-услуги и ресурси, со што на уредите на крајните корисници им се овозможува преку користењето на услугите за интернет-насочување и поврзување да пристапат до тие услуги и ресурси;

15) **„Давател на услуги за DNS“ (DNS service provider)** е субјект што обезбедува:

- јавно достапни повторливи услуги за распределување на имиња на домени на крајните корисници на интернет, или
- меродавни услуги за распределување на имиња на домени за користење од други лица, со исклучок на коренски сервери за имиња;

16) **„регистар на имиња на врвни домени“** (**top-level domain/TLD name registry**) е субјект кому му е доделен конкретен врвен домен и е одговорен за управување

со тој домен, вклучувајќи го регистрирањето на имиња на домени во рамките на врвниот домен и техничкото управување со врвниот домен, вклучувајќи го управувањето со неговите именски сервери, одржувањето на неговите бази на податоци и дистрибуција на зонските датотеки на врвниот домен во именските сервери, без оглед на тоа дали субјектот ги извршува некои од тие операции самостојно или тоа извршување го доделува на други субјекти, со исклучок на ситуациите во кои регистраторот ги користи имињата на врвните домени само за своја употреба;

17) **„субјект што обезбедува услуги за регистрација на имиња на домени“** значи регистратор или застапник што делува во име на регистрите, како што е давател или препродавачи на услуги за приватност или регистрација преку посредник;

18) **„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;

19) „**доверлива услуга“** е електронска услуга при електронски трансакции, која се состои од:

- создавање, проверка (валидација) и потврдување (верификација) на електронски потписи, електронски печати или електронски временски жигови, услуги за електронска препорачана достава, како и сертификати поврзани со овие услуги или
- создавање, валидација и верификација на сертификати за автентичност на веб страници или
- зачувување на електронски потписи, печати или потврди поврзани со овие услуги.

Доверливите услуги може да бидат неквалификувани и квалификувани.

20)„**давател на доверлива услуга**“ е правно лице кое обезбедува една или повеќе доверливи услуги

21)„**квалификувана доверлива услуга**“ е вид на доверлива услуга што ги исполнува условите утврдени со овој закон кои се однесуваат за квалификувана доверлива услуга

22)„**давател на квалификувана доверлива услуга**“ е давател на доверливауслуга кој обезбедува една или повеќе квалификувани доверливи услуги и чиј статус на давател на квалификувана доверлива услуга е доделен од страна на министерот за информатичко општество и администрација со регистрација во Регистарот на шеми за електронска идентификација и на доверливи услуги.

23)**„интернет-пазар (online market place)“** значи услуга овозможена со употреба на софтвер, вклучувајќи интернет-локации, дел од интернет-локации или апликација, управувана од трговец или во негово име од трети страни, што им

овозможува на потрошувачи да склучуваат договори на далечина со други трговци или потрошувачи;

24) **„интернет-пребарувач“ (online search engine)** е вид дигитална услуга која на корисниците им овозможува да вршат пребарување на база со прашалник на која било тема, во принцип, на сите веб-страници или на веб-страници на одреден јазик, врз основа на клучен збор, гласовен внес, фраза или друг внес, при што враќа резултати во кој било формат во кои може да се најдат информации поврзани со бараната содржина;

25) **„услуга за компјутерска обработка во облак“ (cloud computing service**) е дигитална услуга што овозможува администрација на барање и широк далечински пристап до скалабилно и еластично множество на компјутерски ресурси што може да се споделуваат, меѓу другото и кога таквите ресурси се распоредени на неколку локации;

26) **„услуга за податочен центар“ (data centre service)** е услуга што опфаќа структури или групи на инфраструктури што се наменети за централизирано сместување, меѓусебно поврзување и работа на ИТ-опрема и мрежна опрема што обезбедува услуги за складирање, обработка и пренос на податоци, заедно со сите објекти и инфраструктури за дистрибуција на електрична енергија и контрола на температурата, влагата и заштита од непогоди;

27) **„мрежа за испорака на содржини“ (content delivery network**) е мрежа на географски распоредени сервери наменети за осигурување голема достапност, пристапност или брза испорака на дигитални содржини и услуги на корисници на интернет во име на даватели на содржини и услуги;

28) **„платформа за услуги за социјални мрежи“ (social networking services platform**) е платформа што им овозможува на крајните корисници да се поврзуваат, да споделуваат, да откриваат и да комуницираат меѓу себе на повеќе уреди, особено преку разговори, објави, видеа и препораки;

29) „**претставник**“ е физичко или правно лице кое е изречно назначено да делува во име на давател на услуги за DNS, регистар на имиња на врвни домени, субјект/давател на услуги за регистрација на имиња на домени, давател на услуги за компјутерска обработка во облак, давател на услуги за податочен центар, давател на услуги за мрежи за испорака на содржини, давател на управувани услуги, давател на управувани безбедносни услуги, давател на услуга на интернет-пазар, давател на услуги на пребарувачи на интернет или давател на платформи за услуги за социјални мрежи што нема регистрирано седиште во Република Северна Македонија и до кое може да се обрати Агенцијата, односно MKD-CSIRT наместо на конкретниот субјект во однос на обврските на тој субјект што произлегуваат од овој закон;

(30)„**давател на управувани услуги**“ **(managed service provider)** е субјект кој обезбедува услуги поврзани со инсталирање, управување, работење или

одржување на ИКТ-производи, мрежи, инфраструктури, апликации или кои било други мрежни и информациски системи, во облик на помош или активно управување кое се спроведува во просториите на клиентот или на далечина;

(31)„**давател на управувани безбедносни услуги**“ **(managed security service provider)** е давател на управувани услуги што врши или обезбедува помош за активности кои се однесуваат на управување со сајбер безбедносни ризици;

(32) „**истражувачка организација**“ е субјект кој има примарна цел да спроведе применети истражувања или експериментален развој со цел да се искористат резултатите од тоа истражување за комерцијални цели, но кој не ги опфаќа образовните институции.

(33) „**дигитална трансформација на јавниот сектор“** значи воведување и примена на дигитални технологии и иновации со цел подобрување на ефикасноста, пристапноста и квалитетот на јавните услуги кон граѓаните и бизнис-секторот, обезбедување поголема отвореност и транспарентност на јавниот секто, како и обезбедување на безбедносна комуникација..

II. НАДЛЕЖНО ТЕЛО

Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација

Член 4

(1) Надлежно тело за безбедност на мрежни и информациски системи и дигитална трансформација на јавниот сектор во Република Северна Македонија е Агенцијата за безбедност на мрежни и информациски системи и дигитална трансформација (во натамошниот текст: Агенција).

(2) Агенцијата е регулаторно тело во Република Северна Македонија и има статус на правно лице со јавни овластувања утврдени со овој закон.

(3) Република Северна Македонија е основач на Агенцијата. Имотот и средствата за работа на Агенцијата ги користи и со нив управува Агенцијата.

(4) Агенцијата ги извршува работите во согласност со овој закон и прописите донесени врз основа на него, Законот за општата управна постапка, доколку со овој закон поинаку не е одредено, Законот за административни службеници, Закон за вработените во јавниот сектор и други закони и стратешки документи на Република Северна Македонија, како и препораките и насоките на Европската комисија и Агенцијата за сајбер безбедност на Европската Унија (ENISA).

(5) Седиштето на Агенцијата е во Скопје.

Надлежности на Агенцијата

Член 5

Агенцијата ги има следните надлежности:

- соработува со домашни и меѓународни организации, институции и тела и врши координација на национално и меѓународно ниво во однос на справување со сајбер безбедносни инциденти;
- врши следење, анализа, рано предупредување и информирање на сајбер закани, ранливости и инциденти
- обезбедува одговор за справување со сајбер безбедносни инциденти
- информира за состојбите со сајбер безбедноста во државата
- спроведува и унапредува мерки за управување со сајбер безбедносни ризици и за известување за значителни инциденти
- подготвува предлог-листа за утврдување на сектори и потсектори, како и за видовите на претпријатијата во рамките на секторите односно потсекторите, во согласност со овој закон,
- определува оператори на суштински услуги, оператори на важни услуги и правни лица што обезбедуваат услуги за регистрација на домени и им утврдува обврски, во согласност со овој закон,
- води регистар на оператори на суштински услуги, оператори на важни услуги и правни лица што обезбедуваат услуги за регистрација на домени,
- промовира употреба на сајбер безбедносни алатки и апликации со отворен код и отворени стандарди,
- соработува со Министерството за информатичко општество и администрација во подготовката на предлог на Националната стратегија за сајбер безбедност
- врши функција на единствена точка за контакт за безбедност на мрежни и информациски системи,
- го подготвува предлог-Панот за сајбер безбедносни инциденти од големи размери и кризи,
- соработува со организациите и мрежите на Европската Унија надлежни за управување со сајбер безбедносни инциденти од големи размери и кризи,
- врши функција на национално тело за одговор на компјутерски инциденти (MKD-CSRIT),
- донесуваГодишен извештај за состојбите во сајбер безбедноста;
- обезбедува помош за воспоставување на механизми за споделување на информации за сајбер безбедноста,
- обезбедува подршка за малите и средни претпријатија;
- промовира и подржува активна сајбер заштита
- воспоставува и води регистар на субјектите од членот 29 на овој закон,

- организира и спроведува обуки од областа на сајбер безбедноста и дигиталната трансформација и организира кампањи во согласност со овој закон,
- врши надзор над операторите на суштински услуги и операторите на важни услуги и им наметнува мерки во случај кога истите не ги исполнуваат обврските утврдени со овој закон,
- подготвува предлог-План за дигитална трансформација на јавниот сектор и врши надзор над неговото спроведување
- им дава согласност и задолжителни насоки на органите на државната управа во врска со спроведувањето на постапките за јавни набавки за хардвер и софтвер, во согласност со овој закон , ,
- обезбедува затворена оптичка електронска комуникациска мрежа за потребите на органите на државната управа, согласно овој закон,
- врши набавка, одржување, поставување, управување и надзор на активната комуникациска опрема на Владината мрежа во органите на државната управа и мрежните јазли на истата
- врши изградба, управува, развива и одржува владин податочен центар, владин облак и центар за обновување на податоци во случај на катастрофа,
- врши миграција наинформациските системи на јавниот секторво централизираната Владина дигитална инфраструктура,
- обезбедува служба за подршка и информации на јавните институции во однос на развојот и обезбедувањето на дигиталните услуги, согласно овој закон,
- го координира, планира и обезбедува пристапот до Интернет за органите на државната управа,
- дава мислење и предлози и учествува во изработка на закони, стратегии и планови од области поврзани со нејзината надлежност,
- донесува подзаконски акти потребни за спроведување на овој закон, и
- врши и други работи утврдени со овој закон.

Статут на Агенцијата

Член 6

(1) Организацијата и работењето на Агенцијата поблиску се уредува со Статутот на Агенцијата.

(2) Статутот на Агенцијата го донесува Комисијата на Агенцијата по претходно добиена согласност од Владата на Република Северна Македонија.

(3) Статутот на Агенцијата особено содржи одредби за:

- место и заштитен знак,
- изработка и употреба на печати на Агенцијата,

- застапување на Агенцијата,
- начин на именување на членови на Комисијата на Агенцијата;
- начин на именување на извршниот директор на Агенцијата,
- начин на именување и разрешување на членовите на Стручниот совет на Агенцијата,
- начин за донесување на општи, подзаконски и други акти на Агенцијата,
- обврска за вработените во однос на обезбедување доверливост на податоците и заштита на комерцијалните интереси на субјектите согласно овој закон,
- други одредби од значење за работењето на Агенцијата.

(4) Статутот на Агенцијата се објавува во Службен весник на Република Северна Македонија и на веб страната на Агенцијата.

Други акти на Агенцијата

Член 7

(1) Агенцијата донесува општи и подзаконски акти за работите од својата надлежност, Годишен извештај за работа на Агенцијата за претходната година, Годишна програма за работа на Агенцијата за наредната година, Годишна програма за обуки,

(2) Агенција одлучува за работите од својата надлежност со донесување на одлуки и решенија.

Соработка со меѓународни и домашни организации, институции и тела

Член 8

(1) Агенцијата согласно со своите надлежности,утврдени во членот 5 на овој Закон, а во насока на спроведување на одредбите од овој закон, соработува со домашни и меѓународни организации, институции и тела и со нив може да склучува меморандуми за соработка.

(2) Агенцијата согласно ставот (1) на овој член во областа на развој на ИКТ особено соработува со министерството за информатичко општество и администрација во областите поврзни во неговата надлежност.

(3) Агенцијата согласно ставот (1) на овој член во областа на безбедноста на мрежи и информациски ситеми особено соработува со домашни институции и тела надлежни за:

- безбедност и одбрана на Република Северна Македонија
- заштита на личните податоци,
- електронска идентификација и доверливи услуги,
- критична инфраструктура,

- работење на финансискиот сектор,
- цивилниот авиосообраќај,
-електронски комуникации,

(4) Агенцијата е должна со органот на државната управа надлежен за управување со критична инфраструктура во Република Северна Македонија редовно да соработува и разменува информации во однос на утврдување на критични субјекти во државата, за сајбер и не-сајбер ризици, закани и инцидентите кои влијаат на критичните субјекти, како и за преземените мерки како одговор на такви ризици, закани и инциденти.

(5) Агенцијата е должна со институциите и телата надлежни забезбедноста и одбраната на Република Северна Македонија, институциите и телата надлежни за електронска идентификација и доверливи услуги, работењето на финансискиот сектор како и телата надлежни за цивилниот авио сообраќај редовно да разменува информации за релевантни сајбер закани и инциденти.

(6) Агенцијата е должна да соработува со надлежното регулаторно тело за електронски комуникации во Република Северна Македонија за координирани проценки на безбедносни ризици кај добавувачи и производители на мрежна опрема за операторите, како и да соработува со други домашни надлежни институции и тела за координирани проценки на безбедносни ризици на суштински ланци на снабдување на ИКТ-услуги, ИКТ-системи и ИКТ-производи, земајќи ги предвид техничките и не-техничките фактори на ризик. Притоа Агенцијата ги има предвид идентификуваните фактори на ризик од страна на институциите на Европската Унија.

(7) Агенцијата согласно ставот (1) на овој член особено соработува со институции и тела на Европската Унија.

Податоци и информации што не ѝсе достапни на јавноста

Член 9

(1) На јавноста нема да ѝ бидат достапни податоци и информации што се сметаат за доверливи податоци, како и податоци и информации согласно со Законот за класифицирани информации.

(2) Агенцијата со акт ќе ги утврди податоците и информациите кои се сметаат за доверливи податоци.

(3) Членовите на Комисијата, извршниот директор на Агенцијата, членовите на Стручниот совет на Агенцијата и вработените во стручната служба на Агенцијата се должни да не ги откриваат доверливите податоци, како и комерцијалните интереси на субјектите согласно овој закон, без оглед на начинот на кој ги дознале. Обврската за не откривање на доверливите податоци како и на комерцијалните интереси на субјектите трае пет години по престанокот на работниот однос во Агенцијата или по престанокот на мандатот.

Отчетност за работата на Агенцијата

Член 10

(1) Агенцијата за својата работа дава отчет пред Владата на Република Северна Македонија со доставување на Годишен извештај за работа за претходната година и Годишна програма за работа за наредната година,

(2) Годишниот извештај за работа за претходната година, Агенцијата е должна да го достави до Владата на Република Северна Македонија, на усвојување, најдоцна до 31 март во тековната година и истиот особено содржи:

- извештај за реализацијата на активностите утврдени во годишната програма за работа на Агенцијата за претходната година,
- финансиски извештај за реализација на финансискиот план за претходната година и годишна сметка, со податоци за реализирани приходи, расходи, побарувања и обврски за претходната година групирани по структура и по организациска структура на Агенцијата,
- ревизорски извештај од независен меѓународен овластен ревизор и ревизорски извештај од Државниот завод за ревизија, доколку е извршена ревизија од него, како и став на Агенцијата во однос на резултатите од извршената ревизија.

(3) Годишната програма за работа за наредната година, Агенцијата ја изработува во соработка со Министерството за информатичко општество и администрација и е должна да ја достави до Владата на Република Северна Македонија, на усвојување, најдоцна до 30 октомври во тековната година и истата особено содржи:

- програма на планирани активности за наредната година што треба да биде во согласност со Стратегијата за сајбер безбедност и Планот за дигитална трансформација на јавниот сектори
- финансиски план за наредната година, кој содржи податоци за реализација на планираните активности, планираните приходи и расходи на Агенцијата за наредната година групирани по структура и по организациска структура на Агенцијата, како и предвидените капитални инвестиции на Агенцијата за наредната година.

(4) Годишната програма за работа на Агенцијата за наредната година може во текот на годината да се измени, по постапка предвидена за нејзиното донесување.

Органи на Агенцијата

Член 11

Органи на Агенцијата се:

- Комисија,
- Извршен директор, и
- Стручен совет.

Комисија

Член 12

(1) Комисијата се состои од пет члена кои ги именува и разрешува Владата на Република Северна Македонија,

(2) Предлог за именување на членови на Комисијата, до Владата на Република Северна Македонија доставуваат; Министерот за информатичко општество и администрација, Министерот за внатрешни работи, Министерот за одбрана, Министерот за финансии и Министерот за правда и тоа
- Министерот за информатичко општество и администрација, Министерот за внатрешни работи и Министерот за одбрана предлагаат по еден кандидат за член на Комисијата и истиот треба да има завршен VII/1 степен од областа на информатичкитеи комуникациските технологии;
-Министерот за финансии предлага еден кандидат за член на Комисијата и истиот треба да има завршен VII/1 степен од областа на економијата и
- Министерот за правда предлага еден кандидатза член на Комисијата со завршен VII/1 степен од областа на правото.

(3) Министрите од ставот (2) на овој член, предлогот за именување на член на Комисијата го доставуваат врз основа на претходно објавен јавен оглас. Јавниот оглас се објавува , во најмалку два дневни весници кои се објавуваат на целата територија на Република Северна Македонија од кои еден од весниците што се издаваат на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик и на веб страната на соодветното министерство и на Владата на Република Северна Македонија.

(4) Покрај условот за завршено образование утврден во ставот (2) на овој член , за член на Комисијата треба да биде предложено лице кое ги исполнува и следниве услови:

- 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
- има минимум пет години работно искуство во областа на информатичките и комуникациските технологии, правото или економијата и кој е познат во јавноста како експерт од соодветната област;
- поседува еден од следниве меѓународно признати сертификати или уверенија за активно познавање на англискиот јазик не постар од пет години:
  - ТОЕФЛИБТ најмалку 74 бода,
  - ИЕЛТС (IELTS) - најмалку 6 бода,
  - ИЛЕЦ (ILEC) (CambridgeEnglish: Legal) - најмалку Б2 (B2) ниво,
  - ФЦЕ (FCE) (CambridgeEnglish: First) – положен,
  - БУЛАТС (BULATS) - најмалку 60 бода и
  - АПТИС (APTIS) - најмалку ниво Б2 (B2).

(4) Комисијата од редот на своите членови, избира и разрешува претседател и заменик на претседателот на Комисијата на начин утврден во Деловникот за работа на Комисијата.

(5)Членовите на Комисијата се именуваат со мандат од четири години.

(6)Членовите на Комисијата не можат да бидат именувани повеќе од два последователни мандати.

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

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

(9)Во текот на времетраењето на својот мандат, членовите на Комисијата не можат да бидат пратеници во Собранието на Република Северна Македонија, членови на Владата на Република Северна Македонија, лица кои извршуваат должности во органите и телата на политички партии, членови на управни и надзорни органи на јавни претпријатија, вработени во органите на државната управа, вработени во единица на локална самоуправа,како и членови на друг вид асоцијација на правни и физички лица кои би можеле да доведат до конфликт на интересите.

(10)Член на Комисијата, неговиот/нејзиниот брачен другар или невенчан партнер, како и блиски роднини во права линија до второ колено, не можат да бидат:

- сопственици на удели или акции,директно или индиректно, во организации што извршуваат активности што директно спаѓаат под надлежност на Агенцијата,
- да бидат вработени или да вршат работиво или за правно лице кое врши дејност од областа што е во надлежност на Агенцијата утврдена со овој закон или во правно лице кое би можело да доведе до конфликт на интереси согласно со овој и друг закон или
- членови на управен или надзорен орган или да вршат раководна функција во правно лице кое врши дејност од областа што е во надлежност на Агенцијата утврдена со овој закон или во правно лице кое би можело да доведе до конфликт на интереси согласно со овој и друг закон.

(11) Во постапката за именување на член на Комисијата, предложениот кандидат е должен да достави изјава заверена на нотар дека нема неспоивост на функцијата, согласно овој член.

(12) Членовите на Комисијата се должни секоја година во февруари да доставуваат изјава заверена на нотар дека немаат неспоивост на функцијата, согласно овој член.

(13)Ако член на Комисијата има директен или индиректен приватен интерес во врска со донесувањето на одлуки од надлежност на Комисијата, членот е должен за тоа да ја извести Комисијата и да не учествува во одлучувањето по тоа прашање. Не известувањето на Комисијата е основ за негово разрешување и одговорност согласно закон.

(14) Начинот на именување на членовите на Комисијата поблиску се уредува во Статутот на Агенцијата.

Начин на работа и одлучување на Комисијата

Член 13

(1) Комисијата работи и одлучува на состаноци.

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

(3) Претседателот на Комисијата ги свикува состаноците на Комисијата по писмен предлог на Извршниот директор на Агенцијата, или по писмен предлог на тројца членови на Комисијата. Претседателот на Комисијата претседава на состаноците на Комисијата и ја претставува Комисијата, а во случај на негово отсуство или спреченост обврските ги извршува заменикот на претседателот на Комисијата.

(4) Извршниот директорот на Агенцијата присуствува и учествува на состаноците на Комисијата, без право на глас.

(5) На состаноците на Комисијата, без право на одлучување, можат да присуствуваат и членови на Стручниот совет на Агенцијата, вработени од стручната служба на Агенцијата на покана на Комисијата, 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 Комисијата и Статутот на Агенцијата.

(6) Одлуките и другите акти на Комисијата ги потпишува претседателот на Комисијата, а во случај на негова спреченост, заменикот на претседателот на Комисијата, најдоцна во рок од три дена од денот на нивното донесување.

(7) Материјалите за состаноците на Комисијата ги подготвува стручната служба на Агенцијата по предлог на Извршниот директор на Агенцијата и истите се доставуваат до сите членови на Комисијата, на начин и во рок утврден во Деловникот за работа на Комисијата и Статутот на Агенцијата..

(8) Членовите на Комисијата имаат право на:

- месечен надоместок во висина од две просечни месечни плати исплатени во Република Северна Македонија за претходна година според податоците објавени од Државниот завод за статистика.
- надоместок за патни трошоци за оние членови на Комисијата кои живеат надвор од Скопје кога присуствуваат на состаноците на Комисијата и надоместок за патни трошоци, сместување и дневници за службено патување согласно со закон.

(9) Месечниот надоместок од ставот (8) на овој член не се исплатува доколку во тековниот месец не се одржи состанок, како и за неприсуство на одржан состанок.

(10) Средствата за месечниот надоместок и на другите трошоци од ставот (8) на овој член, на членовите на Комисијата се обезбедуваат од средствата на Агенцијата утврдени со финансискиот план.

(11) Дневниот ред, записниците од состаноците на Комисијата и донесените одлуки кои не содржат доверливи податоци согласно овој закон се објавуваат на веб-страната на Агенцијата во рок од седум дена од денот на одржувањето на состанокот.

(12) Работата на Комисијата и начинот на донесување на одлуки поблиску се уредува со Деловник за работа на Комисијата.

Надлежности на Комисијата

Член 14

Комисијата ги има следниве надлежности:

- донесува Статут по претходно добиена согласност од Владата на Република Северна Македонија;
- донесува Деловник за својата работа во согласност со овој закон и Статутот на Агенцијата;
- усвојува Кодекс на однесување на вработените во MKD-CSIRT, по предлог на Извршниот директор на Агенцијата;
- го одобрува Годишниот извештај за работа за претходната година на Агенцијата и Годишната програма за работа за наредната година на Агенцијата;
- ја усвојува завршната сметка на Агенцијата;
- го усвојува Годишниот план за јавни набавки;
- го усвојува Годишниот план за обуки;
- го предлага Планот за одговор на сајбер безбедносни инциденти од големи размери и кризидоставен од извршниот директор на Агенцијата;
- усвојува Годишен извештај за состојбите во сајбер безбедноста;
- го одобрува предлог Планот за дигитална трансформација на јавниот сектор,доставен од извршниот директор на Агенцијата;
- дава претходна согласност за склучување на меморандуми за соработка;
- предлага студииза изводливост согласно овој закон доставени од извршниот директор на Агенцијата;
- дава претходна согласност за склучување на договори во име на Агенцијата;
- дава претходна согласност на одлука за спроведување на постапка за јавна набавка;

- дава претходна согласност за вработување во Агенцијатаили престанок на договорот за вработување на вработен во Агенцијата;
- ги усвојува кварталните извештаи за работа на Агенцијата доставени од извршниот директор на Агенцијата;
- донесува подзаконски акти и други акти за спроведување на овој Закон;
- донесува општи акти за работењето на Агенцијата, утврдени во Статутот на Агенцијата;
- го именува и разрешува извршниот директор на Агенцијата во согласност со овој закон; и
- ги именува и разрешува членовите на Стручниот совет на Агенцијата, во согласност со овој закон.

Разрешување на член на Комисијата

Член 15

(1) Владата на Република Северна Македонија, по предлог на Претседателот на Комисијата на Агенцијата, може да разреши член на Комисијата пред истекот на мандатот:

- на негово барање,
- ако настапила некоја од пречките за членство во Комисијата предвидени во членот 12 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 Комисијата едно по друго или од вкупно пет состаноци за време од една година,
- ако се утврди дека членот на Комисијата во постапката за негово именување дал невистинити податоци или пропуштил да изнесе некои информации кои се важни за неговото именување.

(2) Недоставување на Годишниот извештај за работа на Агенцијата согласно членот 10 од овој закон до Владата на Република Северна Македонија е причина за колективното разрешување на Комисијата.

(3) За исполнување на условите за предвремено разрешување на член на Комисијата, предвидени во ставот (1) на овој член претседателот, односно заменикот на претседателот на Комисијата 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.

Извршен директор на Агенцијата

Член 16

(1) Со Агенцијата раководи извршен директор.

(2) Извршниот директорот на Агенцијата го именува и разрешува Комисијата на Агенцијата.

(3) За именување на извршен директор се објавува јавен оглас, во најмалку два дневни весници кои се објавуваат на целата територија на Република Северна Македонија од кои еден од весниците што се издаваат на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик и на веб страната на Агенцијата..

(4) Мандатот на извршниот директор трае четири години. Извршниот директор не може да биде именуван повеќе од два последователни мандати.

(5) Извршниот директор на Агенцијата е професионално ангажиран во Агенцијата со полно работно време.

(6) Ако мандатот на извршниот директор на Агенцијата е завршен, а постапката за именување на извршен директор не е завршена, извршниот директор на Агенцијата продолжува да ја врши функцијата се додека не се именува извршен директор, но не подолго од шест месеци.

Именување на извршен директор

Член 17

(1) За Извршен директор на Агенцијата може да биде именувано лице кое ги исполнува следниве услови:

-да 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;

-да има завршен VII/1 степен од областа на информатичко комуникациски технологии, односно да има стекнати најмалку 240 кредити според ЕКТС;

- има минимум пет години работно искуство во областа на информатичко комуникациски технологии;

- поседува еден од следниве меѓународно признати сертификати или уверенија за активно познавање на англискиот јазик не постар од пет години:

  - ТОЕФЛИБТ најмалку 74 бода,

  - ИЕЛТС (IELTS) - најмалку 6 бода,

  - ИЛЕЦ (ILEC) (CambridgeEnglish: Legal) - најмалку Б2 (B2) ниво,

  - ФЦЕ (FCE) (CambridgeEnglish: First) – положен,

  - БУЛАТС (BULATS) - најмалку 60 бода и

  - АПТИС (APTIS) - најмалку ниво Б2 (B)

(2) Начинот на именување на Извршниот директор на Агенцијата поблиску се уредува во Статутот на Агенцијата.

Неспоивост на функцијата извршен директор на Агенцијата

Член 18

(1) Извршниот директор на Агенцијата, неговиот брачен другар или невенчан партнер, како и блиски роднини во права линија до второ колено, не можат да бидат:
   - сопственици на удели или акции,директно или индиректно, во организации што извршуваат активности што директно спаѓаат под надлежност на Агенцијата,
   - да бидат вработени или да вршат работиво или за правно лице кое врши дејност од областа што е во надлежност на Агенцијата утврдена со овој закон или во правно лице кое би можело да доведе до конфликт на интереси согласно со овој и друг закон или
   - членови на управен или надзорен орган или да вршат раководна функција во правно лице кое врши дејност од областа што е во надлежност на Агенцијата утврдена со овој закон или во правно лице кое би можело да доведе до конфликт на интереси согласно со овој и друг закон.

(2) Во постапката за именување на извршен директор на Агенцијата, кандидатот е должен да достави изјава заверена на нотар дека нема неспоивост на функцијата, согласно овој член.

(3) Извршниот директор е должен секоја година во февруари да доставува изјава заверена на нотар дека нема неспоивост на функцијата, согласно овој член.

Предвремено разрешување на извршниот директорна Агенцијата

Член 19

(1) Извршниот Директор на Агенцијата може да биде разрешен пред истекот на неговиот мандат во следниве случаи:

- на негово барање,
- ако не е во можност да ја извршува должноста повеќе од шест месеци во континуитет,
- прифаќање на функција или работа што е неспојлива со неговата функција на директор на Агенцијата согласно со членот 18 од овој закон,
- ако е правосилно осуден за кривично дело за кое му е изречена казна затвор во траење подолго од шест месеци или му е изречена мерка на безбедност забрана на вршење на професија, дејност или должност, во траење подолго од шест месеци или
- ако се утврди дека 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 негово предвремено разрешување, Извршниот директор е должен веднаш, а најдоцнаво рок од три дена од денот на исполнувањето на условите од ставот (1) на овој член да ја извести Комисијата на Агенцијата.

Надлежност на извршниот директор на Агенцијата

Член 20

Извршниот директорот на Агенцијата раководи со работата на Агенцијата, е одговорен за законитото работење на Агенцијата и ги има следниве надлежности:

- ја застапува и претставува Агенцијата,
- потпишува договори и меморандуми за соработка во име на Агенцијата по претходно добиена согласност од Комисијата,
- ги предлага Статутот, Годишниот извештај за работа на Агенцијата за претходната година, Годишната програма за работа на Агенцијата за наредната година, како и завршната сметка на Агенцијата, што ги усвојува Комисијата на Агенцијата,
- доставува квартални извештаи за работењето на Агенцијата што ги одобрува Комисијата на Агенцијата,
- ги предлага членовите на Стручниот совет на Агенцијата што ги именува и разрешува Комисијата на Агенцијата,
- ги предлага општите и подзаконските акти кои произлегуваат од овој закон,
- го предлага Годишниот план за јавни набавки, и Годишниот план за обуки што го усвојува Комисијата на Агенцијата,
- го предлага Планот за дигитална трансформација на јавниот сектор,

- презема мерки во согласност со овој закон во случаите кога е извршена повреда на одредбите од овој закон или на прописите донесени врз основа на него,
- донесува одлуки, решенија и други акти по прашања од надлежност на Агенцијата во согласност со овој закон и Статутот на Агенцијата,
- дава овластувања во рамките на своите надлежности,
- овластува лица за вршење на надзор, во согласност со овој Закон,
- донесува годишна програма за вршење на надзор и поднесува годишен извештај за спроведен надзор како составен дел на годишниот извештај за работа на Агенцијата за претходната година, и
- врши и други работи утврдени со овој закон и Статутот на Агенцијата.

Стручен совет на Агенцијата

Член 21

(1) Стручниот совет на Агенцијата се формира со цел да се обезбеди високо ниво на транспарентност во работењето на Агенцијата, а особено во делот на дигиталната трансформација и за заштита на интересите на засегнатите страни согласно овој закон.

(2) Комисијата на Агенцијата именува и разрешува членови на Стручниот совет на Агенцијата, по предлог на извршниот директор на Агенцијата.

(3) Стручниот совет на Агенцијата е составен од единаесет члена кои се познати експерти за јавноста, претставници на релевантните засегнати страни и тоа:

- од индустријата на ИКТ, четири члена;
- од операторите на суштински услуги согласно овој Закон, два члена;
- од операторите на важни услуги согласно овој Закон, два члена; и
- од академскиот сектор од областа на информациско комуникациските технологии, односно сајбер безбедноста три члена.

(4) Мандатот на членовите на Стручниот совет трае три години.

(5) Начинот на именување и разрешување на членовите на Стручниот совет на Агенцијата, поблиску се уредува со Статутот на Агенцијата, при што треба да се обезбеди транспарентност во постапката.

Начин на работа на Стручниот совет на Агенцијата

Член 22

(1) Стручниот совет на Агенцијата работи на состаноцикои ги свикува и со кои претседава извршниот директор на Агенцијата.

(2) Извршниот директор свикува состанок на Стручникот совет најмалку еднаш на три месеци.

(3) На состаноците на Стручниот совет, по покана на Извршниот директор можат да присуствуваат и да учествуваат во неговата работа и други лица за кои Извршниот директор смета дека се релевантни да присуствуваат на состанокот.

(4) Стручниот совет на Агенцијата го советува Извршниот директор на Агенцијата во врска со спроведување на надлежностите на Агенцијата во согласност со овој Закон, а особено при подготовката на Годишната програма за работа на Агенцијата за наредната година, како и за обезбедување на транспарентна комуникација со релевантните засегнати страни по прашања кои се однесуваат на спроведување на Годишната програма за работа на Агенцијата.

(5) Членовите на Стручниот совет на Агенцијата немаат право на паричен надоместок.

Организација и вработување во Агенцијата

Член 23

(1) Стручните, нормативно-правните, управните, управно-надзорните, материјално-финансиските, сметководствените, информатичките и други работи на Агенцијата 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 Агенцијата, како и висината на коефициентот на основната плата ги пропишува Комисијата. Основната плата на вработените во стручната служба на Агенцијата кои имаат завршен VII/1 степен од областа на информатичките икомуникациските технологии треба најмалку да е во висина на просечната плата исплатена во секторот Информатика и комуникации, согласно последниот извештај на Државниот завод на статистика од минатата година.

Финансирање на Агенцијата

Член 24

(1) Средствата за финансирање на оперативните трошоци на Агенцијата (плати, надоместоци, обуки, трошоци за комунални услуги, потрошен материјал, технички средства и сл) се обезбедуваат од Буџетот на Република Северна Македонија, согласно усвоената Годишна програма за работа на Агенцијата за наредната година.

(2) Вкупните годишни средства од ставот (1) на овој член не може да бидат помали од 0,6% од реализираните даночни приходи утврдени во последната донесена завршна сметка на Буџетот на Република Северна Македонија.

(3) Дополнителни средства од Буџетот на Република Северна Македонија се издвојуваат за годишни софтверски лиценци и капитални инвестиции на Агенцијата за развој на своите надлежности за сајбер безбедност и дигитална трансформација, согласно овој закон. Дополнителните средства за капитални инвестиции се одобруваат врз основа на усвоена Студија за изводливост .

(4) Владата, по предлог на Агенцијата ја усвојува Студијата од ставот (3) на овој член во рок од три месеци од денот на нејзиното доставување.

(5) Доколку Агенцијата не ги потроши сите обезбедени средства од Буџетот на Република Северна Македонија во текот на годината, вишокот средства утврдени согласно Годишниот финансискиот извештај се враќа во Буџетот на Република Македонија.

(6) Агенција може да се финансира и од донации, меѓународни проекти и грантови за сајбер безбедност и дигиталната трансформација.

Промовирање употреба на алатки и апликации на отворен код и отворени стандарди

Член 25

(1) Агенцијата промовира употреба на сајбер безбедносни алатки и апликации со отворен код и отворени стандарди, со цел да се обезбеди повисок степен на отвореност, развој на индустриските иновации, користење на заедницата на програмери за овозможување диверзификација на добавувачи, како и за значително намалување на трошоците што е од особено значење за малите и средни претпријатија кои се соочуваат со значителни трошоци за имплементација на сајбер безбедносни алатки и апликации.

(2) Агенцијата во процесот на изготвувањето на техничите решенија и техничките спецификации за потребите на дигиталната трансформација потребно е да цели кон користење на отворен код, отворени стандарди и технологии во процесот на набавка на уреди, софтверски решенија и софтверски лиценци.

Обуки и подигнување на јавната свест за ИКТ

Член 26

(1) Агенцијата организира и спроведува специјализирани обуки за своите вработени кои извршуваат работни задачи од областа на сајбер безбедноста, надзорот и дигиталната трансформација.

(2) Агенцијата организира и спроведува обуки за вработени во институциите на јавниот сектор, со цел да се стекнат со дигитални вештини и исполнување на обврските, односно целите утврдени со овој Закон.

(3) Агенцијата организира и спроведува кампањи за подигнување на јавната свест, особено за важноста на сајбер безбедноста, користењето на дигитални услуги и дигиталната трансформација на општеството.

(4) Комисијата на Агенцијата, по предлог на Извршниот директор на Агенцијата, најдоцна до 1 март во тековната година донесува Годишна програма за обуки која содржи:
- Тема на обуката,
- Начин на реализација,
- Носител на обуката,
- Целна група и
- Потребни Финансиски средства.

(5) За спроведување на обуките од ставот (1) на овој член, а имајќи го предвид ставот (2) на овој член, Агенцијата може да склучува меморандум за соработка за спроведување на обука со институции од јавниот сектор,

(6) Агенцијата може, по пат на јавна набавка да склучи договор за спроврдување на обуките од ставот (1) на овој член со правни лица од приватен сектор, во случај кога одредена обука не може да се релизира поради недостаток на стручни и обучени вработени во Ахенцијата или институциите од јавниот сектор, согласно ставот (3) на овој член.

(7) Агенцијата е должна во Годишниот извештај за работа од членот 10 на овој Закон, посебно да ја прикаже реализацијата на Годишниот план за обуки со податоците утврдени во ставот (2) на овој член

(8) Агенцијата, со подзаконски акт подетално ќе го утврди начинот на спроведување на обуките од ставот (1) на овој член.

III. САЈБЕР БЕЗБЕДНОСТ

III.1 ОПШТИ ОДРЕДБИ

Опфат на примена на законот во однос на сајбер безбедноста

Член 27

(1) Одредбите на овој закон, во однос на сајбер безбедноста се применуваат на органите на државната управа и правните лица на кои со закон им е доверено да вршат јавни овластувања.

(2) Одредбите на овој закон во однос на сајбер безбедноста се применуваат и на работата на субјектите, односно правните лица со регистрирано седиште во Република Северна Македонија а кои се сметаат за средни или големи претпријатија согласно Закон, и обезбедуваат услуги во секторите:

- Енергетика,
- Транспорт,
- Банкарство,
- Финансиски пазар,

- Здравство,
- Снабдување на вода за пиење и дистрибуција,
- Отпадни води,
- Дигитална инфраструктура,
- Управување со ИКТ-услуги (B2B),
- Вселена,
- Дигитални услуги,
- Поштенски и курирски услуги,
- Управување со отпад,
- Изработка, производство и дистрибуција на хемикалии,
- Производство, преработка и дистрибуција на храна,
- Производство,
- Истражување.

(3) Одредбите на овој закон во однос на сајбер безбедностасе применуваат и на правните лица од ставот (2) на овој член независно од нивната големина, доколку:

а) правното лице е:

- давател/оператор на јавни електронски комуникациски мрежи или јавно достапни електронски комуникациски услуги,
- давател на доверливи услуги,
- регистар на имиња на врвни домени или
- давател на услуги за DNS;

б) правното лице е единствен давател на услуга во Република Северна Македонија , која е суштинска за одржување на општествени или економски активности;

в) нарушувањето во функционирањето на услугата што ја обезбедува правното лице има значително влијание врз јавната безбедност, јавната заштита или јавното здравје;

г) нарушувањето во функционирањето на услугата што ја обезбедува правното лице предизвикува значителни системски ризици, особено во секторите во кои таквото нарушување може да има прекугранично влијание;

д) правното лице поради својата посебна важност, се смета за критично за одреден сектор или тип услуга или за други меѓусебно зависни сектори во Република Северна Македонија.

ѓ) правните лица кои се сопственици/оператори на критична инфраструктура, согласно Закон,

е) правните лица што обезбедуваат услуги за регистрација на имиња на домени.

(4) Овој закон не се применува на Собранието на Република Северна Македонија, судовите, јавните обвинителства, државното правобранителство, Народната банка и единиците на локалната самоуправа во Република Северна Македонија.

(5) Овој Закон не се применува на државните органи и правните лица на кои со закон им е доверено да вршат јавни овластувања од областа на безбедноста и одбраната на Република Северна Македонија.

(6) Обврските утврдени со овој Закон не подразбираат давање информации чие откривање би било спротивно на интересите на националната безбедност, јавната безбедност или одбраната на Република Северна Македонија.

(7) Субјекти, односно претпријатија, опфатени во секторите од ставот (2) на овој член се:

а) Во секторот Дигитална инфраструктура:

- даватели на услуги на точки за размена на интернет-сообраќај,
- даватели на услуги за DNS, со исклучок на оператори на коренски сервери за имиња,
- регистар на имиња на врвни домени,
- даватели на услуги за компјутерска обработка во облак,
- даватели на услуги за податочен центар,
- даватели на услуги за мрежи за испорака на содржини,
- даватели на доверливи услуги,
- даватели/оператори на јавни електронски комуникациски мрежи, и
- даватели/оператори на јавнодостапни електронски комуникациски услуги.

б) Во секторот Управување со ИКТ-услуги (B2B):

- давател на управувани услуги, и
- давател на управувани безбедносни услуги.

в) Во секторот Дигитални услуги:

- даватели на услуга на интернет-пазар,
- даватели на услуга на интернет-пребарувач, и
- даватели на платформа за услуги за социјални мрежи,

г) Во секторот Истражување: истражувачки организации.

(8) Владата на Република Северна Македонија по предлог на Агенцијата утврдува листа на потсектори кои се опфатени во рамките на секторите утврдени во ставот (2) на овој член како и видовите на претпријатија во рамките на секторите, односно потсекторите.

Оператори на суштински услуги и оператори на важни услуги

Член 28

(1) За оператори на суштински услуги, во смисла на овој Закон, се сметаат:

а) субјектите, односно правните лица определени во членот 27 став (2) алинеи од 1 до 10 на овој Закон, кои се сметаат за големи претпријатија согласно закон;

б) даватели на квалификувани доверливи услуги, регистар на имиња на врвни домени или давател на услуги за DNS, независно од нивната големина;

в) оператори, односно даватели на јавни електронски комуникациски мрежи и/или јавно достапни електронски комуникациски услуги кои се сметаат за средни или големи претпријатија, согласно закон;

г) органи на државната управа и правни лица на кои со закон им е доверено да вршат јавни овластувања на државно ниво;

д) субјектите, односно правните лица, независно од нивната големина кои обезбедуваат услуги од секторите определениво членот 27 став (2) од овој закон, а кои Агенцијата, врз основа на членот 27 став (3) точки б), в) г) и д) од овој Закон ги има утврдено како оператори на суштински услуги;

ѓ) правни лица кои се утврдени како сопственици/оператори на критична инфраструктура, согласно Закон;

(2) За оператори на важни услуги, во смисла на овој закон, се сметаат сите субјекти од членот 27 став (2) на овој закон, а кои согласно ставот (1) на овој член не се утврдени како оператори на суштински услуги, вклучувајќи ги и субјектите кои Агенцијата, врз основа на членот 27 став (3) точки б), в) г) и д) од овој Закон ги има утврдено како оператори на важни услуги.

(3) Агенцијата, врз основа на ставовите (1) и (2) на овој член донесува одлука со која определува оператор на суштински услуги или оператор на важни услуги. Агенцијата, редовно ја преиспитува одлуката, а најмалку на секои две години.

(4) Агенцијата во одлуката од ставот (3) на овој член на субјектот определен во истиот став му утврдува обврски согласно со овој Закон.

(5) Агенцијата води Регистар на оператори на суштински услуги и оператори на важни услуги согласно ставот (3) на овој член. Регистарот не е јавно достапен и истиотредовно се ажурира.

(6) Субјектите определени во ставот (3) на овој член, а заради водење на регистарот од ставот (5) на овој член, се должни на Агенцијата да и ги достават следните податоци:

а) назив на субјектот

б) податоци за овластеното лице за спроведување на обврските утврдени со овој закон;

в) адреса и податоци за контакт, вклучувајќи адреса на е-пошта, телефонски броеви и ИП-адресен простор

г) релевантниот сектор и/или потсектор од членот 27 ставови (2) и (8) од овој Закон

д) листа на држави во кои субјектот обезбедува услуги од опфатот на примената на овој закон

(7) Субјектите определени во ставот (3) на овој член се должни на Агенцијата да и ја достават секоја измена на податоците утврдени во ставот (6) на овој член, во рок од 15 дена од денот на настаната измена.

(8) Агенцијата со подзаконски акт го пропишува начинот на определување на субјектите од ставот (3) на овој член, како иначинот и образецот за доставување на податоците утврдени во ставот (6) на овој член.

(9) При донесувањето на подзаконскиот акт од ставот (8) на овој член, Агенцијата ги зема предвид препораките и насоките на Европската комисија и Агенцијата за сајбер безбедност на Европската унија(ENISA).

(10) Пред да го донесе подзаконскиот акт од ставот (8) на овој член Агенцијата е должна да се консултира со субјектите од ставот (3) на овој член и да ги земе предвид нивните мислења и забелешки.

Субјекти кои немаат регистрирано седиштево Република Северна Македонија

Член 29

(1) Доколку одредени субјекти немаат регистрирано седиште во Република Северна Македонија, а се даватели на услуги за DNS, регистри на имиња на врвни домени, даватели на услуги за регистрација на имиња на домени, даватели на услуги за компјутерска обработка во облак, даватели на услуги за податочен центар, даватели на услуги за мрежи за испорака на содржини, даватели на управувани услуги, даватели на управувани безбедносни услуги, даватели на услуга на интернет пазар, даватели на услуги на -интернет-пребарувачи или даватели на платформи за услуги за социјални мрежи, должни се да именуваат свој претставник за Република Северна Македонија.

(2) Агенцијата води регистар на субјектите од ставот (1) од овој член.

(3) Субјектите определени во ставот (1) на овој член заради водење на регистарот од ставот (2) на овој член, се должни на Агенцијата да ѝги достават следните податоци:

- име на субјектот;
- релевантниот сектор, потсектор и видот на субјектот согласно членот 27 од овој закон;
- адресата на седиштето на субјектот и на неговиот преставник;
- податоци за контакт, вклучувајќи адреси на е-пошта и телефонски броеви;
- адресен простор на субјектот.

(4) Субјектите од ставот (1) на овој член се должни да ја известат Агенцијата за секоја измена на податоците од ставот (3) на овој член, во рок од три месеци од датумот на извршената измена.

(5) Ако субјектите од ставот (1) на овој член не постапат во согласност со одредбите на овој член, Агенцијата е должна да ја извести Европската комисија и ENISA , доколку се работи за субјект од земја членка на Европската унија, а доколку се работи за субјект кој не е од земја членка на Европската унија, Агенцијата ќе ја извести соодветната држава, односно нејзиното надлежно тело за сајбер безбедност.

База на податоци за регистрација на имиња на домени
Член 30

(1) Со цел да се придонесе за безбедноста, стабилноста и отпорноста на DNS,регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени се должни да собираат и одржуваат точни и целосни податоци за регистрација на имиња на домени во посебна база на податоци, притоа водејќи сметка за заштитата на личните податоци.

(2) Базата на податоци од ставот (1) на овој член треба да содржи информации потребни за идентификација на носителот на името на доменот и контактните точки кои управуваат со имињата на домени во рамките на врвните домени, како и контактите со нив. Информациите треба да содржат податоци за:

- името на доменот;
- датумот на регистрација;
- името на корисникот на доменот, адресата на неговата е-пошта и телефонскиот број за контакт;
- адресата на е-пошта и телефонскиот број за контакт на контактните точки кои управуваат со имињата на доменот, доколку се разликуваат од податоците за корисникот на доменот.

(3) Регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени се должни да воспостават политики и постапки, вклучително и постапки за проверка, со што се обезбедува дека базата на податоци од ставот (1) на овој член содржи точни и целосни информации. Политиките и постапките треба јавно да се објават.

(4) Регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени, по извршената регистрација на домени, без непотребно одлагање јавно да ги објават податоците за регистрација, притоа водејќи сметка за заштитата на личните податоци.

(5) Регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени се должни да обезбедат пристап до одредени податоци за регистрацијата на имиња на домени, врз основа на законски и оправдани барања, доставени од легитимни баратели за пристап, а при тоа водејќи сметка за заштитата на личните податоци. Регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени се должни без непотребно одлагање, а најдоцна во рок од 72 часа од приемот на барањето за пристап, да одговорат на таквото барање,

(6) Со цел исполнување на обврските утврдени во овој член, регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени се должни меѓусебно да соработуваат.

III.2 РАМКА ЗА САЈБЕР БЕЗБЕДНОСТ

Поддршка на малите и средните претпријатија
Член 31

(1) Агенцијата преку своја контакт точка за поддршка на мали и средни претпријатија, особено оние кои се исклучени од опфатот на овој закон, ќе обезбеди лесно достапни насоки и помош за нивните специфични потреби поврзани со сајбер безбедност или нивно насочување до надлежни тела, како и за решавање на предизвиците кои ги имаат во ланците за снабдување на ИКТ услуги, ИКТ системи и ИКТ производи

(2) Агенцијата може на микро и мали претпријатија кои немаат можности, да им обезбеди одредени услуги, како на пример, конфигурирање веб-локации и евиденции на податоци (логови).

Промовирање на активна сајберзаштита
Член 32

(1) Агенцијата како дел од националната сајбер стратегија согласно членот33 од овој закон, треба да промовира и подржува активна сајбер заштита, односно наместо реактивен одговор, сајбер заштитата да подразбира активна превенција, откривање, следење, анализа и ублажување на повредите на безбедноста на мрежите, комбинирани со користење на капацитетите кои се применуваат во и надвор од мрежата која е жртва на сајбер напад.

(2) Агенцијата согласно Националната стратегија за сајбер безбедностј од членот 33 на овој закон може за одредени субјекти бесплатно да понуди услуги или алатки како што се услугиза самостојна проверка и алатки за откривањеи услуги за отстранување.

Национална стратегија за сајбер безбедност

Член 33

(1) Владата на Република Северна Македонија, на предлог на Министерството за информатичко општество и администрација, донесува Национална стратегија за сајбер безбедност. Министерството за информатичко општество и администрација предлогот го подготвува во соработка со Агенцијата, државните органи и правните лица на кои со закон им е доверено да вршат јавни овластувања од областа на безбедноста и одбраната на РСМ.

(2) Со националната стратегија од ставот (1) на овој член се дефинираат стратешките цели, ресурсите потребни за постигнување на целите, соодветни политики и регулаторни мерки со цел да се постигне и одржи високо ниво на сајбер безбедност.

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

- цели и приоритети на стратегијата за сајбер безбедност што ги опфаќа особено секторите наведени во членот 27 од овој закон;
- рамка за управување за постигнување на целите и приоритетите наведени во ачинеја 1 од овој став, вклучувајќи ги и политиките наведени во ставот(4) од овој член;
- рамка за управување со која се дефинираат улогите и одговорностите на релевантните засегнати страни на национално ниво, подржувајќи ја соработката и координацијата со Агенцијата и другите надлежните органи и тела во државата;
- механизам за утврдување на релевантните средства и проценка на ризиците во државата;
- идентификација на мерки кои обезбедуваат подготвеност, одговор и закрепнување од инциденти, вклучително и соработка помеѓу јавниот и приватниот сектор, согласно овој закон;
- список на надлежни органи и засегнати страни кои се вклучени во спроведувањето на националната стратегија за сајбер безбедност;
- рамка на политика за обезбедување засилена координација помеѓу Агенцијата и органот на државната управа надлежен за управување со критична инфраструктура, со цел споделување информации за ризици, сајбер закани и инциденти, како и за не-сајбер ризици, закани и инциденти и извршување на надзорни задачи, по потреба;
- план, вклучувајќи и неопходни мерки, за подигнување на свесноста кај граѓаните за сајбер-безбедноста.

(4) Националната стратегија за сајбер безбедност од ставот(1) на овој член, треба да содржи политики за:

- адресирање на сајбер безбедноста во ланецот за снабдување на ИКТ производи и ИКТ услуги што ги користат субјектите во обезбедувањето на нивните услуги;
- вклучување и дефинирање на сајбер безбедносни барања за ИКТ производи и ИКТ услуги во јавните набавки, вклучувајќи во однос на сајбер безбедносна сертификација, шифрирањеи употребата на сајбер безбедносни производи со отворен код согласно овој закон;

- управување на ранливости, вклучувајќи промовирање и олеснување на координирано откривање на ранливост согласно член 40 од овој закон ;
- одржување на достапност, интегритет и доверливост на јавното јадро на отворен интернет;
- промовирање на развојот и интеграција на релевантни напредни технологии со цел да се имплементираат најсовремени мерки за управување со сајбер безбедносни ризици;
- промовирање и развивање на едукација и обуки за сајбер-безбедност, вештини за сајбер-безбедност, подигање на свеста и иницијативи за истражување и развој во областа на сајбер безбедност, како и насоки за најдобри практики и контроли за сајбер хигиена, насочени кон граѓаните, засегнатите страни и субјектите;
- поддршка на академските и истражувачките организации во развој, подобрување и потикнување на воведување алатки за сајбер безбедност и безбедна мрежна инфраструктура;
- релевантни процедури и соодветни алатки за размена на информации со цел поддршка на доброволното споделување информации за сајбер-безбедноста помеѓу субјектите согласно овој закон;
- зајакнување на сајбер отпорноста и основното ниво сајбер хигиена кај малите и средни претпријатија, особено оние кои се исклучени од опфатот на овој закон, преку обезбедување лесно достапни насоки и помош за нивните специфични потреби, согласно овој закон;
- промовирање на активна сајбер заштита.

(5) Националната стратегија за сајбер безбедност од ставот(1) на овој член, се ажурира на секои пет години.

Единствена точка за контакт за безбедност на мрежни и информациски системи

Член 34

(1) Единствената точка за контакт за безбедност на мрежни и информациски системи (во натамошниот текст: Единствена точка за контакт) има функција на поврзување со цел да се обезбеди прекугранична соработка во областа на

безбедноста на мрежните и информациски системи со релевантни државни органи и тела на други држави, а по потреба и со Европската комисија и ENISA.

(2) Единствената точка за контакт од ставот (1) на овој член е надлежна да проследи известување за значаен инцидент со прекугранично влијание до точката за контакт или еквивалентно такво тело на друга засегната држава.

(3) Единствената точка за контактод ставот (1) на овој член обезбедува меѓусекторска соработка со другите надлежни тела на национално ниво.

(4) Единствената точка за контакт од ставот (1) на овој членпримените релевантни информации за инциденти од меѓународни надлежни тела ги проследува до другите национални надлежни тела согласно овој закон.

(5) Функцијата на единствената точка за контактод ставот (1) на овој член ја врши Агенцијата.

План за одговор на сајбер безбедносни инциденти од големи размери и кризи

Член 35

(1) Владата на Република Северна Македонија по предлог на Агенцијата усвојува План за одговор на сајбер безбедносни инциденти од големи размери и кризи, во кој ќе бидат утврдени целите и обврските во управувањето со сајбер безбедносни инциденти од големи размери и кризи.

(2) Агенцијата го предлага Планот од ставот (1) на овој член во соработка со Министерството за информатичко општество и администрација и другите државни органи и тела што имаат надлежност поврзана со управувањето со кризи.

(3) Планот од ставот (1) на овој член особено содржи:

- цели на мерките и активностите за обезбедување национална подготвеност;
- задачите и надлежностите на Агенцијата и другите надлежни органи и тела;

- процедурите за управување со сајбер кризи, нивната интеграција во општата национална рамка за управување со кризи и каналите за размена на информации;
- мерки за национална подготвеност, вклучувајќи вежби и активности за обука;
- релевантните јавни и приватни засегнати страни и инволвирана инфраструктура;
- процедури и обврски помеѓу државни органи и тела за да се обезбеди ефективно учество и поддршка на државата во координирано управување со сајбер безбедносни инциденти од големи размери и кризи на ниво на регион или пошироко.

(4) Агенцијата соработува со организациите и мрежите на Европската Унија надлежни за управување со сајбер безбедносни инциденти од големи размери и кризи (EU-CyCLONe).

Национално тело за одговор на компјутерски инциденти (MKD-CSIRT)

Член 36

(1) Национално тело за одговор на компјутерски инциденти (MKD-CSIRT) е посебна организациона единица во состав на Агенцијата.

(2) MKD-CSIRT е надлежно тело за справување со инциденти, согласно точно пропишана процедура, во чиј опфат спаѓаат најмалку секторите и потсекторите утврдени во членот 27 од овој закон, односно операторите на суштински услуги и операторите на важни услуги согласно членот 28 од овој закон.

(3) MKD- CSIRT треба да располага со соодветна, безбедна и еластична комуникациска и информациска инфраструктура преку која се разменува информации со операторите на суштински услуги и операторите на важни

услуги и со други релевантни субјекти. За таа цел, MKD-CSIRT промовира користење алатки за безбедна размена на информации.

(4) MKD-CSIRT соработува и таму каде е соодветно разменува релевантни информации во согласност со членот 47 од овој закон.

(5) MKD-CSIRT може да учествува во мрежата на CSIRT на Европската Унија и на други еквивалентни такви меѓународни мрежи.

(6) MKD-CSIRT воспоставува односи за соработка со националните тимови за одговор на сајбер безбедносни инциденти од други држави, при што за да се обезбеди ефикасна и безбедна размена на информации, се користат релевантни протоколи за споделување информации. При тоа, размената на лични податоци се обезбедуваат согласно закон.

(7) MKD-CSIRT во својата работа и развој ги зема предвид препораките и насоките на Европската комисија и Агенција за сајбер безбедност на Европската унија (ENISA).

Услови кои треба MKD-CSIRT да ги исполни

Член 37

(1) MKD-CSIRT треба да ги исполнува следните услови:

- да обезбеди високо ниво на достапност на неговите канали за комуникација преку избегнување на поединечни точки на прекин и во секое време да обезбеди неколку начини/средства за негово контактирање и за контактирање на другите; јасно да ги наведеканалите за комуникација и за нив да ги запознае своите клиенти/конституенти и соработници;
- просториите и информациските системи на MKD-CSIRT треба да се наоѓаат на безбедни локации;
- да биде опремен со соодветен систем за управување и насочување на барањата, со цел обезбедување ефективна и ефикасна комуникација односно примопредавање;
- да обезбеди доверливост и веродостојност на неговите активности, односно на неговите операции.
- да располага со доволно вработени за да се обезбеди достапност на неговите услуги во секое време, а вработените во MKD-CSIRT треба да се соодветно обучени.

- да обезбеди редундантност на системите и резервен простор со цел да се осигура континуитет во неговата работа, односно услуги.

(2) За обезбедување доверливост и веродостојност на активностите и операциите, Агенцијата усвојува Кодекс на однесување на вработените во MKD-CSIRT.

Технички способности и капацитети на MKD-CSIRT

Член 38

За MKD- CSIRT ефективно да ги извршува своите задачи утврдени во членот 39 од овој закон, потребно е да располага со неопходни технички способности и капацитети.

Задачи на MKD-CSIRT

Член 39

(1) MKD-CSIRT ги врши следните задачи:

- следи и анализира сајбер закани, ранливости и инциденти на национално ниво, а по барање обезбедува помош на операторите на суштински услуги и на операторите на важни услуги во врска со следење на нивните мрежни и информациски системи во реално или речиси во реално време;
- доколку е можно речиси во реално време до операторите на суштински услуги и операторите на важни услуги, надлежни тела и други засегнати страни доставуварани предупредувања, најави, соопштенија и доставувањена информации за сајбер закани, ранливости и инциденти;
- обезбедува одговор на инциденти, и онаму каде што е применливо, обезбедува помош на операторите на суштински услуги и операторите на важни услуги;
- собира и анализира форензички податоци, обезбедува динамична анализа на ризици и инциденти, и информира за состојбите во сајбер безбедноста;
- на барање на оператори на суштински услуги и на оператори на важни услуги обезбедува проактивно скенирање на нивните мрежни и информациски системи со цел откривање на ранливости со потенцијал за значителновлијание;
- учествува во мрежи на CSIRT и обезбедува взаемна помош во согласност со своите капацитети и надлежности на други членови на мрежата по нивно барање;

- каде што е применливо, делува како координатор во постапка за координирано откривање на ранливост согласно член 40 став (1) од овој закон; и
- придонесува за користење на алатки за безбедносна размена на информации во согласност со член 47 став (3) од овој закон.

(2) MKD-CSIRT може да спроведува проактивно неинтрузивно скенирање на јавно достапни мрежни и информациски системи на операторите на суштински услуги и операторите на важни услуги. Скенирањето се врши со цел да се откријат ранливи или несигурно конфигурирани мрежни и информациски системи и како би се информирале засегнатите субјекти. Ваквото скенирање не треба да има негативно влијание врз функционирањето на услугите кои ги обезбедува операторот.

(3) При извршување на задачите наведени во ставот (1) на овој член, MKD- CSIRT може да приоретизира одредени задачи врз основа на пристап базиран на ризик.

(4) MKD-CSIRT воспоставува односи за соработка со релевантните чинители во приватниот сектор, со цел да се постигнат целите на овој закон. Со цел да се олесни соработката MKD-CSIRT треба да промовира усвојување и примена на заеднички или стандардизирани практики, шеми за класификација и таксономии во врска со:

- процедури за справување со инциденти;
- управување со кризи; и
- координирано откривање на ранливост согласно член 40 став (1) од овој закон

Координирано откривање на ранливости

Член 40

(1) MKD-CSIRT е координатор во процес на координирано откривање на ранливости.

(2) MKD-CSIRT треба да делува како доверлив посредник, олеснувајќи ја, онаму каде што е потребно, интеракцијата помеѓу физичко или правно лице кое пријавува ранливост и производител или обезбедувач на потенцијално ранливи ИКТ-производи или ИКТ-услуги, на барање на која било од страните.

(3) Задачите на MKD-CSIRT како координатор се:
- идентификување на засегнатите субјекти и контактирањесо нив;
- давање помош на физичките или правните лица кои пријавиле ранливост; и
- преговарање за временските рокови за обелоденување и управување со ранливостите кои влијаат на повеќе субјекти.

(4) Физички или правни лица можат анонимно да пријават ранливост до MKD-CSIRT. MKD-CSIRT во однос на пријавената ранливост треба да обезбеди внимателни последователни активности кои треба да се спроведат и да обезбеди анонимност на физичкото или правното лице кое ја пријавило ранливоста.

(5) Кога пријавената ранливост од ставот (4) на овој член би можела да има значително влијание врз субјекти во повеќе држави, MKD-CSIRT соработува со националните тимовите за одговор на компјутерски безбедносни инциденти на другите засегнати држави или еквивалентни такви тела, а доколку станува збор за земји-членки на ЕУ, ќе соработува со CSIRT назначени како координатори во мрежата на CSIRT на Европската Унија.

(6) MKD-CSIRT во својата работа ја има предвид европската база на информации за ранливости.

III.3 МЕРКИ ЗА УПРАВУВАЊЕ СО САЈБЕР БЕЗБЕДНОСНИ РИЗИЦИ И ОБВРСКИ ЗА ИЗВЕСТУВАЊЕ

Управување со сајбер безбедносни ризици

Член 41

.

Членовите на управувачките тела на операторите на суштински услуги и на операторите на важни услуги треба да посетуваат обуки, и на нивните вработени да им овозможат посетување обуки на редовна основа со цел да се стекнат со доволно знаење и вештини за да можат да идентификуваат ризици и да проценат дејствија за управување со сајбер безбедносни ризици и нивното влијание врз услугите што ги обезбедуваат.

Мерки за управување со сајбер безбедносни ризици

Член 42

(1) Операторите на суштински услуги и операторите на важни услуги се должни да преземат соодветни и сразмерни технички, оперативни и организациски мерки за управување со ризиците кои претставуваат закана за нивните мрежи и информациски системи преку кои тие ги обезбедуваат своите услуги, како и да се спречи или сведе, на најмала можна мера, влијанието на инцидентот врз корисниците на нивните услуги и на други услуги.

(2) Со мерките од ставот (1) на овој член треба да се обезбеди ниво на безбедност на мрежите и информациските системи, соодветно на ризиците. При оцената на пропорционалноста на мерките, треба да се има предвид степенот на изложеност на ризици, на операторот на суштински услуги или на операторот на важни услуги, неговата големина, веројатноста за појава на инциденти и нивната сериозност, вклучувајќи го и нивното социјално и економско влијание.

(3) Мерките од ставот (1) на овој член треба да се базираат на пристап со кој се земаат предвид сите опасности и чија цел е заштита на мрежните и информациските системи и физичкото опкружување на тие системи и го вклучуваат најмалку следново:

- политики на анализа на ризикот и безбедноста на информациските системи;
- справување во случај на инциденти;
- континуитет на работењето, како што е управување со резервните копии и закрепнување од катастрофи и управување со кризи;
- безбедност на ланецот на снабдување, вклучувајќи ги безбедносните аспекти на односот меѓу секој субјект и неговите директни добавувачи или обезбедувачи на услуги;
- безбедност при набавување, развој и одржување на мрежни и информациски системи, вклучувајќи решавање ранливости и нивно откривање;
- политики и постапки за процена на ефикасноста на мерките за управување со сајбер безбедносните ризици;
- основни практики на сајбер хигиена и обуки за сајбер безбедност;
- политики и постапки за криптографија и, по потреба, шифрирање;

- безбедност на човечките ресурси, политики за контрола на пристап и управување со имот;
- користење проверка на автентичноста со повеќе фактори или решенија за континуирана проверка на автентичноста, заштитени гласовни, видео и текстуални комуникации и безбедни системи за комуникација во итни случаи во рамките на операторот на суштински услуги или операторот на важни услуги, според потребите.

(4) Операторите на суштински услуги и операторите на важни услуги при определувањето на мерките од ставот (3) алинеја 4 на овој член треба да ја имаат предвид ранливоста што е специфична за секој непосреден добавувач и давател на услуги, квалитетот на производите и нивната сајбербезбедносна пракса, вклучувајќи ги и нивните безбедни развојни постапки, а исто така, треба да ги имаат предвид резултатите од координираните проценки на безбедносните ризици на синџиритена снабдување што се спроведени во согласност со членот 40 став (5) од овој закон.

(5) Агенцијата, со подзаконски акт ќе ги утврди техничките и методолошките барања за мерките од ставот (3) на овој член кои се однесуваат на давателите на услуги за DNS, регистри на имиња на врвни домени, даватели на услуги за компјутерска обработка во облак, даватели на услуги за податочен центар, даватели на услуги за мрежи за испорака на содржини, даватели на управувани услуги, даватели на управувани безбедносни услуги, даватели на услуги на интернет пазари, даватели на услуги на пребарувачи на интернет и даватели на платформи за услуги за социјални мрежи, како и даватели на доверливи услуги.

(6) Агенцијата во подзаконскиот акт од ставот (5) на овој член може да утврди и технички и методолошки барања за мерките од ставот (3) на овој член, а кои се однесуваат на оператори на суштински услуги и оператори на важни услуги кои не се наведени во ставот (5) на овој член. При изработката на подзаконскиот акт, Агенцијата ќе ги има предвид европските и меѓународните норми и релевантните технички спецификации.

Обврски за известување

Член 43

(1) Операторите на суштински услуги и операторите на важни услуги се должни без непотребно одложување да го известат MKD-CSIRT односно Агенцијата за секој значителен инцидент што има влијание врз обезбедувањето на нивните услуги, и да и ги достават на Агенцијата сите информации со кои ќе ѝовозможат да го утврди прекуграничното влијание на инцидентот.

(2) Каде што е применливо, операторите на суштински услуги и операторите на важни услуги се должни, без непотребно одлагање, да ги известат корисниците на нивните услуги на кои може да влијае сериозна сајбер закана, за сите мерки или правни средства кои тие можат да ги преземат како одговор на заканата, а доколку е потребно и за самата сериозна сајбер закана.

(3) За значителен инцидент од ставот (1) на овој член се смета инцидент кој:

- предизвикал или може да предизвика сериозни нарушувања во функционирањето на услугите или да предизвика финансиски загуби за соодветниот оператор на суштински услуги или оператор на важни услуги;
- влијаел или може да влијае врз други физички или правни лица со предизвикување значителна материјална или нематеријална штета.

(4) Со цел исполнување на обврските од ставовите (1) и (2) на овој член, операторите на суштински услуги и операторите на важни услуги се должни на MKD-CSIRT, да ѝдостават:

a. во рок од 24 часа од дознавањето за значителниот инцидент,рано предупредување во коешто доколку е соодветно, ќе се наведе дали постои сомневање дека значителниот инцидент е предизвикан од незаконско или злонамерно дејствување или може да има прекугранично влијание;

b. во рок од 72 часа од дознавањето за значителниот инцидент, известување за инцидентот во коешто, доколку е соодветно, ќе се ажурираат информациите од точката (a) на овој став и ќе ја наведе почетната процена на значителниот инцидент, вклучувајќи ја неговата сериозност и влијание како и показателите за загрозеност, доколку се достапни;

c. на барање од MKD-CSIRT, привремено известување за релевантните ажурирања на статусот;

d. во рок од еден месец по доставувањето на известувањето за инцидентот од точката (b) на овој став, завршно известување што го вклучува следново:
   (i) детален опис на инцидентот, вклучувајќи ја неговата сериозност и влијание;
   (ii) типот на закана или главната причина што најверојатно го предизвикала инцидентот;
   (iii) мерките на ублажување што се примениле и се применуваат;
   (iv) прекуграничното влијание на инцидентот, доколку е соодветно;

e. Операторите на суштински услуги и операторите на важни услуги се должни во случај на инцидент што е во тек во моментот на

поднесувањето на завршното известување од ставот (3) точка (d) на овој член, доMKD-CSIRT, да доставаат извештај за напредокот во тој момент, како и завршен извештај во рок од еден месец од решавањето на инцидентот.

(5) Давател на доверливи услуги, без непотребно одложување, но во секој случај во рок од 24 часа од дознавањето за значителниот инцидент, е должен да го извести MKD-CSIRT, за значителните инциденти кои имаат влијание врз давањето на неговите доверливи услуги.

(6) MKD-CSIRT, односно Агенцијата, треба во рок од 24 часа од приемот на раното предупредување од ставот (4) точка (а) на овој член на операторот на суштински услуги или на операторот на важни услуги да му достави одговор, вклучувајќи ги првичните повратни информации за значителниот инцидент, а на барање на операторот на суштински услуги или операторот на важни услуги, да му даде насоки или оперативни совети за спроведување на можни мерки за ублажување, како и дополнителна техничка подршка.Доколку постои сомневање дека значителниот инцидент е од криминална природа, Агенцијата ќе даде насока истиот да се пријави кај надлежните органите на прогон.

(7) Доколку значителниот инцидент се однесува на повеќе држави, единствената точка за контакт, односно Агенцијата, е должна без непотребно одложување да ги извести засегнатите држави и да им ги достави оние информации што се примени согласно ставот (4) на овој член, притоа, водејќи сметка за заштита на безбедноста и комерцијалните интереси на операторот на суштински услуги или на операторот на важни услуги, како и за доверливоста на доставените информации.

(8) Доколку за спречувањето на значителен инцидент или за решавање на значителен инцидент што е во тек е потребно да се извести јавноста, или доколку откривањето на значителниот инцидент е во интерес на јавноста од некоја друга причина, Агенцијата може, по извршена консултација со засегнатиот оператор на суштински услуги или оператор на важни услуги, да ја извести јавноста за значителниот инцидент или да побара од соодветниот оператор да го направи тоа.

(9) Агенцијата со подзаконски акт дополнително ќе го утврди видот на информациите, како и формата и постапката за доставување на известувања во согласност со ставовите (1) и (2) од овој член и членот 48 од овој закон.

(10) Агенцијата ќе донесе подзаконски акт со кој дополнително ќе се утврдат и случаите во кои инцидентот се смета за значителен, а се однесува на давателите на DNS-услуги,регистраторот на имиња на врвни домени, даватели на компјутерски услуги во облак, даватели на услуги за податочен центар, даватели на мрежи за испорака на содржини, даватели на управувани услуги, даватели на управувани безбедносни услуги, даватели на интернет-пазари,

даватели на интернет-пребарувачи и даватели на платформи за услуги за социјални мрежи и на други оператори на суштински или оператори на важни услуги.

Годишен извештај за состојбите во сајбербезбедноста
Член 44

(1) Агенцијата донесува Годишен извештај за состојбите во сајбер безбедноста.

(2) Годишен извештај од ставот (1) на овој член вклучува анонимизирани и збирниподатоци за значителни инциденти, инциденти, сериозни сајбер закани и избегнати инциденти за кои има добиено известувања во согласност со членот 43 став (1) и членот 48 од овој закон како и проценка за ризиците во областа на сајбер безбедноста имајќи ги предвид сајбер заканите, развојот на сајбербезбедносните капацитети во јавниот и приватниот сектор, проценка за свесноста на граѓаните и правните лица особено кај малите и средни претпријатија за сајбер безбедноста и сајбер хигиената.

(3) Годишниот извештај содржи информации за имплементација на Националната стратегија за сајбер безбедност согласно членот 33 од овој закон.

(4) Годишниот извештај содржи и препораки за политики во насока на решавање на недостатоците и подобрување на нивото на сајбер безбедноста во Република Северна Македонија.

(5) Годишниот извештајот од ставот (1) на овој член, Агенцијата го доставува до Владата на Република Северна Македонија до крајот на февруари тековната година. По барање на Владата на Република Северна Македонија, Агенцијата е должна да и достави и резимиран извештај согласно ставот (1) на овој член и за пократок временски период.

Примена на европски програми за сајбер безбедносна сертификација

Член 45

(1) Со цел да се докаже усогласеноста со одредени обврски од членот42 од овој закон, Агенцијата може да бара од операторите на суштински услуги или од операторите на важни услуги користење на одредени ИКТ-услуги, ИКТ-системи и ИКТ-производи кои ги развил самиот оператор или се набавени од трета страна кои се сертифицирани врз основа на европски програми за сајбер безбедноснасертификација.

(2) Агенцијата ги поттикнува операторите на суштински услуги и операторите на важни услуги да користат квалификувани доверливи услуги.

Стандардизација

Член 46

(1) Со цел промовирање на конвергентна имплементација на членот 42 ставови (1), (2) и (3) од овој закон, без наметнување или дискриминација во корист на употреба на одредена технологија, Агенцијата поттикнува користење европски и меѓународни стандарди и технички спецификации за безбедност на мрежни и информациски системи.

(2) Агенцијата по консултација со релевантните засегнати страни 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.

III. 4 РАЗМЕНА НА ИНФОРМАЦИИ

Механизми за размена на информации за сајбер безбедност

Член 47

(1) Субјектите кои припаѓаат во опфатот на примената на овој закон и по потреба другите субјекти кои не припаѓаат во опфатот на примената овој закон, можат меѓусебно доброволно да разменуваат релевантни информации за сајбер безбедноста, вклучително и информации во врска со сајбер закани,избегнати инциденти, ранливости, техники и процедури, индикатори за загрозеност, непријателски тактики, информации за субјектот на заканата, сајбер безбедносни предупредувања и препораки за конфигурацијата на сајбер безбедносните алатките за откривање сајбер напади, доколку таквото споделување на информации:

- има за цел да спречи или открие инцидент, одговори на инцидент, закрепне од инцидент или да го ублажи неговото влијание;
- го подобри нивото на сајбер безбедност, особено преку подигање на свеста за сајбер заканите, ја ограничува или ја попречува способноста на таквите закани да се шират, поддржува низа одбранбени способности, помогне за отстранување и откривање на ранливости;

- помогне за развивање натехники за откривање на закани, ограничување и превенција, стратегии за ублажување или фази на одговор и обновување или промовирање на заедничко истражување на сајбер закани.

(2) Размената на информации од ставот (1) на овој член треба да се одвива во рамките на заедниците на операторите на суштински и операторите на важни услуги, и каде што е релевантно, и нивните добавувачи или даватели на услуги. Размената на информации треба да се спроведува преку сајбер безбедносни механизми за размена на информации.

(3) За да се олесни воспоставувањето механизми за размена на информации за сајбер безбедност наведени во став (2) на овој член, потребно е да се дефинираат оперативните елементи како на пример користење на наменски ИКТ-платформи и алатки за автоматизација, содржината и условите на механизмите за размена на информации.

(4) Операторите на суштински и операторите на важни субјекти се должни да ја известат Агенцијата за нивното учество во механизмите за споделување информации за сајбер безбедноста наведени во став (2) од овој закон, или за нивното повлекување од учеството во таквите механизми.

(5) Агенцијата ќе обезбеди помош за воспоставување на механизми за споделување информации за сајбер безбедноста наведени во став (2) од овој закон преку примена на најдобрите практики од ЕУ.

Доброволно известување за релевантни информации

Член 48

(1) Покрај обврската за известување предвидена во членот 43 од овој закон, известувања на доброволна основа до MKD-CSIRT односно до Агенцијата, може да достават:

a. оператори на суштински и оператори на важни услуги во врска со инциденти, сајбер закани и избегнати инциденти кои не се значителни;
b. субјекти различни од субјектите наведени во точка (а) од овој став, без оглед на тоа дали припаѓаат во опфатот на примената овој закон, во однос на значителни инциденти, сајбер закани или избегнати инциденти.

(2) MKD-CSIRT ги обработува известувањата наведени во ставот (1) на овој член во согласност со постапката утврдена во членот 43 од овој закон.

(3) MKD-CSIRT е должен да им даде приоритет на обработка на задолжителните известувања , пред обработката на доброволните известувања.

(4) При доброволно известување Агенцијата нема да му наметне дополнителни обврски на субјектот кој известил, кои истите не би ги добил ако не доставил известување.

III.5 НАДЗОР

Надлежност за вршење на надзор

Член 49

(1) Агенцијата врши стручен надзор над операторите на суштински услуги и над операторите на важни услуги, согласно овој закон, во однос на исполнувањето на нивните обврски утврдени со овој закон.

(2) Агенцијата при спроведување на надзорот од ставот (1) на овој член, а доколку се работи за решавање на инциденти кои за последица имаа повреда на личните податоци, соработува со надлежното тело за заштита на личните податоци во Република Северна Македонија.

(3) Агенцијата врши редовен, вонреден и контролен стручен надзор.

(4) Редовниотстручен надзор се врши врз основа на годишната програма за вршење на надзор и опфаќа надзор над спроведувањето на овој закон, прописите донесени врз основа на него како и обврските, препораките и насоките дадени од страна на Агенцијата.

(5) Вонредниот струченнадзор се врши врз основа на писмена иницијатива поднесена од државни органи, оператори на суштински услуги или оператори на важни услуги,, физички или правни лица, како иво случај на сомневање по службена должност на Агенцијата.

(6) Контролниот струченнадзор се врши по истекот на рокот определен во поединечен акт донесен од страна на извршниот директор на Агенцијата со цел да се утврди дали субјектот на надзорот:

- постапил по актот во целост,

- делумно постапил по актот, или

- не постапил по актот.

Овластено лице

Член 50

(1) Надзорот од членот 49 од овој закон го вршат вработени во стручната служба на Агенцијата согласно со актот за систематизација на работите и задачите во стручната служба на Агенцијата и кои за таа цел се овластени од извршниот директор на Агенцијата (во натамошниот текст: овластено лице).

(2) Агенцијата на овластеното лице му издава службена легитимација која му служи за докажување на неговото службено својство и која е должен да ја покаже при вршењето на надзорот.

(3) Формата и содржината на службената легитимација од ставот (2) на овој член и начинот на издавање и одземање се утврдуваат со подзаконски акт.

(4) Овластеното лице треба да има високо образование од областа на информациско комуникациските технплпгии, со најмалку три години работно искуство во областа на сајбер безбедноста.

Вршење на надзор кај субјект на надзорот

Член 51

Во случаи кога се врши редовен или контролен стручен надзор кај субјект на надзорот, Агенцијата е должна писмено за тоа да го извести субјектот на надзорот најмалку три дена пред почетокот на надзорот. Во писменото известување Агенцијата е должна да даде образложение за причините за вршење на надзор.

Обврска на субјектот на надзорот во постапката настручен **надзор**

Член 52

(1) Субјектот на надзорот е должен на овластеното лице кое врши стручен надзор да му овозможи непречено вршење на надзорот и да му ги даде сите информации и податоци потребни за вршење на надзорот.

(2) Субјектот на надзорот е должен на овластеното лице кое врши надзор да му ги обезбеди условите неопходни за непречена работа и утврдување на фактичката состојба.

(3) Субјектот на надзорот е должен на овластеното лице кое врши надзорда му овозможи во определениот рок утврден од овластеното лице пристап до просториите и документите што се предмет на надзорот.

Права на субјектот на надзорот во постапката на надзор

Член 53

(1) Субјектот на надзорот има право да дава изјави на записник и забелешки во однос на постапката на надзорот, односот на овластеното лице кое го врши надзорот или точноста на утврдената фактичка состојба, со образложение за причините за тоа.

(2) Субјектот на надзорот има право да одбие да го потпише записникот, ако не се согласува со фактите кои се наведени во записникот или ако му е оневозможено правото од ставот (1) на овој член.

(3) Одбивањето да се потпише записникот не го спречува натамошното водење на постапката на надзор.

Записник

Член 54

(1) За извршениот надзор овластеното лице кое го врши надзорот составува записник на местото на вршење на надзорот.

(2) Овластеното лице кое го врши надзорот и субјектот на надзорот го потпишуваат записникот по завршувањето на надзорот. На субјектот на надзорот му се предава примерок од записникот.

(3) Ако субјектот на надзорот одбие да го потпише записникот, овластеното лице кое го врши надзорот ќе ги наведе причините за одбивањето.

(4) Записникот треба да содржи приказ на утврдената фактичка состојба при извршениот надзор, како и констатирани забелешки, изјави и други релевантни факти и околности.

(5) Образецот на формата и задолжителните елементи на записникот од извршениот надзор ги пропишува Агенцијата.

(6) Овластеното лице кое го врши надзорот е должно најдоцна во рок од три дена од денот на извршениот надзор, записникот од извршениот надзор да го достави до извршниот директорна Агенцијата.

Извештај за извршен струченнадзор

Член 55

(1) За секој извршенстручен надзор се составува писмен извештај кој се доставува до извршниот директорот на Агенцијата во рок од 15 дена од денот на извршениот надзор.

(2) Доколку со надзорот е констатирана повреда или прекршување, писмениот извештај содржи и предлог на мерка согласно со овој закон.

Решение

Член 56

(1) Во случај на повреда на одредбите на овој закон или друг пропис донесен врз основа на овој закон,, утврдена од страна на овластеното лице, констатирана со записник и по доставениот извештај за извршениот надзор, извршниот директор на Агенцијата е должен во рок од 15 дена од денот на приемот на извештајот да донесе решение.

(2) Со решението од ставот (1) на овој член се утврдуваат услови и се наложуваат обврски, мерки и активности кој субјектот врз кој е извршен надзорот е должен да ги исполни и изврши, заради отстранување на утврдените неправилности, во рокови определени соодветно на природата и тежината на условите и обврските.

Право на судска заштита

Член57

(1) Решението на Агенцијата донесено во управна постапка е конечно.

(2) Против решението од ставот (1) на овој член мпже да се поднесе тужба за поведување управен спор пред надлежен суд.

(3) Тужбата за поведување управен спор се поднесува во рок од 30 дена од денот на приемот на решението и истата не го одлага извршувањето на решението.

Стручен надзор кај операторите на суштински услуги

Член 58

(1) Надзорот или мерките наметнати на операторите на суштински услуги во однос на обврските утврдени со овој закон, треба да се ефективни и пропорционални, а при тоа, земајќи ги предвид околностите на секој поединечен случај.

(2) Агенцијата, односно овластеното лице при вршење на надзорот од членот 49 на овој закон има право од операторите на суштински услуги да бара:

a. надзор на лице место и надзор надвор од локацијата на операторот на суштински услуги, вклучувајќи случајни проверки ;

b. да спроведат редовни и безбедносни ревизии со конкретна цел извршени од квалификуван независен ревизор;

c. да спроведат адхок ревизии, во случај кога тоа е оправдано, а поради настанат значителен инцидент или прекршување на овој закон од страна на операторот на суштински услуги;

d. да спроведат анализи за безбедност врз основа на објективни, недискриминаторски, праведни и транспарентни критериуми за проценка на ризикот, доколку е тоа потребно, во соработка со операторот на суштински услуги;

e. информации неопходни за проценка на мерките за управување со сајбер безбедносни ризици што се донесени од операторот на суштински услуги, вклучително и донесени и усвоени политики за сајбер безбедност;

f. да овозможи пристап до податоци, документи и информации неопходни за извршување на надзорот;

g. да достават докази за спроведување на донесените и усвоени политики за сајбер безбедност, како што се резултатите од безбедносните ревизии извршени од квалификуван независен ревизор и други соодветни докази.

(3) Безбедносните ревизии со конкретна цел од став (2) точка b) од овој член треба да се извршат врз основа на проценки на ризик утврдени од Агенцијата од операторот на суштински услуги кој е предмет на ревизија, или на други достапни информации поврзани со ризикот.

(4) Резултатите од која било безбедносната ревизија со конкретна цел треба да и бидат достапни на Агенцијата. Трошоците за безбедносната ревизија со конкретна цел спроведена од квалификуван независен ревизор ги плаќа

операторот на суштински услуги кој е предмет на ревизија, освен во соодветно оправдани случаи кога Агенцијата ќе одлучи поинаку.

(5) Операторите на суштински услуги се должни на писменоа барање на Агенцијата да ѝги обезбедат информациите и податоците од ставот (2) точки е), f) или g) на овој член, на ниво на деталност и во рок којшто не може да биде пократок од 15 дена од денот на приемот на барањето. Агенцијата е должна во барањето да ги наведе причините и целта за користење на побараните информации.

Мерки кај операторите на суштински услуги

Член 59

(1) Агенцијата при вршење на надзор има право на операторот на суштински услуги да му ги наметне следните мерки:

a. писмено да го предупреди за прекршување на одредбите на овој Закон;

b. да донесе обврзувачки упатства, вклучително и во однос на мерките неопходни за спречување или отстранување на инцидент со временски рокови за спроведување на таквите мерки и за известување за нивното спроведување;

c. да донесе наредба со која се бара од операторите на суштински услуги да ги отстранат идентификуваните недостатоци или да престанат со однесувањето кое доведува до прекршување на овој Закон, како и да се откажат од повторување на тоа однесување;

d. да му нареди на операторот на суштински услуги да обезбеди дека неговите мерки за управување со сајбер безбедносен ризик се усогласени со член 42 од овој закон или да ги исполнат обврските за известување утврдени во член 43 од овој закон, на одреден начин и во одреден период;

e. да му наложи на операторот на суштински услуги да ги информира физичките или правните лица на кои им обезбедува услуга, а на кои би можела да влијае значителна сајбер закана,за природата на заканата, како и за сите можни заштитни или корективни мерки кои би можеле да бидат преземени од нивна страна како одговор на таа закана;

f. да му нареди на операторот на суштински услуги во разумен рок да ги спроведе препораките што се резултат на безбедносната ревизија;

g. да побара од операторот на суштински услуги да определи вработено лице со конкретно дефинирани задачи и за одреден временски период, кое ќе ја

следи и надгледува усогласеноста на операторот на суштински услуги со членовите 42 и 43 на овој Закон;

h. да му наложи на операторот на суштински услуги на одреден начин, да објави јавно достапни податоци за сторено прекршување на овој Закон;

i. да поднесе барање за поведување прекршочна постапка пред надлежен суд

(2) Кога мерките донесени во согласност со ставот (1) точки a), b), c), d) и f) нема да ги дадат очекуваните резултати, Агенцијата ќе определи рок во кој операторите на суштински услуги се должни да преземат мерки за отстранување на неправилноста или да ги исполнат барањата на Агенцијата.

(3) Доколку операторот на суштински услуги не постапи во согласност со ставот (2) на овој член, Агенцијата има право да:

a. побара од надлежниот суд на операторот на суштински услуги да му изрече мерка со која привремено ќе му забрани вршење на дел или на сите релевантни услуги или дејности што ги обезбедува;
b. побара од надлежниот суд на извршниот директор, односно на одговорното физичко лице или на правниот застапник на операторот на суштински услуги, да му изрече привремена мерка на безбедност забрана за вршење на професија, дејност или должност.

(4) Мерките определени во ставот (3) на овој член не се применуваат на органите на државната управа кои се опфатени со овој закон.

(5) Доколку органот на државната управа опфатен со овој закон не постапи во согласност со ставот (2) на овој член, Агенцијата за истото ќе ја извести Владата на Република Северна Македонија, во рок од 30 дена од денот кога органот на државната управа го примил решението од членот 56 на овој Закон.

(6) При изрекувањето на мерките од ставот (1) или ставот (3) на овој член, Агенцијата треба да има го предвид следново:

a. сериозноста на повредата и важноста на прекршените одредби, при што за сериозна повреда, меѓу останатото, се смета следното:

- повторување на повредата;
- непријавување или несправувањесозначителни инциденти;
- неотстранување на недостатокот во согласност со задолжителните упатства дадени од Агенцијата;
- попречување на ревизијата што ја побарала Агенцијата по утврдената повреда;

- давање лажни или особено неточни информации во врска со мерките за управување со безбедносните ризици или обврската за известување утврдена во членовите 42 и 43 од овој закон;

b. времетраење на повредата;

c. сите релевантни претходни повреди сторени од операторот на суштински услуги;

d. секоја материјална или нематеријална штета која е предизвикана, вклучувајќи ги сите финансиски или економски загуби, влијанието врз другите услуги, како и бројот на погодените корисници;

e. дали повредата е направена со намера или од небрежност;

f. сите мерки кои операторот на суштински услуги ги презел со цел да ја спречи или ублажи материјалната или нематеријалната штета;

g. секое почитување на одобрените кодекси на однесување или одобрените механизми на сертификација, и

h. нивото на соработка на одговорните физички или правни лица со Агенцијата.

(7) Агенцијата е должна детално да ги образложи донесените мерки. Агенцијата, пред донесувањето на мерките, треба да го извести операторот на суштински услуги за прелиминарните наоди и да му даде разумен рок во кој истиот може да даде забелешки, освен во случаи кога се работи за преземање на итни мерки за спречување на инцидентот.

(8) Агенцијата е должна да го извести органот на државна управа надлежен за управување со критична инфраструктура, доколку се работи за преземање на мерки кон оператор на критична инфраструктура, определен согласно закон.

Надзор кај операторите на важни услуги

Член 60

(1) Агенцијата, конооператор на важни услуги презема екс пост надзорни меркиврз основа на добиен доказ или информација дека операторот на важни услуги не работи во согласност со овој Закон, а особено согласно членовите 42 и 43на овој закон. Преземените мерки треба да се ефективни и пропорционални, а при тоа имајќи ги предвид околностите за секој поединечен случај.

(2) Агенцијата, односно овластеното лице при вршењето на надзорот согласно членот 49 на овој Закон, има право од операторот на важни услуги да бара:

a. надзор на лице место и екс пост надзор надвор од локацијата на операторот на важни услуги, :
b. безбедносни ревизии со конкретна цел кои ги спроведува квалификуван независен ревизор
c. безбедносни скенирања врз основа на објективни, недискриминаторски, праведни и транспарентни критериуми за проценка на ризик, а ако е потребно во соработка со операторот;
d. достава на информации потребни за екс пост оценување на мерките за управување со безбедносните ризици, донесени од страна на операторот на важни услуги, вклучувајќи и донесени и усвоени безбедносни политики;
e. обезбедување пристап до податоци, документи и информации потребни за извршување на надзорот;
f. доставување докази за спроведената донесена и усвоенабезбедноснаполитика, како што се резултатите од безбедносната ревизија што ја спровел квалификуван независен ревизор и други соодветни докази.

(3) Безбедносните ревизии со конкретна цел од ставот (2) точка b) на овој член се базираат на проценките за ризик кои ги утврдила Агенцијата или операторот на важни услуги или на други достапни информации поврзани со ризикот.

(4) Резултатите од секоја безбедносна ревизија со конкретна цел ѝ се ставаат на располагање на Агенцијата. Трошоците за безбедносната ревизија со конкретна цел која ја спроведува независен квалификуван ревизор ги сноси операторот на важни услуги над кого е спроведена ревизијата, освен во одредени оправдани случаи, кога Агенцијата ќе одлучи поинаку.

(5) Операторите на важни услуги се должни на писмено барање на Агенцијата да ѝги обезбедат информациите и податоците од ставот (2) точки d), e) или f) на овој член, на ниво на деталност и во рок којшто не може да биде пократок од 15 дена од денот на приемот на барањето. Агенцијата е должна во барањето да ги наведе причините и целта за користење на побараните информации.

Мерки кај операторите на важни услуги

Член 61

(1) Агенцијата, при вршење на надзор, има право на операторот на важни услуги да му ги наметне следните мерки:

a. писмено да го предупреди за прекршување на одредбите на овој Закон;

b. да донесе задолжителни упатства или наредби со кои од операторот на важни услуги ќе побара да ги отстрани утврдените недостатоци или прекршувања на овој закон;
c. да му нареди на операторот на важни услуги да престане со постапувања со кои се прекршува овој закон и да не го повторува таквото постапување;
d. да му нареди на операторот на важни услуги да обезбеди дека неговите мерки за управување со безбедносните ризици се во согласност со обврските утврдени во членот 42 на овој закон или да ја исполни обврската за известување утврдена во членот 43 на овој Закон, на определен начин и во определен рок;
e. да му нареди на операторот на важни услуги да ги извести физичките или правните лица на кои им обезбедува услуги, а на кои би можела да влијае сериозната безбедносна закана, за природата на таа закана, како и за сите заштитни или корективни мерки кои тие лица можат да ги преземат како одговор на таа закана;
f. да му нареди на операторот на важни услуги, во разумен рок да ги спроведе препораките дадени врз основа на извршената безбедносна ревизија;
g. да му нареди на операторот на важни услуги на определен начин да ги објави аспектите на прекршувањето на овој закон;
h. да поднесе барање за поведување на прекршочна постапка пред надлежен суд.

(2) Обврските од членот 59 ставови (6) и (7) од овој закон соодветно се применуваат (mutatis mutandis) за мерките кај операторите на важниуслуги предвидени со овој член.

IV. ДИГИТАЛНА ТРАНСФОРМАЦИЈА НА ЈАВНИОТ СЕКТОР

Јавни институции опфатени со дигиталната трансформација

Член 62

(1) Дигиталната трансформација на јавниот сектор, се однесува на органите на државната управа, освен на органите на државната управа од областа на безбедноста и одбраната на Република Северна Македонија.

(2) Дигиталната трансформација се однесува и на јавните институции кои не се наведени во ставот (1) на овој член, по нивно барање, а во согласност со овој закон и Планот за дигитална трансформација на јавниот сектор од членот 63 на овој закон.

План за дигитална трансформација на јавниот сектор

Член 63

(1) Владата на Република Северна Македонија,на секои три години, на предлог на Агенцијата донесува План за дигитална трансформација на јавниот сектор со кој ќе се обезбеди транзиција од дистрибуирана дигитална инфраструктура на јавниот сектор кон централизирана Владина дигитална инфраструктура, согласно член 58 од овој закон односно миграција на информациските системи на јавниот сектор во Владин облак.

(2) Агенцијата го подготвува предлогот на Планот од ставот (1) на овој член по претходно спроведена анализа за потребите на јавниот сектор, а во соработка со Министерството за информатичко општество и администрација.

(3) Со анализата од ставот (2) на овој член треба да се изврши евидентирање особено на:

- вкупната постојна дигитална инфраструктура кај органите на државната управа;
- дигиталните услуги што ги обезбедуваат органите на државната управа;
- употребената инфраструктура и технологии;
- постојни човечки и други ресурси и софтверски лиценци;
- функционалностите и можностите на информациските системи;
- протоколите/комуникација/интеграцијата со други системи; и
- подготвеноста на постојните системи за работа во облак, со посебен осврт на софтверските лиценци;

(4) Планот од ставот (1) на овој член особено содржи:

- начин и рокови за изградба на централизирана Владина дигитална инфраструктура;
- потребните инвестиции во централизирана Владина дигитална инфраструктура(хардвер, виртуелизација, системски софтвер и сл.);
- начин и рокови и потребни средства со кои ќе се обезбеди миграција на информациските системи на јавниот сектор во Владиниот облак;
- Воведување на нови и надградба на постојни на дигитални услуги на јавниот сектор;
- начин и рокови во кои ќе се обезбеди поврзување на постојните децентрализирани информациски системина националната платформа за

интероперабилност и потребата за воспоставување на нови информациски системи од страна на органите на државната управа;

- начин и рокови ви кои ќе се обезбеди електронско комуникациско поврзување на органите на државната управа на владината мрежа и пристап до интернет на органите на државната управа.

(5) Агенцијата врши надзор на спроведувањето на Планот од ставот (1) на овој член од страна на органите на државната управа.

Обезбедување на електронско комуникациско поврзување на органите на државната управа

Член 64

(1) Агенцијата обезбедува затворена оптичка електронска комуникациска мрежа, за сопствени потреби, за поврзување на органите на државната управа (во понатамошниот текст: владина мрежа), согласно усвоените стратегии и планови на Владата на Република Северна Македонија.

(2) Владината мрежа од ставот (1) на овој член опфаќа повеќе затворени подмрежи и тоа:

- затворена подмрежа со која се обезбедува поврзување на органите на државната управа, и
- затворени подмрежи за сопствени потреби на органите на државна управа, со исклучок на мрежите на образовните и безбедносните институции.

(3) Обезбедувањето на владината мрежа од ставот (1) од овој член се врши на начин со кој максимално ќе се искористат постојните слободни капацитети на физичка оптичка инфраструктура (слободни оптички кабли/влакна, кабелска канализација итн.) изградена од приватни лица или јавни институции.

(4) Физичката инфраструктура на владината мрежа треба да се базира и на националната транспортна оптичка мрежа што е во надлежност на ЈП МРД согласно закон.

(5) ЈП МРД по барање на Агенцијата обезбедува оптичко физичко поврзување.

(6) Агенцијата врши набавка, одржување, поставување, управување и надзор на активната комуникациска опрема на Владината мрежа во органите на државната управа и мрежните јазли на истата.

(7) Агенцијата воспоставува мрежен оперативен центар (NOC) и безбедносен оперативен центар (SOC) на владината мрежа.

Обезбедување пристап до интернет на органите на државната управа

Член 65

Агенцијата го координира, планира и обезбедува пристапот до интернет за органите на државна управа.

Централизирана Владина дигитална инфраструктура

(Владин податочен центар, Владин облак и Центар за обновување на податоци во случај на катастрофа)

Член66

(1) Агенцијата вршиизградба, управување, развивање и одржување на следната централизирана Владина дигитална инфраструктура:

- податочен центар за органите на државната управа (владин податочен центар)
- обезбедување услуга за компјутерска обработка во облак за органите на државна управа, (владин облак)
- центар за обновување на податоци во случај на катастрофа.

(2) Централизираната владина дигитална инфраструктура од ставот (1) на овој член се реализира врз основа на Студија за изводливост која ја усвојува Владата на Република Северна Македонија по предлог на Агенцијата, Агенцијата предлогот го подготвува во соработка со Министерството за информатичко општество и администрација. Владата ја усвојува Студијата во рок од 30 дена од денот на приемот на предлогот.

(3) Владиниот облак од ставот (1) алинеја 2 на овој член, нуди услуги за пресметување во облак на ниво на инфраструктура и платформи (IaaS, PaaS и

SaaS) , а согласно со Планот за дигитална трансформација на јавниот сектор од членот 63 на овој Закон, .

(4)Агенцијата за потребите на централизираната Владина дигитална инфраструктура одставот (1) на овој член обезбедува хардвер и софтвер..

Поделба на надлежностите на Агенција и јавните институции

Член 67

(1) Агенцијата во согласност со Планот за дигитална трансформација на јавниот сектор од членот 63 на овој закон, врши миграцијанаинформациските системи на јавниот секторво централизираната Владина дигитална инфраструктура од членот 66 на овој закон

(2) Агенцијата врши развивање, надградба, одржување и управувањена нови информацискисистеми, односно дигитални услуги на Владиниот облак,согласно Планот за дигитална трансформација на јавниот сектор од членот 63 на овој закон.

(3) Агенцијата врши развивање, надградба, одржување и управување на мигрираните информациските системи од ставот (1) на овој член.

(4) Агенцијата обезбедува служба за подршка и информации на јавните институции во однос на развојот и обезбедувањето на дигиталните услуги, согласно овој закон

(5) Јавната институција чиј информациски систем е мигриран согласно ставот (1) на овој член и/или е воспоставен нов информациски систем согласно став (2) е надлежна за:

- дефинирање на функционалностите на информацискиот систем, во соработка со Агенцијата.
- податоците кои се во негова надлежност а кои се обработуваат во информацискиот систем во централизираната Владина дигитална инфраструктура од членот 66 на овој закон
- подршка за користењето на информацискиот систем од негова надлежност на крајните корисници,

V. ПРЕКРШОЧНИ ОДРЕДБИ

Прекршоци

Член68

(1) Глоба во износ од 2% од вкупниот годишен приход на операторот на суштински услуги, односно глоба во износ од 1,4% од вкупниот годишен приход на операторот на важни услуги (изразена во апсолутен износ) остварен во деловната година што и претходи на годината кога е сторен прекршокот или од вкупниот приход остварен за пократок период од годината што му претходи на прекршокот, доколку во таа година операторот на суштински услуги, односно операторот на важни услуги започнал да работи, ќе му се изрече за прекршок на операторот на суштински услуги со исклучок на органите на државната управа и правнитене лица на кои со закон им е доверено да вршат јавни овластувања на државно ниво, како и на операторот на важни услуги ако:

1) Не преземе соодветни и сразмерни технички, оперативни и организациски мерки за управување со ризиците, член 42 став (1);
2) Не го извести MKD CSIRT, односно Агенцијата за секој значителен инцидент што има влијание врз обезбедувањето на неговите услуги и не и ги достави на Агенцијата сите информации што ќе и овозможат да го утврди прекуграничното влијание на инцидентот, член 43 став (1);
3) Не ги извести корисниците на неговите услуги на кои може да влијае сајбер закана за сите мерки или правни средства кои тие можат да ги преземат како одговор на заканата , член 43 став (2);
4) Не постапи во согласност со членот 43 став (4);
5) Не го извести MKD CSIRT за значителните инциденти, член 43 став (5);
6) Операторот на суштински услуги во рокот определен од страна на Агенцијата не преземе мерки за отстранување на неправилноста или не ги исполни барањата на Агенцијата. член 59 став (2).

(2) Глоба во износ од 30% од одмерената глоба за операторот на суштински услуги, односно за операторот на важни услуги ќе му се изрече и на одговорното лице во операторот на суштински услуги, односно во операторот на важни услуги за прекршоците од ставот 1 на овој член.

(3) Глоба во износ од 1000 евра во денарска противвредност ќе му се изрече за прекршоците од ставот (1) на овој член на функционерот кој раководи со органот на државната управа или со правното лице на кое со закон му е доверено да врши јавни овластувања на државно ниво.

Член 69

(1) Глоба во износ од 5.000 евра во денарска противвредност ќе му се изрече за прекршок на операторот на суштински услуги, со исклучок на органите на

државната управа и правните лица на кои со закон им е доверено да вршат јавни овластувања на државно ниво, како и на операторот на важни услуги ако:

1) Не ги достави податоците од членот 28 став (6);
2) Не достави измена на податоците согласно членот 28 став (7);
3) Не ја воспостави базата на податоци за регистрација на имиња на домени согласно членот 30;
4) Не ја извести Агенцијата за неговото учество во механизмите за споделување на информации за сајбер безбедноста , член 47 став (4);
5) Не ги исполни обврските од членот 52;
6) Не и ги достави на Агенцијата резултатите од било која безбедносна ревизија со конкретна цел , член 58 став (4), односно член 60 став (4);
7) На писмено барање на Агенцијата не ги обезбеди информациите и податоците согласно член 58 став (5), односно член 60 став (5).

(2) Глоба во износ од 30% од одмерената глоба за операторот на суштински услуги, односно за операторот на важни услуги ќе му се изрече и на одговорното лице во операторот на суштински услуги, односно во операторот на важни услуги за прекршоците од ставот 1 на овој член.

(3) Глоба во износ од 500 евра во денарска противвредност ќе му се изрече за прекршоците од ставот (1) на овој член на функционерот кој раководи со органот на државната управа или правното лице на кое со закон му е доверено да врши јавни овластувања на државно ниво

Прекршочни санкции

Член70

(1) На операторот на суштински услуги за сторен прекршок од членот 68 став (1) точка 6), покрај глобата ќе му се изрече и прекршочна санкција забрана на вршење на определена дејност во траење од шест месеци до три години..

(2) На одговорното лице на операторот на суштински услуги за сторен прекршок од членот 68 став (1) точка 6) покрај глобата, ќе му се изрече и прекршочна санкција забрана за вршење на професија, дејност или должност во траење од три месеци до една година.

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 71

(1) Агенцијата ќе започне со работа со именување на членовите на Комисијата и на Извршниот директор на Агенцијата.

(2) Владата на Република Северна Македонија ќе ги именува членовите на Комисијата во рок од 30 дена од денот на влегување во сила на овој закон.

(3) Комисијата од редот на своите членови, на првата конститутивна седница, избира претседател и заменик на претседателот на Комисијата.

(4) Комисијата ќе донесе Деловник за работа на Комисијата во рок од 15 дена од денотна нејзиното конституирање.

(5) Комисијата ќе го именува Извршниот директор на Агенцијата во рок од 60 дена од денот на нејзиното конституирање.

(6) Извршниот директор ќе ги предложи членовите на Стручниот совет на Агенцијата во рок од три месеци од денот на именувањето

(7) Комисијата ќе ги именува членовите на Стручниот совет на Агенцијата во рок од 30 дена од денот на приемот на предлогот.

Член 72

Планот за дигитална трансформација на јавниот сектор од членот 63 на овој закон, ќе го донесе Владата на Република Северна Македонија, по предлог на Комисијата на Агенцијата во рок од девет месеци од денот на влегувањето во сила на овој Закон

Член 73

(1) Статут на Агенцијата, Правилникот за внатрешна организација, Правилникот за систематизација и Правилникот за плати и надоместоци на плати на Комисијата на Агенцијата ќе и ги предложи Извршниот директор на Агенцијата во рок од 60 дена од денот на неговото именување.

(2) Комисијата на Агенцијата ќе ги донесе актите од ставот (1) на овој член во рок од 30 дена од денот на приемот на предлогот.

Член 74

(1) Владата на Република Северна Македонија , по предлог на Министерот за информатичко општество и администрација, на Агенцијата ќе и обезбеди простории за работа и соодветна опрема и средства за работа.

(2) На Извршниот директор на Агенцијата, до денот на донесувањето на Правилникот за плати и надоместоци на плати, ќе му се исплатува плата во висина од две просечни плати исплатени во секторот Информатика и комуникации, согласно последниот извештај на Државниот завод на статистика од минатата година.

Член 75

(1)Вработените во органите на државната управа кои имаат завршен VII/1 степен од областа на информатичките и комуникациските технологии ќе ги презема Агенцијата, согласно со своите акти за организација и за систематизација.

(2)Со актите за организација и систематизациј треба да се обезбеди сите вработени од ставот (1) на овој член кои имаат засновано работен однос на неопределено време до денот на влегувањето во сила на овој закон да бидат преземени во Агенцијата.

Член 76

Комисијата на Агенцијата ќе ги усвои подзаконските акти кои произлегуваат од овој Закон, во рок од девет месеци од денот на влегување во сила на овој закон.

Член 77

Законот за електронски документи, електронска идентификација и доверливи услуги, Законот за електронски услуги и електронско управување и Законот за централен регистар на население ќе се усогласат со одредбите од овој закон во рок од две години од денот на влегување во сила на овој закон.

Член 78

(1)Националниот центар за одговор на компјутерски инциденти MKD-CIRT кој согласно Законот за електронски комуникации (“Службен весник на Република Северна Македонија“ број 39/14, 188/14, 44/15, 193/15, 11/18, 21/18 и „Службен весник на Република Северна Македонија“ бр. 98/19, 153/19 и 92/21) функционира како посебна организациона единица во рамките на Агенцијата за електронски комуникации, продолжува со својата работа до 01.01.2026 година,

(2)Националниот центар за одговор на компјутерски инциденти MKD-CIRT согласно ставот (1) од овој член е должен да соработува и разменува податоци со Агенцијата

Член 79

(1)Владиниот облак од членот 66 на овој закон, Агенцијата ќе го воспостави во рок од 24 месеци од денот на влегување во сила на овој закон.

(2)Операторите на суштински услуги и операторите на важни услуги се должни да го усогласат своето работење согласно одредбите на овој закон во рок од 24 месеци од денот на влегување на сила на овој закон.

Член 80

Транзицијата од дистрибуирана дигитална инфраструктура на јавниот сектор кон централизирана Владина дигитална инфраструктура од членот 66 од овој закон односно миграцијата на информациските системи на јавниот сектор во Владин облак ќе се изврши во рок од десет години од денот на влегување во сила на овој закон, а согласно Планот за дигитална трансформација на јавниот сектор од членот 63 на овој закон.

Член 81

(1)До завршувањето на процесот на транзиција од дистрибуирана дигитална инфраструктура на јавниот сектор кон централизирана Владина дигитална инфраструктура од членот 66 на овој закон односно до завршување намиграцијата на информациските системи на јавниот сектор во Владин облак, јавните институции се должни од Агенцијата да побараат согласност за техничките спецификациии наменети за набавка на услуга за развој, надградба и одржување на софтверот и хардверот за потребите на нивните информациски системи, сметано од 01.01.2026 година.

(2) Агенцијата е должна да ја даде согласност од ставот (1) на овој член, во рок од 15 дена од денот на приемот на барањето за согласност. Доколку Агенцијата не даде согласност, треба да даде образложение за истото и во рок од 45 дена од денот на приемот на барањето за согласност, да даде обврзувачки насоки за техничките спецификации од ставот (1) на овој член. Доколку обврзувачките насоки се исполнети, Агенцијата е должна да ја даде побараната согласност во рок од 15 дена од денот на приемот на новото барање за согласност.

Член 82

Дигиталната инфраструктура, односно информацискиот систем на јавната институција по извршената миграција согласно членот 66 од овој закон преминува

во Агенцијата соглано Закон за користење и располагање со стварите во државна сопственост и со стварите во општинска сопственост.

Член 83

За операторите, односно давателите на јавни електронски комуникациски мрежи и/или јавно достапни електронски комуникациски услуги, овој закон ќе започне да се применува од 01.01.2026 година.

Член 84

Овој закон влегува во сила осмиот ден од денот на објавувањето во Службен весник на Република Северна Македонија.