20251352969

СОБРАНИЕ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Врз основа на членот 75, ставови 1 и 2 од Уставот на Република Северна Македонија, претседателот на Република Северна Македонија и претседателот на Собранието на Република Северна Македонија издаваат

УКАЗ ЗА ПРОГЛАСУВАЊЕ НА ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАЦИСКИ СИСТЕМИ(*)

Се прогласува Законот за безбедност на мрежни и информациски системи(*),
што Собранието на Република Северна Македонија го донесе на седницата одржана на 27 јуни 2025 година.

Бр. 08-3690/1
27 јуни 2025 година
Скопје

Претседател на Република
Северна Македонија,
Гордана Силјановска Давкова, с.р.

Претседател
на Собранието на Република
Северна Македонија,
Африм Гаши, с.р.

ЗАКОН ЗА БЕЗБЕДНОСТ НА МРЕЖНИ И ИНФОРМАЦИСКИ СИСТЕМИ (*)

I. ОПШТИ ОДРЕДБИ

Предмет

Член 1

Со овој закон се уредува безбедноста на мрежните и информациските системи, надлежните органи за безбедност на мрежните и информациските системи и управување со значајни сајбер безбедносни инциденти и сајбер безбедносни инциденти со голем опфат, единствената точка за контакт за сајбер безбедност, тимовите за одговор на компјутерски инциденти , мерките за безбедност на мрежни и информациски системи и за управување со ризикот за сајбер безбедност, обврските за известување за сите аспекти на безбедност на мрежни и информациски системи за правните лица кои обезбедуваат услуги во областите со висока критичност и другите критични области, правилата и обврските за известување и размена на информации за инциденти, обврската за усвојување на стратегија која ја опфаќа безбедноста на мрежните и информациските системи, надзорот над спроведувањето на одредбите од овој закон, како и други прашања поврзани со безбедност на мрежни и информациски системи.

(*) Со овој закон се врши усогласување со ДИРЕКТИВА (ЕУ) 2022/2555 НА ЕВРОПСКИОТ ПАРЛАМЕНТ И НА СОВЕТОТ од 14 декември 2022 година за мерките за високо заедничко ниво на кибербезбедност низ Унијата, за изменување на Регулативата (ЕУ) бр. 910/2014 и Директивата (ЕУ) 2018/1972 и за укинување на Директивата (ЕУ) 2016/1148 (Директива NIS) со CELEX број 32022L2555

Цели

Член 2

Цели на овој закон се изградба на капацитети за безбедност на мрежни и информациски системи во државата, намалување на заканите за мрежните и информациските системи што се користат за обезбедување основни услуги во областите со висока критичност и другите критични области и обезбедување на континуитет на таквите услуги во случај на инциденти, со што се придонесува кон безбедноста на Република Северна Македонија и ефективно функционирање на нејзината економија и општество.

Дефиниции

Член 3

Одделни изрази употребени во овој закон го имаат следното значење:

1) „активната сајбер заштита“ е спречување, откривање, следење, анализа и ублажување на прекршувањата на безбедноста на мрежните и информациските системи на активен начин, во комбинација со користење на капацитети распоредени во и надвор од мрежата на жртвите на сајбер напади, вклучително и услуги или алатки за самопроверки, откривање и услуги за отстранување.

2) „безбедност на мрежни и информациски системи“ е способност на мрежните и информациските системи, да се спротивстават, со одредено ниво на доверба, на секое дејство кое ја загрозува достапноста, 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) „Врвни национални интернет домени“ се врвните македонски домени .mk (во натамошниот текст: доменот .mk) и .мкд (во натамошниот текст: доменот .мкд);

4) „големи субјекти“ се големите трговци класифицирани во зависност од бројот на вработените, годишниот приход и просечната вредност на вкупните средства по годишните сметки во последните две години согласно законот со кој се уредуваат трговските друштва;

5) „давател на доверлива услуга“ е правно лице кое дефинирано како давател на доверлива услуга согласно со прописите од областа на електронските документи, електронска идентификација и доверливи услуги;

6) „давател на квалификувана доверлива услуга“ е правно лице кое е дефинирано како давател на квалификувана доверлива услуга согласно со прописите од областа на електронските документи, електронска идентификација и доверливи услуги;

7) „давател на ДНС услуга“ е правно лице што обезбедува:

1) јавно достапни повторливи услуги за распределување на имиња на домени на крајните корисници на интернет или

2) меродавни услуги за распределување на имиња на домени за користење од други лица, со исклучок на коренски сервери за имиња;

8) „давател на управувани услуги“ е правно лице кое 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;

9) „давател на управувани безбедносни услуги“ е давател на управувани услуги што врши или обезбедува помош за активности кои се однесуваат на управување со сајбер безбедносни ризици;

10) „дигитална средина“ е виртуелниот простор создаден од компјутерски системи, интернет и дигитални технологии, каде што се комуницира, се разменува информации и се извршуваат различни активности. Оваа средина вклучува веб-страници, социјални мрежи, онлајн платформи, апликации и дигитални уреди;

11) „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. Дигиталната услуга ги опфаќа и електронските услуги како административни услуги за чиешто обезбедување се одговорни органите согласно законот кој ги уредува електронското управување и електронските услуги;

12) „доверлива услуга“ е електронска услуга која е дефинирана како доверлива услуга согласно со прописите од областа на електронските документи, електронска идентификација и доверливи услуги;

13) „други органи на централната државна власт“ се органите на законодавната и судската власт, како и институциите од јавниот сектор кои одговараат пред Собранието на Република Северна Македонија (во натамошниот текст: Собранието);

14) „Единствен регистар на врвни домени“ е база на податоци на имиња на домени, нивните регистранти и овластени лица за нивна администрација согласно со кој се уредува работата на Македонската академска истражувачка мрежа.

15) „значајна сајбер закана“ е сајбер закана за која 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 на тој субјект преку предизвикување значителна материјална или нематеријална штета;

16) „значаен сајбер безбедносен инцидент“ е сајбер безбедносен инцидент кој:

1) предизвикал или може да предизвика сериозни нарушувања во функционирањето на услугите или да предизвика финансиски загуби за соодветниот клучен, односно важен субјект;

2) влијаел или може да влијае врз други физички или правни лица со предизвикување значителна материјална или нематеријална штета.

17) „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 установи;

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

19) „инцидент“ е настан кој ги загрозува достапноста, автентичноста, интегритетот или доверливоста на зачуваните, пренесените или обработените податоци или на услугите понудени од или достапни преку мрежните и информациските системи;

20) „ИКТ производ“ е елемент или група елементи на мрежен или информациски систем;

21) „ИКТ услуга“ е вид на дигитална услуга што целосно или претежно се состои од пренесување, чување, добивање или обработување на информации преку мрежни и информациски системи;

22) „ИКТ процес“ е група активности што се вршат за дизајнирање, развивање, испорака или одржување на ИКТ-производ или ИКТ-услуга;

23) „имиња на домени“ се 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;

24) „интернет продажба“ е 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 потрошувачите да склучуваат договори на далечина со други трговци или потрошувачи;

25) „интернет-пребарувач“ 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 дава резултати во кој било формат во кои може да се најдат информации поврзани со бараната содржина;

26) „јавна електронска комуникациска мрежа“ е јавна комуникациска мрежа дефинирана како таква согласно со законот со кој се уредуваат електронските комуникации;

27) „електронска комуникациска услуга“ е јавна електронска комуникациска услуга дефинирана како таква согласно со законот со кој се уредуваат електронските комуникации;

28) „квалификувана доверлива услуга“ е електронска услуга која е дефинирана како квалификувана доверлива услуга согласно со прописите од областа на електронските документи, електронска идентификација и доверливи услуги;

29) „критична инфраструктура“ се информатичко комуникациски (ИКТ) средства, системи, објекти, мрежи или нивни делови со кои се остваруваат витални функции на општеството, а кои се од суштинско значење и прекинот на нивната работа или нивното уништување може да има сериозни последици за безбедноста на граѓаните, демократскиот систем, економијата, животната средина и другите национални вредности, односно националната безбедност и одбраната во Републиката.

30) „мерки за безбедност на мрежни и информациски системи“ се мерки и активности кои се пропишани со општите правила за заштита на мрежните и информациските системи кои се спроведуваат на физичко, техничко или организациско ниво, а имаат за цел да ја зајакнат безбедноста на мрежите и информациските системи.

31) „мрежа за испорака на содржини“ 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;

32) „мрежен и информациски систем“ е:

1) електронска комуникациска мрежа согласно Законот за електронските комуникации;

2) 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

3) дигитални податоци кои се складираат, обработуваат, преземаат или пренесуваат со средствата од точките 1) и 2) на оваа точка, со цел нивно работење, употреба, заштита и одржување;

33) „надлежен орган“ е субјект кој согласно со одредбите од овој закон има надлежност да пропишува мерки и стандарди за безбедност на мрежи и информациски системи, како и да врши надзор над нивното работење;

34) „стратегија која ја опфаќа безбедноста на мрежните и информациските системи“ е стратешки документ усвоен од Владата на Република Северна Македонија (во натамошниот текст: Владата), со кој се предвидуваат стратешки цели и приоритети и нивна реализација во областа на сајбер безбедноста и управувањето;

35) „офицер за сајбер безбедност“ е лице кое задолжително се ангажира кај суштинските субјекти, кое има соодветни посебни работни компетенции, е одговорно за спроведување на мерките за сајбер безбедност утврдени со овој закон, е во директна комуникација и соработува со надлежниот орган и надлежниот тим за одговор на компјутерски инциденти за доследна имплементација на одредбите на овој закон;

36) „платформа за услуги за социјални мрежи“ 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;

37) „субјекти од областа на дигиталната инфраструктура“ се:

1) давателите на услуги на точки за размена на интернет-сообраќај,

2) давателите на ДНС услуги, со исклучок на оператори на коренски сервери за имиња,

3) субјектот кој го води Единствениот регистар на врвни домени (доменот мк и доменот mkd),

4) давателите на услуги за компјутерска обработка во облак,

5) давателите на услуги за податочен центар,

6) давателите на услуги за мрежи за испорака на содржини,

7) давателите на доверливи услуги,

8) давателите/операторите на јавни електронски комуникациски мрежи и

9) давателите/операторите на јавно достапни електронски комуникациски услуги.

38) „субјекти кои даваат дигитални услуги“ се:

1) давателите на услуги на интернет продажба,

2) давателите на услуги на интернет-пребарувач и

3) давателите на услуги на платформи за услуги за социјални мрежи.

39) „истражувачка организација“ е субјект кој има примарна дејност за спроведување на применети истражувања или експериментален развој со цел да ги искористи резултатите од тоа истражување за комерцијални цели, но кој не вклучува образовни институции

40) „правно лице со регистрирано седиште во Републиката за давање на управувани ИКТ-услуги“ е:

1) давател на управувани услуги и/или

2) давател на управувани безбедносни услуги.

41) „претставник“ е физичко или правно лице кое е изречно назначено да делува во име на давател на ДНС услуги, 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 продажба, давател на услуги на интернет -пребарувач или давател на платформи за услуги за социјални мрежи што нема регистрирано седиште во Република до кое може да се обрати Министерството за дигитална трансформација (во натамошниот текст: Министерството) во однос на обврските на тој субјект што произлегуваат од овој закон;

42) „ризик“ е можност за загуба или за нарушување предизвикано од инцидент и треба да се изрази како комбинација на опфатот на таквата загуба или нарушување и веројатноста за појава на таков инцидент;

43) „ранливост“ е слабост, чувствителност или недостаток на ИКТ-производи или ИКТ-услуги што може да бидат искористени од страна на сајбер заканата;

44) „субјект за регистрирање на имиња на врвни домени“ е субјект на кој 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;

45) „сајбер безбедност“ е систем на активности и мерки потребни за заштита на мрежните и информациските системи, корисниците на таквите системи и другите лица погодени од закани преку компјутерски мрежи;

46) „сајбер безбедносен инцидент со голем опфат“ 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;

47) „сајбер екосистем“ е комплексен систем што вклучува различни елементи, какви што се технологија, инфраструктура, корисници, органи за регулирање и услуги, кои сите заедно функционираат во дигиталната средина. Целта на сајбер екосистемот е да обезбеди безбедна, ефикасна и инклузивна дигитална средина, каде што поединци и организации можат да комуницираат и да разменуваат информации безбедно и доверливо.

48) „сајбер закана“ е секоја потенцијална околност, настан или активност што може да оштети, наруши или на друг начин негативно да влијае врз мрежните и информациските системи, корисниците на таквите системи и други лица;

49) „сајбер криза“ е настан или настани во сајбер просторот што би можеле да предизвикаат или веќе предизвикале значително нарушување на безбедноста на граѓаните, демократскиот систем, економијата, животната средина и другите национални вредности, односно националната безбедност и одбраната во Републиката.

50) „ надлежен орган“ е орган основан согласно со Устав и со закон во кои се утврдени најмалку истите или повисоки стандарди од оние утврдени со овој закон, а кој е надлежен орган за субјектите од областа за која е основан.

51) „справување со инцидент“ се сите преземени дејства и процедури заради спречување, откривање, анализа, запирање на инцидент или одговор на инцидентот, како и закрепнување од инцидентот;

52) „средни субјекти“ се средните трговци класифицирани во зависност од бројот на вработените, годишниот приход и просечната вредност на вкупните средства по годишните сметки во последните две години согласно законот со кој се уредуваат трговските друштва;

53) „субјект“ е физичко или правно лице регистрирано согласно закон на државата каде е основано и кое функционира под свое име и остварува права и обврски;

54) „субјект што обезбедува услуги за регистрација на имиња на домени“ е регистратор или застапник што делува во име на регистрите, како што е давател или препродавач на услуги за заштита на приватност или регистрација преку посредник;

55) „област производство“ опфаќа производство на:

1) медицински помагала и ин-витро дијагностички медицински помагала,

2) компјутерски, електронски и оптички производи,

3) електрична опрема,

4) машини и опрема кои не се класифицирани на друго место,

5) моторни возила, приколки и полуприколки и/или

6) друга транспортна опрема.

56) „тим за одговор на компјутерски инциденти (CSIRT)“ е тело надлежно за справување со инциденти, согласно пропишана процедура;

57) „точка за размена на интернет-сообраќај“ е 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 кои 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;

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

59) „услуга за податочен центар“ е услуга што опфаќа структури или групи на структури 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.

Опфат на законот

Член 4

(1) Овој закон се применува на следните институции од јавниот сектор:

1) Собранието;

2) Самостојните државни органи и регулаторни тела основани од и одговорни пред Собранието;

3) Владата;

4) Министерствата;

5) Самостојните органи на државната управа;

6) Органите на државната управа во состав на министерствата;

7) Управните организации;

8) Судовите и

9) општините, општините во градот Скопје и градот Скопје.

(2) Одредбите на овој закон се применуваат на работата на средни и големи субјекти кои обезбедуваат услуги во:

1) Енергетиката,

2) Транспортот;

3) Банкарството;

4) Финансискиот пазар;

5) Здравството;

6) Дигиталната инфраструктура;

7) Управувањето со ИКТ-услуги (B2B);

8) Снабдувањето на вода за пиење и дистрибуција;

9) Отпадните води;

10) Поштенските и курирски услуги;

11) Управувањето со отпад;

12) Изработката, производството и дистрибуцијата на хемикалии;

13) Производството, преработката и дистрибуцијата на храна;

14) Производството;

15) Давателите на дигитални услуги и

16) Истражувањето.

(3) Одредбите на овој закон се применуваат на сите правни лица со регистрирано седиште во Републиката, доколку:

1) се давател/оператор на јавни електронски комуникациски мрежи или јавно достапни електронски комуникациски услуги;

2) е давател на доверливи услуги;

3) кое го води Единствениот регистар на врвни домени (доменот мк и доменот mkd) согласно закон;

4) е давател на ДНС услуги;

5) е единствен давател на услуга во Републиката која е суштинска за одржување на општествени или економски активности;

6) услугата што ја обезбедуваат има значително влијание врз јавната безбедност, јавната заштита или јавното здравје;

7) услугата што ја обезбедуваат предизвикува значителни системски ризици, особено во областите во кои таквото нарушување може да има прекугранично влијание;

8) поради својата посебна важност, се смета за критични за одредена област или тип услуга или за други меѓусебно зависни области во Републиката;

9) се сопственици/оператори на критична инфраструктура, согласно закон или

10) обезбедуваат услуги за регистрација на имиња на домени.

(4) За секој од областите од ставот (2) на овој член, се утврдуваат повеќе подобласти.

Исклучоци од примена на законот

Член 5

(1) По исклучок од членот 4 ставот (1) од овој закон, одредбите од овој закон не се задолжителни за органите од областа на безбедноста, одбраната и органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела, и тоа:

1) Министерството за внатрешни работи;

2) Агенцијата за национална безбедност на Република Северна Македонија;

3) Оперативно-техничката Агенција;

4) Дирекцијата за безбедност на класифицирани информации;

5) Агенцијата за разузнавање;

6) Министерството за одбрана и

7) Јавното обвинителство на Република Северна Македонија.

(2) Одредбите од овој закон не се применуваат за Народната банка на Република Северна Македонија (во натамошниот текст: Народната банка).

(3) Одредбите од овој закон не се применуваат на другите субјекти кои обезбедуваат услуги исклучиво за органите од областа на безбедноста и одбраната и органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела.

(4) Исклучоците од ставовите (1) и (3) на овој член, не важат доколку органите од областа на безбедноста и одбраната и органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела, односно субјектите кои им даваат услуги на овие органи се јавуваат како даватели на доверливи услуги.

(5) Овој закон не се применува на комуникациско-информациските системи кои се безбедносно акредитирани согласно Законот за класифицирани информации.

Примена на другите закони

Член 6

(1) Суштинските и важните субјекти, надлежните органи и тимовите за одговор на компјутерски инциденти ги обработуваат личните податоци само до оној степен кој што е потребен за целите на овој закон и во согласност со прописите за заштита на личните податоци. Примената на одредбите од овој закон не влијае на обврските на суштинските и важните субјекти да известуваат во случај на нарушување на безбедноста на личните податоци во согласност со Законот за заштита на личните податоци.

(2) Доколку при спроведувањето на овој закон произлезат или пак се користат класифицирани информации, за тие информации се применуваат прописите за класифицираните информации.

(3) Примената на одредбите од овој закон не влијае на обврските на давателите/операторите на јавни електронски комуникациски мрежи и давателите на јавно достапни електронски комуникациски услуги да ги обработуваат личните податоци во согласност со посебните прописи за заштита на личните податоци.

(4) Примената на одредбите од овој закон не влијае на обврските за спроведување на основните услови за електронската комуникациска инфраструктура и другата поврзана опрема уредени со законот со кој се регулираат електронските комуникации.

(5) Примената на одредбите од овој закон не влијае на правилата за регистрација на врвните национални интернет домени и управувањето со Единствениот регистар на имиња на врвни домени (доменот mk и доменот мкд), како и на правата и обврските на корисниците на домени пропишани со закон.

(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 Републиката.

(7) Со посебните закони работите кои се однесуваат на критериумите и правилата за безбедност на мрежни и информациски системи, како и надзорот и прекршоците може да се уредат поинаку од овој закон, доколку не се во спротивност со целите на овој закон и не ја намалуваат безбедноста на мрежните и информациските системи.

Детални листи на области со висока критичност и други критични области

Член 7

(1) Владата на предлог на Министерството утврдува:

1) детална листа на области и видови на субјекти од областите со висока критичност од член 4 став (2) од овој закон;

2) детална листа на подобласти и видови на субјекти во другите критични области од членот 4 ставот (2) од овој закон;

3) детална листа на суштински субјекти;

4) детална листа на важни субјекти и

5) деталната листа на правните лица од членот 4 став (3) точките 2), 3), 4), 5) и 6) од овој закон.

(2) Предлог листите од ставот (1) точките 1) и 2) на овој член, Министерството ги подготвува согласно со мерките и правилата согласно закон, законодавството на ЕУ и други релевантни меѓународни мерки и правила.

(3) Предлог листите од ставот (1) точките 3) и 4) на овој член, Министерството ги подготвува врз основа на критериумите за класификација на субјектите утврдени со членот 8 од овој закон.

(4) Деталните листи од ставот (1) точките 1) и 2) на овој член, Владата на предлог на Министерството, ги ажурира кога ќе настанат промени на мерките и правилата на законодавството на ЕУ и други релевантни меѓународни мерки и правила за безбедност на мрежните и информациските системи.

(5) Деталните листи од ставот (1) точките 3) и 4) на овој член, особено содржат податоци за називот на субјектите, нивните контакти (седиште, телефон, електронска адреса), услугите кои ги даваат, односно активностите кои ги вршат и опсегот на IP на субјектот.

(6) Владата на предлог на Министерството редовно ги ажурира деталните листи од ставот (1) точките 3), 4) и 5) на овој член, кога треба да се додадат или бришат субјекти или правни лица.

(7) Пред да го достави предлогот за ажурирање на листите од ставот (1) точките 3) и 4) на овој член, Министерството задолжително прибавува мислење од надлежните органи и со сите субјекти кои дополнително ќе бидат опфатени или отстранети од листите.

(8) Надлежните органи од ставот (7) на овој член, се должни да го информираат Министерството за потребата од редовно ажурирање на деталните листи од ставот (1) точки 3) и 4) на овој член, доколку настанат промени во областа за која тие се надлежни.

(9) Врз основа на листите од ставот (1) на овој член, Министерството во електронска форма води:

1) регистар на области со висока критичност;

2) регистар на други критични области;

3) регистар на суштински субјекти и

4) регистар на важни субјекти.

(10) Податоците од регистрите од ставот (9) на овој член, се класифицирани информации со соодветен степен на тајност, согласно со законот со кој се уредуваат класифицираните информации.

(11) Начинот на идентификација на областите и подобластите и видовите субјекти заради утврдување на деталните листи од ставот (1) точките 1) и 2) на овој член, начинот на класификација на деталните листи од ставот (1) точките 3) и 4) на овој член, формата и содржината на деталните листи, како и формата, содржината и начинот на водење на регистрите од ставот (9) на овој член на предлог на министерот за дигитална трансформација (во натамошниот текст: министерот) ги уредува Владата со уредба.

Суштински и важни субјекти

Член 8

(1) Суштински субјекти од аспект на безбедност на мрежни и информациски системи се:

1) големите субјекти кои припаѓаат на областите од членот 4 ставот (2) од овој закон;

2) даватели на квалификувани доверливи услуги, регистар на имиња на врвните домени (доменот mk и доменот мкд) или давател на ДНС услуги, независно од нивната големина;

3) оператори, односно даватели на јавни електронски комуникациски мрежи и/или јавно достапни електронски комуникациски услуги кои се сметаат за средни и големи субјекти;

4) институциите на јавниот сектор од членот 4 став (1) од овој закон;

5) субјектите, независно од нивната големина кои припаѓаат на групата на субјекти од членот 4 став (3) точките 2) и 3) од овој закон;

6) субјектите кои се утврдени како сопственици/оператори на критична инфраструктура;

7) субјектите кои согласно националното законодавство се утврдени како суштинските субјекти;

8) други субјекти, кои согласно закон или врз основа на направена проценка на ризик се утврдени како суштинските субјекти.

(2) Важните субјекти, од аспект на безбедност на мрежни и информациски системи се:

1) сите субјекти од деталната листа на областите со висока критичност од член 7 став (1) точка 1) од овој закон, а кои не спаѓаат во групата на суштинските субјекти согласно став (1) на овој член и

2) други субјекти, кои согласно закон или врз основа на направена проценка на ризик се утврдени како важни субјекти.

(3) Методологијата за проценка на ризик заради утврдување на суштинските субјекти од ставот (1) точката 8 на овој член, како и методологијата за проценка на ризик заради утврдување на важните субјекти од ставот (2) точката 2) на овој член ги пропишува надлежниот орган, за субјектите од негова надлежност.

(4) Надлежниот орган подготвува и води листа во електронска форма на суштински и важни субјекти од негова надлежност, која ја доставува до Министерството заради утврдување на деталните листи од членот 7 став (1) точките 3) и 4) од овој закон.

(5) Суштински и важните субјекти кои не се ставени на деталната листа на суштински субјекти од членот 7 став (1) точката 3) од овој закон, или на деталната листа на важни субјекти од членот 7 став (1) точката 4) од овој закон, а ги исполнуваат условите да бидат на овие листи се должни до надлежниот орган да достават известување дека ги исполнуваат условите за клучен субјект, односно важен субјект.

(6) Во суштинските субјекти од став (1) точка 1) на овој член, во зависност од големината и обемот на работа задолжително овластуваат најмалку едно лице за офицер за сајбер безбедност.

(7) Поблиските критериуми во однос на големината и обемот на работа за формирање на организациска единица, односно определувањето на офицер за сајбер безбедност ги пропишува министерот.

Субјекти кои немаат регистрирано седиште

Член 9

(1) Субјектите кои немаат регистрирано седиште во Републиката, должни се по електронски пат да регистрираат претставник во Министерството ако се даватели на:

1) ДНС услуги, регистри на имиња на врвни домени;
2) услуги за регистрација на имиња на домени;
3) услуги за компјутерска обработка во облак;
4) услуги за податочен центар;
5) услуги за мрежи за испорака на содржини;
6) управувани услуги;
7) управувани безбедносни услуги;
8) услуга на интернет продажба;
9) услуги на интернет-пребарувачи;
10) платформи за услуги за социјални мрежи,
11) услуги на суштински субјекти или
12) услуги на важните субјекти.

(2) Министерството води Регистар на овластени претставници од ставот (1) на овој член.

(3) За претставник може да биде назначено лице кое има постојано живеалиште или престојувалиште во Републиката.

(4) Регистрацијата од ставот (1) на овој член особено ги содржи следните податоци:

1) податоци за давателот на услугата (назив, седиште и контакт податоци);

2) релевантната област, подобласт и видот на субјектот согласно членот 7 став (1) точките 1) и 2) од овој закон;

3) име, презиме и матичниот број на лицето кое е регистрирано за претставник;

4) контакт податоци на претставникот (адреса, е-пошта и телефонски број);

5) опсегот на IP на субјектот.

(5) Субјектите од ставот (1) на овој член, се должни електронски да ја внесат секоја измена на податоците од ставот (3) на овој член, во рок не подолг од еден месец од датумот на извршената измена.

(6) Институциите од јавниот сектор не може да склучуваат договори за јавни набавки со субјектите од ставот (1) на овој член, кои нема да назначат свој претставник во Републиката.

(7) Министерството може да ја извести Европската Комисија (во натамошниот текст: ЕК) и Агенцијата за сајбер безбедност на Европската унија (ENISA) за субјектите од став (1) на овој член, кои нема да назначат свој претставник во Републиката, доколку се работи за субјект од земја членка на Европската унија (во натамошниот текст: ЕУ), Северно-атлантската договорна организација – НАТО (во натамошниот текст: НАТО),, односно соодветната држава, односно нејзиното надлежно тело за сајбер безбедност, доколку се работи за субјект кој не е од држава членка на ЕУ.

(8) Содржината и начинот на регистрација и на водењето на регистарот од ставот (2) на овој член, ги пропишува министерот.

База на податоци за регистрација на имиња на домени

Член 10

(1) Со цел да се придонесе за безбедноста, стабилноста и отпорноста на ДНС, регистрите на имиња на врвни домени (mk и мкд) 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 да соберат и објават само неопходни и пропорционални податоци, согласно законите за заштита 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 контакт точките кои управуваат со имињата на домени во рамките на врвните домени, како и контактите со нив. Информациите треба да содржат податоци за:

1) името на доменот;

2) датумот на регистрација;

3) името на корисникот на доменот, адресата на неговата е-пошта и телефонскиот број за контакт;

4) 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) Македонската академска истражувачка мрежа и давателите на услуги за регистрација на имиња на домени се должни да воспостават политики и постапки за регистрација, вклучително и постапки за верификација, за да се осигурат дека базите на податоци од ставот (1) на овој член, вклучуваат точни и целосни информации, кои треба да бидат јавно објавени.

(4) Регистрите на имиња на врвни домени и давателите на услуги за регистрација на имиња на домени, по извршената регистрација на домени, најдоцна во рок од седум дена од денот на регистрацијата ги објавува податоците за регистрација, во согласност со прописите што ја уредуваат заштитата на личните податоци.

(5) Правното лице кое го води Единствениот регистар 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 барања доставени од надлежен орган или друг субјект за кој со закон е утврдено дека може да ги побара истите, а притоа 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 веднаш, 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, Единствениот регистар на врвни домени и давателите на услуги за регистрација на имиња на домени се должни меѓусебно да соработуваат.

II. НАДЛЕЖНИ ОРГАНИ

Надлежни органи за безбедност на мрежни и информациски системи

Член 11

(1) Надлежни органи за спроведување на одредбите од овој закон се:

1) Министерството, како надлежен орган за субјектите од членот 4 став (1) точките 3), 4), 5), 6), 7) и 9) од овој закон и

2) Агенцијата за електронски комуникации преку Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) како надлежен орган за безбедност на мрежни и информациски системи за субјектите од членот 4 став (1) точките 1), 2), и 8), став (2) и став (3) од овој закон.

(2) Со посебни закони во кои се утврдени најмалку истите стандарди или повисоки стандарди од оние утврдени со овој закон може да се назначат или воспостават надлежни органи за субјектите од членот 4 ставови (2) и (3) од овој закон.

(3) Надлежните органи треба да обезбедат соодветни ресурси за да ги извршуваат задачите што им се доделени на ефективен и ефикасен начин.

Министерство за дигитална трансформација

Член 12

(1) Министерството како надлежен орган за безбедност на мрежни и информациски системи ги има следните надлежности:

1) на Владата и предлага стратегијата која ја опфаќа безбедноста на мрежните и информациските системи и акциски планови, како и прописи од областа на безбедноста на мрежните и информациските системи;

2) подготвува годишен план за работа како и извештај за реализација на годишниот план за работа на Министерството кои ги одобрува Владата;

3) подготвува план за одговор на сајбер безбедносни закани, значајни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи, во соработка со Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) и другите надлежни органи и институции;

4) изготвува упатства за начинот на проценка на информациската безбедност на мрежните и информациските системи на Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје, како и протоколи и технички правила за безбедноста на мрежните и информациските системи;

5) дава предупредувања, соопштенија и информации за ризици и инциденти до Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје;

6) постапува по пријавени или идентификувани инциденти на мрежните и информатичките системи на Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје;

7) води евиденција за пријавени инциденти на мрежата и информациските системи на Владата, министерствата, самостојните органи на државната управа, органите на државната управа во состав на министерствата, управните организации, општините, општините во градот Скопје и градот Скопје;

8) соработува со Национален центар за одговор на компјутерски инциденти (MKD-CIRT) и надлежните органи, како и со тимовите за одговор на компјутерски инциденти, вклучително и оние во рамките на органите од областа на безбедноста и одбраната, органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела и Народната банка заради размена на информации за сајбер безбедносни закани, значајни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи;

9) 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;

10) утврдува и до Владата доставува предлог детална листа на области со висока критичност, предлог детална листа на други критични области, предлог детална листа на суштински субјекти и предлог детална листа на важни субјекти;

11) води регистар на области со висока критичност, регистар на други критични области, регистар на суштински субјекти, регистар на важни субјекти и регистар на правни лица кои се даватели на услуги за регистрација на имиња на домени;

12) води Регистар на инциденти за субјектите од негова надлежности и доставува известување до Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) согласно одредбите од овој закон;

13) промовира употреба на сајбер безбедносни алатки и апликации со отворен код и отворени стандарди;

14) врши функција на единствена точка за контакт за безбедност на мрежни и информациски системи и врши координација на надлежните органи од членот 11 став (1) точката 2) и ставот (2) од овој закон;

15) соработува со организациите и мрежите на ЕУ и НАТО надлежни за управување со сајбер безбедносни инциденти со голем опфат и кризи;

16) ја врши функцијата тим за одговор на компјутерски инциденти за органите на извршната власт (GOV-CSIRT) ;

17) подготвува Годишен извештај за состојбите во сајбер безбедноста;

18) обезбедува помош за воспоставување на механизми за споделување на информации за сајбер безбедноста преку повеќе канали, вклучително и соодветна платформа;

19) обезбедува стручна поддршка за сите заинтересирани субјекти согласно овој закон;

20) промовира и поддржува активна сајбер заштита

21) организира и спроведува специјализирани обуки од областа на сајбер безбедноста и организира кампањи во согласност со овој закон;

22) дефинира мерки за безбедност на мрежни и информациски системи;

23) врши надзор над суштинските и важните субјекти во однос на кои има надлежност и им наметнува мерки во случај кога истите не ги исполнуваат обврските утврдени со овој закон;

24) дава мислење, изготвува и учествува во изготвување на закони и други прописи, стратегии и планови од области поврзани со неговата надлежност;

25) го води единствениот портал за сајбер безбедност и

26) врши и други работи утврдени со закон кои се однесуваат на безбедноста на мрежните и информациските системи.

(2) Формата, содржината и начинот на водење на евиденцијата на пријавени инциденти на мрежата и информациските системи од ставот (1) точката 7) на овој член, ги пропишува министерот.

Соработка

Член 13

(1) Министерството согласно своите надлежности утврдени во членот 12 од овој закон, а во насока на спроведување на одредбите од овој закон, соработува со домашни и меѓународни организации, институции, тела и други заинтересирани страни и со нив склучува меморандуми или протоколи за соработка.

(2) Министерството согласно ставот (1) на овој член, во областа на безбедноста на мрежни и информациски системи особено соработува со домашни институции и тела надлежни за:

1) безбедност и одбрана на Републиката;

2) заштита на личните податоци;

3) електронска идентификација и доверливи услуги;

4) критична инфраструктура;

5) работење на банкарскиот и финансискиот сектор,

6) електронски комуникации;

7) високо образование и

8) управување со кризи.

(3) Министерството со органот на државната управа надлежен за управување со критична инфраструктура во Републиката редовно соработува и разменува информации во однос на утврдувањето на критични субјекти во државата, за сајбер безбедносни ризици и други ризици, закани и инциденти кои влијаат на критичните субјекти, како и за преземените мерки за одговор на таквите ризици, закани и инциденти.

(4) Министерството со институциите и телата надлежни за безбедноста и одбраната на државата, управувањето со кризи, институциите и телата надлежни за електронска идентификација и доверливи услуги, работењето на банкарскиот и финансискиот сектор, телата надлежни за цивилниот авио сообраќај, како и другите заинтересирани страни редовно разменува информации за релевантни сајбер закани и инциденти, а согласно склучен меморандум или протокол за соработка.

(5) Министерството врши редовни консултации со органите од областа на безбедноста и одбраната и органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела, од членот 5 ставот (1) од овој закон.

(6) Министерството 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, а соработува и со други домашни надлежни институции и тела за координирани проценки на безбедносни ризици при снабдување на ИКТ-услуги, ИКТ-системи и ИКТ-производи, земајќи ги предвид техничките и не-техничките фактори на ризик, имајќи ги предвид идентификуваните фактори на ризик од страна на институциите на ЕУ и НАТО.

(7) Министерството согласно ставот (1) на овој член, особено соработува со Агенција за сајбер безбедност на ЕУ (ENISA) и организациите и мрежите на ЕУ надлежни за управување со сајбер безбедносни инциденти со голем опфат и кризи (EU-CyCLONe) и други институции и тела на ЕУ и НАТО за управување со сајбер безбедносни ризици и инциденти.

Подигнување на јавната свест за сајбер безбедноста

Член 14

(1) Министерството организира и спроведува кампањи за подигнување на јавната свест, особено за важноста на сајбер безбедноста.

(2) Заради подигање на свеста за сајбер безбедноста и за унапредување на сајбер хигиената кај учениците, Министерството во соработка со Министерството за образование и наука ќе развие и имплементира едукативни програми во основните и средните училишта.

(3) Заради подигање на свеста за сајбер безбедноста и за унапредување на сајбер хигиената кај останатата популација Министерството во соработка со медиумите ќе развие и имплементира едукативни програми за пошироката јавност.

(4) Министерството се грижи за постојано стручно усовршување на своите вработени кои извршуваат работни задачи од областа на сајбер безбедноста и надзорот.

(5) Министерството подготвува предлози на теми за специјализирани обуки од областа на сајбер безбедноста за вработените во јавниот сектор, како и методологија за нивно спроведување кои може да ги реализира или во согласност со закон да ги достави за реализација до институцијата надлежна за стручно усовршување и обука на вработените во јавниот сектор.

(6) Во реализацијата на активностите од ставовите (1), (2), (3), (4) и (5) на овој член, Министерството може да побара поддршка од Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) и надлежните органи.

(7) Министерството и другите надлежни органи се должни да изработуваат упатства и прирачници на разбирлив јазик, најдобри практики и едукативни материјали за спроведување на одредбите од овој закон, како и за пријавување на сајбер безбедносните инциденти, кои ќе бидат објавени на нивните интернет страници.

(8) За реализација на активностите од ставовите (1), (2), (3), (4) и (5) на овој член, Министерството соработува со домашни и меѓународни високо-образовни и научни установи.

Единствена точка за контакт

Член 15

(1) Функцијата на единствена точка за контакт за безбедност на мрежни и информациски системи (во натамошниот текст: Единствена точка за контакт) ја врши Министерството.

(2) Министерството како Единствена точка за контакт:

1) обезбедува соработка со надлежните органи од областите;

2) ги проследува примените релевантни информации за инциденти од меѓународни надлежни тела до Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) и надлежни органи;

3) ги проследува известувањата за значаен инцидент со прекугранично влијание до точката за контакт или еквивалентно такво тело на друга засегната држава;

4) обезбедува координација на прекугранична соработка во областа на безбедноста на мрежните и информациските системи со релевантни државни органи и тела на други држави, а по потреба и со ЕК, Агенција за сајбер безбедност на ЕУ (ENISA) и НАТО и

5) соработува со организациите и мрежите на ЕУ надлежни за управување со сајбер безбедносни инциденти со голем опфат и кризи (EU-CyCLONe).

(3) Надлежниот тим за одговор на компјутерски инциденти е должен да го информира Министерството како единствена точка за контакт за инциденти, сајбер закани и избегнати инциденти поднесени во согласност со овој закон.

(4) Министерството треба да обезбеди соодветни ресурси за да ги извршува, на ефективен и ефикасен начин задачите што му се доделени согласно ставот (2) на овој член.

(5) Заради централизирано и унифицирано регистрирање на суштинските и важните субјекти и пријавување на сајбер безбедносните инциденти, како и заради олеснето вршење на надзор и достапност на едно место на сите податоци, информации и акти поврзани со сајбер безбедноста кои произлегуваат од овој закон, Министерството воспоставува и одржува единствен портал за сајбер безбедност.

(6) Преку порталот од ставот (5) на овој член, ќе се генерираат сите податоци во Националниот регистар на сајбер инциденти.

(7) Суштинските субјекти од членот 8 ставот (1) од овој закон, и важните субјекти од членот 8 ставот (2) од овој закон задолжително ќе бидат регистрирани и ќе ги пријавуваат сајбер инцидентите согласно одредбите од овој закон, преку порталот од ставот (5) на овој член.

(8) Начинот на пристап и користење на порталот од ставот (5) на овој член, ги пропишува министерот.

Национален центар за одговор на компјутерски инциденти (MKD-CIRT)

Член 16

(1) Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) кој претставува посебна организациона единица во рамките на Агенцијата за електронски комуникации како надлежен орган за безбедност на мрежни и информациски системи во областите и субјектите од членот 4 ставови (2) и (3) од овој закон, ги врши следните работи:

1) подготвува годишен план за работа на Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) како и извештај за реализација на годишниот план за работа во координација со Министерството, кој го одобрува Владата;

2) изготвува упатства за начинот на проценка на информацискатa безбедност на мрежните и информациските системи на субјектите за кои е надлежен, како и протоколи и технички правила за безбедноста на мрежните и информациските системи;

3) дава предупредувања, соопштенија и информации за ризици, закани, ранливости, напади и инциденти до субјектите за кои е надлежен;

4) постапува по пријавени инциденти на мрежните и информатичките системи на субјектите за кои е надлежен;

5) води евиденција за пријавени инциденти на мрежните и информациските системи на субјектите за кои е надлежен;

6) соработува со Министерството и со надлежни органи, како и со тимовите за одговор на компјутерски инциденти, вклучително и оние во рамките на органите од областа на безбедноста и одбраната, органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела и Народната банка на Република Северна Македонија заради размена на информации за сајбер безбедносни закани, значајни сериозни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи, во согласност со овој закон;

7) соработува со домашни и меѓународни организации, институции и тела во однос на справување со сајбер безбедносни инциденти;

8) се грижи за безбедноста на мрежните и информациските системи за субјектите од негова надлежност, преку проактивен пристап, со дефинирање на мерки, континуиран надзор и давање на препораки;

9) ја информира јавноста и засегнатите страни за состојбите со сајбер безбедноста во областите за кои е надлежен;

10) води Национален регистар на сајбер инциденти;

11) промовира употреба на сајбер безбедносни алатки и апликации со отворен код и отворени стандарди во областите за кои е надлежен;

12) дава поддршка на Министерството при подготовка на стратешкиот документ за сајбер безбедност;

13) соработува со Министерството при подготовка на предлог-Планот за одговор на сајбер безбедносни закани, значајни сериозни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи;

14) ја врши функција на тим за одговор на компјутерски инциденти во областите за кои е надлежен;

15) доставува податоци до Министерството потребни за донесување Годишен извештај за состојбите во сајбер безбедноста;

16) обезбедува помош за воспоставување на механизми за споделување на информации за сајбер безбедноста преку повеќе канали, вклучително и соодветна платформа во областите за кои е надлежен;

17) обезбедува стручна поддршка за сите заинтересирани субјекти согласно овој закон во областите за кои е надлежен;

18) промовира и поддржува активна сајбер заштита во областите за кои е надлежен;

19) организира и спроведува специјализирани обуки од областа на сајбер безбедноста и организира кампањи во согласност со овој закон во областите за кои е надлежен;

20) врши надзор над суштинските и важните субјекти во однос на кои има надлежност и им наметнува мерки во случај кога истите не ги исполнуваат обврските утврдени со овој закон;

21) дава мислење и предлози и учествува во изработка на закони, стратегии и планови од области поврзани со нејзината надлежност;

22) предлага на Агенцијата за електронски комуникации акти потребни за спроведување на овој закон и

23) врши и други работи утврдени со овој закон и законот кој ги уредува електронските комуникации.

(2) Заради водење на Националниот регистар на сајбер инциденти, сите тимови за одговор на компјутерски инциденти се должни веднаш, а најдоцна во рок од пет дена од денот на настанување, да достават извештај до Национален центар за одговор на компјутерски инциденти за настанатиот инцидент.

(3) Националниот центар за одговор на компјутерски инциденти доставува до Министерството најмалку два извештаи (полугодишен и годишен) за настанатите сајбер инциденти за периодот на кој се однесуваат.

(4) Пристап до Националниот регистар од ставот (1) точката 10) на овој член, имаат органите од областа на безбедноста, одбраната и спроведувањето на законот заради извршување на нивните законски надлежности.

(5) Формата, содржината и начинот на водење на евиденцијата на пријавени инциденти на мрежата и информациските системи од ставот (1) точката 5) на овој член, ја пропишува директорот на Агенцијата за електронски комуникации.

(6) Формата, содржината и начинот на водење на Националниот регистар на сајбер инциденти од ставот (1) точката 10) на овој член, ја пропишува директорот на Агенцијата за електронски комуникации.

Надлежни органи за областите

Член 17

(1) Со посебните закони може да се основаат други надлежни органи за областите и субјектите од членот 4 ставовите (2) и (3) од овој закон и нивните надлежности, доколку тоа не е во спротивност со целите на овој закон и не ја намалува безбедноста на мрежните и информациските системи.

(2) Надлежниот орган од ставот (1) на овој член, ги има особено следните надлежности:

1) изготвува упатства за начинот на проценка на информацискатa безбедност на мрежните и информациските системи на субјектите за кои е надлежен, како и протоколи и технички правила за безбедноста на мрежните и информациските системи;

2) дава предупредувања, соопштенија и информации за ризици и инциденти до субјектите за кои е надлежен;

3) постапува по пријавени инциденти на мрежните и информациски системи на субјектите за кои е надлежен и ги проследува истите до надлежниот тим за одговор на компјутерски инциденти;

4) води евиденција за пријавени инциденти на мрежата и информациските системи на субјектите за кои е надлежен;

5) соработува со Министерството и со надлежните органи заради размена на информации за сајбер безбедносни закани, значајни сериозни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи и информации за нивно надминување, во согласност со овој закон;

6) соработува со домашни и меѓународни организации, институции и тела во однос на справување со сајбер безбедносни инциденти;

7) во соработка со Министерството се грижи за безбедноста на мрежните и информациските системи, преку проактивен пристап, со дефинирање на мерки, континуиран надзор и давање на препораки;

8) врши следење, анализа, рано предупредување и информирање за сајбер закани, ранливости и инциденти;

9) ја информира јавноста и засегнатите страни за степенот на реализација на упатствата и процедурите, за бројот на пријавените инциденти и за други прашања поврзани со сајбер безбедноста во областа за која е надлежен;

10) спроведува и унапредува мерки за управување со сајбер безбедносни ризици и за известување за значителни инциденти;

11) ги проследува пријавите за сајбер инциденти до Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), веднаш, а најдоцна во рок од 24 часа;

12) доставува податоци до Министерството потребни за донесување Годишен извештај за состојбите во сајбер безбедноста;

13) обезбедува помош за воспоставување на механизми за споделување на информации за сајбер безбедноста преку повеќе канали, вклучително и соодветна платформа;

14) обезбедува стручна поддршка за сите заинтересирани субјекти согласно овој закон;

15) промовира и поддржува активна сајбер заштита;

16) организира и спроведува специјализирани обуки од областа на сајбер безбедноста и организира кампањи во согласност со овој закон;

17) врши надзор над суштинските и важните субјекти во однос на кои има надлежност и

18) врши и други работи утврдени со овој закон.

(3) Со посебните закони од ставот (1) на овој член, преку партнерство со други институции на јавниот сектор или преку јавно приватно партнерство може да се воспостават и тимови за одговор на компјутерски инциденти (секторски CSIRT) за областите и субјектите од членот 4 ставовите (2) и (3) од овој закон.

(4) Доколку надлежните органи од ставот (1) на овој член не воспостават тим за одговор на компјутерски инциденти, надлежен тим за одговор е Националниот центар за одговор на компјутерски инциденти (MKD-CIRT).

(5) Формата, содржината и начинот на водење на пријавени инциденти на мрежата и информациските системи од ставот (2) точката 4) на овој член, ја утврдува раководното лице на надлежниот орган.

Тим за координација на одговори по инциденти со голем опфат и кризни состојби

Член 18

(1) Заради справување и одговор по инциденти со голем опфат и кризни состојби предизвикани поради нарушување на безбедноста на мрежните и информациските системи се воспоставува Тим за координација на одговор по инциденти со голем опфат и кризни состојби (во натамошниот текст: Тим за координација).

(2) Доколку инцидентите со голем опфат довеле до прогласување на кризна состојба согласно закон, Тимот за координација работи во рамките на Центарот за управување со кризи согласно законот со кој се уредува управувањето со кризи.

(3) Доколку инцидентите со голем опфат не довеле до прогласување на кризна состојба, Тимот за координација работи во рамките на Министерството согласно со одредбите од овој закон.

(4) Во случаите од ставот (2) на овој член, тимот за координација го сочинуваат членовите на Управувачкиот комитет согласно прописите за управување со кризи, во кој задолжително е вклучен министерот за дигитална трансформација, а по потреба може да се вклучат и Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), раководителите на надлежните органи, како и експерти од областа на безбедноста на мрежните и информациските системи, а со тимот раководи министерот.

(5) Во случаите од ставот (3) на овој член, тимот за координација го сочинуваат министерот како координатор, претставник од тимот за одговор на компјутерски инциденти за органите на извршната власт (GOV-CSIRT), раководителот на Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), раководителите на надлежните органи, раководните лица на тимовите за одговор на компјутерски инциденти во рамките на државните органи, органите од областа на безбедноста и одбраната, органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела, Народната банка и високо-образовните установи, како и експерти од областа на безбедноста на мрежните и информациските системи.

(6) Начинот на работа на Тимот за координација на одговори по инциденти со голем опфат и кризни состојби одговор на компјутерски инциденти во случаите од ставот (3) на овој член, го пропишува министерот.

Податоци и информации кои не се достапни на јавноста

Член 19

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

(2) Субјектите сами определуваат кои податоци се деловна тајна и подлежат на заштита.

(3) Министерот, заменикот на министер, државниот секретар, административните службеници и другите лица ангажирани во Министерството 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 класифицираните информации, како и на деловните тајни на субјектите, трае и по престанокот на работниот однос во Министерството или по престанокот на мандатот, односно ангажманот.

Тимови за одговор на компјутерски инциденти (CSIRT)

Член 20

(1) Заради одговор и справување со компјутерски инциденти со овој закон се воспоставуваат следните тимови за одговор на компјутерски инциденти:

- MKD-GOV-CSIRT- Тим за одговор на компјутерски инциденти за органите на извршната власт во рамките на Министерството, како надлежен тим за одговор на компјутерски инциденти за субјектите од членот 4 став (1) точките 3), 4), 5), 6), 7) и 9) од овој закон и

- MKD-CIRT – Националниот центар за одговор на компјутерски инциденти во рамките на Агенцијата за електронски комуникации, како надлежен тим за одговор на компјутерски инциденти надлежен за субјектите од членот 4 став (1) точките 1), 2), и 8), ставовите (2) и (3) од овој закон.

(2) Тимовите за одговор на компјутерски инциденти треба да располагаат со соодветна, безбедна комуникациска и информациска инфраструктура преку која се должни да овозможат и по електронски пат да разменуваат информации со суштинските субјекти и важните субјекти и со други субјекти, во случај на сајбер безбедносни закани, значајни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи, како и во други случаи во кои е потребна размена на информации. За таа цел, тимовите за одговор на компјутерски инциденти промовираат користење дигитални алатки за безбедна размена на информации.

Мрежа на тимови за одговор на компјутерски инциденти

Член 21

(1) Заради унапредување на соработката помеѓу тимовите за одговор на компјутерски инциденти се воспоставува Мрежа на тимови за одговор на компјутерски инциденти во чија работа учествуваат претставници од:

1) Тим за одговор на компјутерски инциденти за органите на извршната власт;

2) Националниот центар за одговор на компјутерски инциденти (MKD-CIRT);

3) Тимови за одговор на компјутерски инциденти за областите и субјектите од член 4 ставовите (2) и (3) од овој закон;

4) Тимовите за одговор на компјутерски инциденти во рамките на органите од областа на безбедноста и одбраната, органот кој ги гони сторителите на кривични дела и на други со закон утврдени казниви дела и Народната банка и/или

5) Тимовите за одговор на компјутерски инциденти во рамките на високо-образовните установи.

(2) Мрежа на тимови за одговор на компјутерски инциденти од ставот (1) на овој член се состанува најмалку еднаш месечно, а ја координира претставникот на Тимот за одговор на компјутерски инциденти за органите на извршната власт.

(3) На Мрежата на тимови за одговор на компјутерски инциденти се разгледуваат сите прашања од значење за одговор на компјутерски инциденти и се координираат активностите на тимовите, кога е потребно заедничко делување или поддршка на некој од тимовите за одговор на компјутерски инциденти од другите тимови.

(4) Тимовите за одговор на компјутерски инциденти кои се дел од Мрежата од ставот (1) на овој член се должни меѓусебно да соработуваат, таму каде е соодветно да разменуваат релевантни информации, како и да си даваат стручна поддршка.

(5) Тимовите за одговор на компјутерски инциденти се должни да соработуваат со Агенцијата за сајбер безбедност на ЕУ (ENISA), организациите и мрежите на ЕУ надлежни за управување со сајбер безбедносни инциденти со голем опфат и кризи (EU-CyCLONe) и други институции и тела на ЕУ и НАТО.

(6) Националниот центар за одговор на компјутерски инциденти и тимовите за одговор на компјутерски инциденти и субјектите од членот 4 ставовите (2) и (3) од овој закон се должни да соработуваат со Тимот за одговор на компјутерски инциденти за органите на извршната власт и да постапуваат по неговите насоки и барања.

(7) Тимот за одговор на компјутерски инциденти за органите на извршната власт може да учествува во мрежата на CSIRT на ЕУ и на други еквивалентни такви меѓународни мрежи.

(8) Тимовите за одговор на компјутерски инциденти воспоставуваат 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 протоколи за споделување информации.

(9) Тимовите за одговор на компјутерски инциденти во својата работа и развој ги земаат предвид препораките и насоките на ЕК и Агенцијата за сајбер безбедност на ЕУ (ENISA), како и на НАТО.

(10) Начинот на работа на Мрежата на тимови за одговор на компјутерски инциденти се уредува со деловник, кој со мнозинство гласови го донесуваат членовите на Мрежата.

Услови кои треба да ги исполнат тимовите за одговор на компјутерски инциденти

Член 22

(1) Тимовите за одговор на компјутерски инциденти од членот 20 ставовите (1) и (2) од овој закон треба да ги исполнуваат следните услови:

1) да обезбедат повеќе различни канали за комуникација кои ќе бидат достапни постојано, при што се должни да внимаваат прекинот на еден од повеќето канали да не доведе до прекин на сите канали за двонасочна комуникација

2) на своите интернет страници да ги наведат каналите за комуникација и за нив да ги запознаат своите клиенти/конституенти и соработници;

3) просториите на тимот и придружните информациски системи да се наоѓаат на безбедни локации;

4) да бидат опремени со соодветен стандардизиран систем за управување и насочување на барањата, со цел обезбедување ефективна и ефикасна комуникација односно примопредавање;

5) да обезбедат доверливост и веродостојност на нивните активности, односно на нивните операции;

6) да располагаат со доволно вработени/ангажирани лица за да се обезбедат достапност на нивните услуги во секое време, а вработените треба да поседуваат сертификат за помината обука за работа во тимот за одговор на компјутерски инциденти која ја организира и/или спроведува Министерството;

7) да располагаат со неопходни технички способности и капацитети;

8) да обезбедат резервна копија на системите и резервен простор, со цел да се осигура континуитет во нивната работа, односно услуги и

9) да се усогласат со мерките, процедурите, упатствата, насоките, препораките и добрите практики на национално ниво, утврдени од надлежниот орган.

(2) За обезбедување доверливост и веродостојност на активностите и операциите, институцијата во чиј состав е тимот усвојува посебен Кодекс на однесување на вработените/ангажираните кои извршуваат работни задачи во тимовите, согласно овој закон и склучуваат поединечни договори со секој од вработените/ангажираните со кој детално се уредуваат обврските за доверливост и веродостојност, како и последиците за непочитување на овие обврски.

(3) Начинот на пријава и постапување по пријавени или идентификувани инциденти на мрежните и информатичките системи го пропишува раководното лице на органот во чиј состав е тимот за одговор на компјутерски инциденти.

(4) Бројот на вработени/ангажирани лица од ставот (1) точката 6) на овој член и неопходните технички способности и капацитети од ставот (1) точката 7) на овој член, ги утврдува раководното лице на надлежниот орган во чиј состав е тимот за одговор на компјутерски инциденти.

Надлежности на тимовите за одговор на компјутерски инциденти

Член 23

(1) Тимовите за одговор на компјутерски инциденти ги вршат следните задачи:

1) следат и анализираат сајбер закани, ранливости и инциденти во субјектите од нивна надлежност, а по барање да обезбедат помош на суштинските субјекти и важните субјекти во врска со следење на нивните мрежни и информациски системи во реално време;

2) доколку е можно во реално време до суштинските субјекти и важните субјекти, надлежните органи од членот 11 од овој закон и другите засегнати страни доставува рани предупредувања, најави, соопштенија и доставување на информации за сајбер закани, ранливости и инциденти;

3) обезбедуваат одговор на инциденти и онаму каде што е применливо, обезбедува помош на суштинските субјекти и важните субјекти, како и по барање на надлежните органи од членот 11 од овој закон и другите засегнати страни;

4) собираат и анализираат форензички податоци, обезбедуваат динамична анализа на ризици и инциденти и информираат за состојбите во сајбер безбедноста;

5) на барање на суштинските субјекти и важните субјекти, како и на барање на надлежните органи од членот 11 од овој закон и другите засегнати страни, поднесено преку суштинските и важните субјекти чии мрежни и информациски системи се скенираат, обезбедуваат проактивно скенирање на нивните мрежни и информациски системи, со цел откривање на ранливости со потенцијал за значително влијание;

6) за резултатите од извршеното проактивно скенирање согласно точката 5) на овој став, да ги известат субјекти чии мрежни и информациски системи се скенирани;

7) учествуваат во мрежата на тимови за одговор на компјутерски инциденти и обезбедуваат взаемна помош во согласност со своите капацитети и надлежности на други членови на мрежата по нивно барање и

8) придонесуваат за користење на алатки за безбедносна размена на информации.

(2) Тимовите за одговор на компјутерски инциденти може да спроведуваат проактивно ненаметливо скенирање на јавно достапни мрежни и информациски системи на суштинските субјекти и важните субјекти кои се во нивна надлежност. Скенирањето се врши со цел да се откријат ранливи или несигурно конфигурирани мрежни и информациски системи и за истото да се информираат засегнатите субјекти. Ваквото скенирање не треба да има негативно влијание врз функционирањето на услугите кои ги обезбедува операторот.

(3) При извршување на задачите од ставот (1) на овој член, тимовите за одговор на компјутерски инциденти може да приоретизираат одредени задачи врз основа на спроведена анализа на ризик.

(4) Заради постигнување на целите на овој закон, тимовите за одговор на компјутерски инциденти соработуваат со суштинските и важните субјекти од приватниот сектор, како и со други засегнати страни од приватниот сектор.

(5) Заради олеснување на соработката тимовите за одговор на компјутерски инциденти треба да применат заеднички или стандардизирани практики, шеми за класификација и класификации утврдени од Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) во врска со:

1) процедури за справување со инциденти;

2) управување со кризи и

3) координирано откривање на ранливост.

(6) Методологијата за спроведување на анализата на ризик од ставот (3) на овој член, ја пропишуваат надлежните органи на предлог на надлежните тимови за одговор на компјутерски инциденти, за областите за кои се надлежни.

Координирано откривање на ранливости

Член 24

(1) Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) е координатор во процесот на координирано откривање на ранливости кај ИКТ-производи или ИКТ-услуги, доколку откривањето на ранливости со други закони не е поинаку уредено.

(2) Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) ќе делува како 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 Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) како координатор се:

1) идентификување на засегнатите субјекти и контактирање со нив;

2) давање помош на физичките или правните лица кои пријавиле ранливост и

3) 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 Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) кој во однос на пријавената ранливост треба да обезбеди спроведување на потребните активности и да ја заштити 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, тимовите за одговор на компјутерски инциденти соработуваат со националните тимови 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 Тимот за одговор на компјутерски инциденти за органите на извршната власт, како член во мрежата на CSIRT на ЕУ.

Офицер за сајбер безбедност

Член 25

(1) Институциите од членот 4 ставот (1) од овој закон, во зависност од видот и бројот на мрежни и информациски системи и бројот на вработени во институцијата се должни да назначат еден или повеќе административни службеници како офицери за сајбер безбедност.

(2) Останатите суштински субјекти од членот 8 став (1) точките 1), 2), 3), 5), 6), 7) и 8) од овој закон, се должни да имаат вработено или на друг начин ангажирано офицер за сајбер безбедност.

(3) Офицерот за сајбер безбедност од ставот (1) на овој член, се назначува од редот на вработените со завршено високо образование од областа на ИКТ, телекомуникации, безбедност или право, врз основа на неговите стручни квалификации, а особено врз основа на стручни знаења за сајбер безбедноста и практиките во областа на сајбер безбедноста.

(4) Задачите и овластувањата на офицерот за сајбер безбедност вклучуваат, но не се ограничени на организација, координација и одговорност за извршување на следното:

1) спроведување и/или надзор на соодветната примена на одредбите содржани во овој закон и други подзаконски акти ;

2) следење и примена на меѓународни технички стандарди и правила, прописи за сајбер безбедност;

3) изработка и спроведување на сајбер безбедносна програма која ќе опфати политики, процедури и мерки за заштита од сајбер напади и зголемување на сајбер отпорноста на информациски технологии и оперативни технологии;

4) откривање на структурни и системски слабости и ризици во информациско комуникациските системи и мрежи, како и во физичката и виртуелната инфраструктура;

5) дефинирање на сценарија и процена на ризици по сајбер безбедноста во процесот на воспоставување на систем за управување со ризици;

6) редовно следење на ранливоста на системите, следење и проценка на актуелните опасности кон мрежните податоци и воведување мерки за ублажување на последиците од сајбер инциденти;

7) обезбедување на ажурирање на хардверските уреди и софтверските апликации;

8) координација во справувањето со потенцијалните сајбер напади и инциденти преку учество во преземање мерки за заштита на системите;

9) комуникација со раководните лица и останатите единици, како и со други засегнати субјекти за прашања од сајбер безбедноста во енергетиката;

10) редовна комуникација и координација со надлежниот орган и надлежниот тим за одговор на компјутерски инциденти и

11) задолжително и без одлагање пријавување на значајни сајбер безбедносни инциденти до надлежниот тим за одговор на компјутерски инциденти.

(5) Суштинските субјекти се должни на соодветен начин и навремено да го вклучат офицерот за сајбер безбедност во сите прашања поврзани со безбедноста на мрежните и информациските системи.

(6) Суштинските субјекти се должни да му обезбедат поддршка на офицерот за сајбер безбедност при извршувањето на работите од ставот (2) на овој член, обезбедувајќи им ресурси неопходни за извршување на тие работи и пристап до мрежните и информациските системи, како и одржување и унапредување на неговото стручно знаење.

(7) Суштинските субјекти се должни да гарантираат дека офицерот за сајбер безбедност нема да добива никакви упатства од раководните лица на субјектот, ниту да трпи било какви последици во однос на извршувањето на нивните работи.

(8) Офицерот за сајбер безбедност директно одговара пред раководните лица на суштинскиот субјект.

(9) Офицерот за сајбер безбедност е должен да ја почитува тајноста или доверливоста во однос на извршувањето на своите работи, во согласност со закон.

(10) Поблиските критериуми во однос видот и бројот на мрежни и информациски системи и бројот на вработени кои се услов за утврдување на бројот на офицери за сајбер безбедност согласно ставот (1) на овој член ги пропишува министерот.

(11) Потребните стручни квалификации, општи и посебни компетенции за офицер за сајбер безбедност во институциите од членот 4 ставот (1) од овој закон, ги пропишува министерот.

Национален координатор за безбедност на мрежни и информациски системи

Член 26

(1) Владата, на предлог на министерот назначува Национален координатор за безбедност на мрежни и информациски системи.

(2) Националниот координатор за безбедност на мрежи и информациски системи го координира разменувањето на податоци и информации поврзани со безбедност на мрежните и информациските системи во и надвор од државата.

(3) Националниот координатор за безбедност на мрежи и информациски системи ја координира соработката и учеството на надлежните органи во меѓународните организации.

III. РАМКА ЗА САЈБЕР БЕЗБЕДНОСТ

Стручна поддршка на субјектите

Член 27

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

(2) Во реализација на надлежностите од ставот (1) на овој член, Министерството може да побара поддршка од Националниот центар за одговор на компјутерски инциденти (MKD-CIRT) и надлежни органи за областите и субјектите од член 4 ставовите (2) и (3) од овој закон.

Промовирање на активна безбедност на мрежни и информациски системи

Член 28

(1) Министерството како надлежно за спроведување на стратегијата која ја опфаќа безбедноста на мрежните и информациските системи, треба да промовира и поддржува активна безбедност на мрежни и информациски системи која 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) Надлежниот орган согласно стратегијата која ја опфаќа безбедноста на мрежните и информациските системи од ставот (1) на овој член, може да понуди алатки за самостојна проверка, алатки за откривање и насоки за отстранување на сајбер безбедносни ризици за субјектите од негова надлежност.

(3) Стратегијата која ја опфаќа безбедноста на мрежните и информациските системи од ставот (1) на овој член, се усвојува за период од најмалку пет години, а секоја година сите носители на активности од акцискиот план доставуваат до Министерството извештаи за реализација на нивните обврски, врз основа на кои извештаи Министерството изготвува збирен извештај кој го доставува на усвојување до Владата.

Стратегија која ја опфаќа безбедноста на мрежните и информациските системи

Член 29

(1) Владата на предлог на Министерството ја усвојува стратегијата која ја опфаќа безбедноста на мрежните и информациските системи кој се однесува на сајбер безбедноста и кој вклучува и Акциски план за нејзина имплементација.

(2) Стратегијата која ја опфаќа безбедноста на мрежните и информациските системи од ставот (1) на овој член, Министерството го подготвува во соработка со останатите надлежни органи од членот 11 ставот (1) од овој закон, Министерството за внатрешни работи, Министерството за одбрана и други државни органи и правни лица на кои со закон им е доверено да вршат јавни овластувања кои се однесуваат на безбедност на мрежни и информациски системи.

(3) Со стратегијата која ја опфаќа безбедноста на мрежните и информациските системи 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, како и план со неопходни мерки, за подобрување на општото ниво на свесност за сајбер безбедноста кај граѓаните.

(4) Министерството во соработка со Националниот координатор за безбедност на мрежни и информациски системи од членот 25 ставот (1) од овој закон, е надлежно за следење на имплементацијата на стратегијата која ја опфаќа безбедноста на мрежните и информациските системи од ставот (1) на овој член.

План за одговор на сајбер безбедносни закани, сериозни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи

Член 30

(1) Владата на предлог на Министерството, усвојува План за одговор на сајбер безбедносни закани, значајни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи.

(2) Министерството предлогот на Планот од ставот (1) на овој член, го подготвува во соработка со Министерството за внатрешни работи, Министерството за одбрана, Центарот за управување со кризи, Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), надлежните органи за областите и субјектите од членот 4 ставовите (2) и (3) од овој закон, државни органи и тела надлежни за координација, управување и проценка на кризна состојба, согласно закон, високо-образовните установи, како и правни лица на кои со закон им е доверено да вршат јавни овластувања кои се однесуваат на безбедност на мрежни и информациски системи.

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

1) мерки и активности за обезбедување национална подготвеност, вклучувајќи вежби и активности за обука;

2) обврски и задачи на Министерството и другите надлежни органи и тела согласно овој закон;

3) процедури за управување со сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи, согласно закон;

4) субјектите и инфраструктурата на кои се однесува планот и

5) капацитетите, средствата и постапките што може да се применат во случај на сајбер безбедносна криза.

IV. МЕРКИ ЗА УПРАВУВАЊЕ СО САЈБЕР БЕЗБЕДНОСНИ РИЗИЦИ И ОБВРСКИ ЗА ИЗВЕСТУВАЊЕ

Управување со сајбер безбедносни ризици

Член 31

(1) Органите на управување на суштинските субјекти од членот 8 ставот (1) од овој закон и на важните субјекти од членот 8 ставот (2) од овој закон, се должни да донесат и најмалку еднаш годишно да направат проценка на ризиците согласно со методологијата од членот 8 ставот (3) од овој закон, како и да ги ажурираат мерките за управување со сајбер безбедносни ризици, согласно членот 32 од овој закон и да вршат надзор над нивното спроведување.

(2) Со цел спроведување на одредбата од ставот (1) на овој член, суштинските субјекти и важните субјекти се должни да обезбедат редовни обуки за членовите на нивните органи на управување и на нивните вработени 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 32

(1) Суштинските субјекти и важните субјекти се должни да преземат соодветни технички, оперативни и организациски мерки, сразмерни (пропорционални) на ризикот и во согласност со современите достигнувања, заради управување со ризиците кои претставуваат закана за нивните мрежни 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 суштинскиот, односно важниот субјект, 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, најмалку вклучуваат:

1) анализа на ризикот и безбедноста на информациските системи;

2) справување со инциденти;

3) континуитет на работењето, како што е управување со резервните копии и закрепнување по катастрофален испад и кризен менаџмент;

4) безбедност на ланецот на снабдување, вклучувајќи ги безбедносните аспекти на односот меѓу секој субјект и неговите директни добавувачи или обезбедувачи на услуги;

5) безбедност при набавување, развој и одржување на мрежни и информациски системи, вклучувајќи решавање ранливости и нивно откривање;

6) политики и постапки за процена на ефикасноста на мерките за управување со сајбер безбедносните ризици;

7) основни практики на сајбер хигиена и обуки за сајбер безбедност;

8) политики и постапки за користење на криптографски техники и соодветно шифрирање;

9) безбедност на човечките ресурси, политиките за контрола на пристап и управување со имот;

10) користење на повеќе-факторска автентификација или решенија за континуирана автентификација, заштитени гласовни, видео и текстуални комуникации и безбедни системи за комуникација во итни случаи во рамките на субјектот, според потребите.

(4) Суштинските субјекти и важните субјекти при определувањето на мерките кои треба да придонесат за безбедност на ланецот на снабдување, вклучувајќи ги безбедносните аспекти на односот меѓу секој субјект и неговите директни добавувачи или обезбедувачи на услуги треба да ја имаат предвид ранливоста што е специфична за секој непосреден добавувач и давател на услуги, квалитетот на производите и нивната сајбер безбедносна пракса, вклучувајќи ги и нивните безбедни развојни постапки, треба да ги имаат предвид резултатите од координираните проценки на безбедносните ризици на ланецот на снабдување.

(5) Техничките и методолошките барања за мерките од ставот (1) на овој член, кои се однесуваат на субјектите од членот 4 став (1) точките 3), 4), 5), 6), 7) и 9) од овој закон, ги пропишува Тим за одговор на компјутерски инциденти за органите на извршната власт (MKD-GOV_CSIRT).

(6) Техничките и методолошките барања за мерките од ставот (1) на овој член кои се однесуваат на субјектите од членот 4 став (1) точките 1), 2) и 8), ставовите (2) и (3) од овој закон, ги утврдува раководното лице на надлежниот орган, односно Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), доколку нема надлежен орган.

(7) Субјектот кој не ги исполнува мерките од ставот (3) на овој член, веднаш, а најдоцна во рок од 30 дена да ги презема сите неопходни, соодветни и пропорционални корективни активности за исполнување на овие мерки од ставор (3) на овој член.

(8) Технички и методолошки барања за мерките од ставот (3) на овој член, за суштинските и важните субјекти од ставовите (5) и (6) на овој член, надлежниот орган ги утврдува земајќи ги во предвид европските и меѓународните норми и релевантните технички спецификации.

Задолжително пријавување на значајни сајбер безбедносни инциденти и закани

Член 33

(1) Суштинските субјекти и важните субјекти се должни веднаш, а најдоцна во рок од три часа од моментот на дознавањето за настанување на инцидентот и/или сајбер заканата, да го известат надлежниот тим за одговор на компјутерски инциденти за секој значаен сајбер безбедносен инцидент и/или значајна сајбер закана што има влијание врз обезбедувањето на нивните услуги и да ги достават сите информации, со кои ќе ѝ овозможат да го утврди прекуграничното влијание на инцидентот. Доколку известувањето е доставено до надлежниот орган, тој е должен истото без непотребно одлагање, а не подоцна од два часа од моментот на прием на известувањето, да го проследи истото до надлежниот тим за одговор на компјутерски инциденти.

(2) Доколку е можно, суштинските субјекти и важните субјекти се должни, веднаш, а најдоцна наредниот работен ден од моментот на дознавањето за сајбер заканата 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) Со цел исполнување на обврските од ставовите (1) и (2) на овој член, суштинските и важните субјекти се должни:

1) во рок од 24 часа од дознавањето за значајниот сајбер безбедносен инцидент на надлежниот тим за одговор на компјутерски инциденти да му достават рано предупредување во коешто доколку е соодветно, ќе се наведе дали постои сомневање дека значајниот инцидент е предизвикан од незаконско или злонамерно дејствување или може да има прекугранично влијание;

2) во рок од 72 часа од дознавањето за значајниот сајбер безбедносен инцидент на надлежниот тим за одговор на компјутерски инциденти, да му достават известување за инцидентот во коешто, доколку е соодветно, ќе се ажурираат информациите од точката 1) 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;

3) на барање од надлежниот тим за одговор на компјутерски инциденти да му достават привремено известување за релевантните ажурирања на статусот;

4) на надлежниот тим за одговор на компјутерски инциденти во рок од еден месец по доставувањето на известувањето за значајниот сајбер безбедносен инцидент од точката 2) на овој став, да му достават завршно известување што го вклучува следново:

а) детален опис на инцидентот, вклучувајќи ја неговата сериозност и влијание;

б) типот на закана или главната причина што најверојатно го предизвикала инцидентот;

в) мерките за ублажување што се применили и се применуваат и

г) прекугранично влијание на инцидентот, доколку е соодветно.

5) во случај кога значајниот сајбер безбедносен инцидент е во тек во моментот на поднесувањето на завршното известување од точка 2) на овој став, до надлежниот тим за одговор на компјутерски инциденти да достават извештај за напредокот во тој момент, како и завршен извештај во рок од еден месец од решавањето на инцидентот.

(4) Давателот на доверливи услуги, без непотребно одложување, а најдоцна во рок од 24 часа од дознавањето за значајниот сајбер безбедносен инцидент е должен да го извести надлежниот тим за одговор на компјутерски инциденти за инцидентот кој има влијание врз давањето на неговите доверливи услуги.

(5) Надлежниот тим за одговор на компјутерски инциденти е должен во рок од 24 часа од приемот на раното предупредување од ставот (3) точката 1) на овој член, на суштинскиот, односно важниот субјект да му достави одговор, вклучувајќи ги првичните

повратни информации за значајниот сајбер безбедносен инцидент, а на барање на суштинскиот, односно важниот субјект, да му даде насоки или оперативни совети за спроведување на можни мерки за ублажување, како и дополнителна техничка поддршка.

(6) Доколку надлежниот тим за одговор на компјутерски инциденти не е прв примател на известувањето од ставот (1) на овој член, согласно со посебен закон, насоките или оперативните совети ги обезбедува надлежниот орган во соработка надлежниот тим за одговор на компјутерски инциденти.

(7) Надлежниот тим за одговор на компјутерски инциденти обезбедува дополнителна техничка поддршка доколку засегнатиот субјект тоа го побара.

(8) Доколку постои сомневање дека со значајниот сајбер безбедносен инцидент е сторено кривично дело, надлежниот тим за одговор на компјутерски инциденти ќе даде насока истиот да се пријави кај надлежните органи.

(9) Доколку значајниот сајбер безбедносен инцидент се однесува на повеќе држави, надлежниот тим за одговор на компјутерски инциденти покрај обврската од став (6) на овој член, е должен без непотребно одложување да го извести Министерството, кое најдоцна два часа од моментот на дознавањето ги известува засегнатите држави и им ги достави оние информации што се примени согласно став (3) на овој член, во соработка со суштинскиот, односно важниот субјект, притоа водејќи сметка за заштита на безбедноста и комерцијалните интереси на истиот, како и за доверливоста на доставените информации. Во рок од пет дена од денот на надминување на значајниот сајбер безбедносен инцидент со прекугранично влијание, тимот за одговор на компјутерски инциденти ќе достави детален извештај за инцидентот и/или заканата до Министерството, кое во рок од два дена го проследува деталниот извештај до засегнатите држави.

(10) Доколку за спречување или за решавање на значајниот сајбер безбедносен 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, Министерството може, по извршена консултација со засегнатиот суштинскиот, односно важниот субјект, да ја извести јавноста за значајниот сајбер безбедносен инцидент или да побара од соодветниот субјект да го направи тоа.

(11) Секој личен податок во извештаите за значаен сајбер безбедносен инцидент треба да биде ограничен на она што е строго неопходно за опис и решавање на инцидентот.

(12) Поблиските критериуми, како и прагот на определување на обични и значајни сајбер безбедносни инциденти се утврдуваат со методологии по области кои ги донесуваат надежните органи членот 11 од овој закон, за секоја област поединечно, односно за субјектите од својата надлежност, по претходна согласност на Министерството, а која се ажурира најмалку еднаш годишно.

Годишен извештај за состојбите во сајбер безбедноста

Член 34

(1) Министерството изготвува и доставува до Владата на усвојување Годишен извештај за состојбите во сајбер безбедноста.

(2) Годишен извештај од ставот (1) на овој член, содржи анонимизирани и збирни податоци за сајбер безбедносни закани, значајни сериозни сајбер безбедносни закани, значајни сајбер безбедносни инциденти, сајбер безбедносни инциденти со голем опфат и сајбер безбедносни кризи и избегнати инциденти, како и проценка за ризиците во областа на сајбер безбедноста имајќи ги предвид сајбер заканите, развојот на сајбер безбедносните капацитети во јавниот и приватниот сектор, проценка за свесноста на граѓаните и правните лица особено кај малите и средните субјекти за сајбер безбедноста и сајбер хигиената.

(3) Годишниот извештај од ставот (1) на овој член, содржи информации за имплементација на Националната стратегија за сајбер безбедност.

(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, Министерството го доставува до Владата најдоцна до 1 март во тековната за претходната година. По барање на Владата, Министерството е должно да и достави и збирен извештај и за пократок временски период.

(6) Заради подготовка на Годишниот извештај од ставот (1) на овој член, Националниот центар за одговор на компјутерски инциденти (MKD-CIRT), надлежните органи и секторските тимови за одговор на компјутерски инциденти за областите и субјектите од член 4 ставовите (2) и (3) од овој закон се должни најдоцна до 31 јануари во тековната за претходната година до Министерството да достават извештај со податоци од ставот (2) на овој член, за субјектите од својата надлежност.

(7) Тимовите за одговор на компјутерски инциденти, до Министерството се должни да достават и вонредни извештаи кога тоа ќе им биде побарано.

Примена на европски и меѓународни програми за сајбер безбедносна сертификација

Член 35

(1) Министерството задолжително ќе бара од суштинските и од важните субјекти да користат ИКТ-услуги, ИКТ-системи и ИКТ-производи кои се сертифицирани врз основа на европски и меѓународни програми за сајбер безбедносна сертификација, заради исполнување на техничките и методолошките барања од членот 32 ставовите (5) и (6) од овој закон и редовно ќе контролира дали се почитува оваа обврска.

(2) Министерството презема активности од промотивен и стимулативен карактер, преку спроведување на информативни и советодавни кампањи или на друг соодветен начин за поттикнување на суштинските субјекти и важните субјекти да користат квалификувани доверливи услуги.

(3) ИКТ- услугите, ИКТ-системите и ИКТ-производите од ставот (1) на овој член, како и критериумите за определување на суштинските и важните субјекти на кои ќе се однесува овој став ги пропишува министерот.

Стандарди за безбедност на мрежни и информациски системи

Член 36

(1) Министерството утврдува стандарди за безбедност на мрежните и информациските системи усогласени со ЕУ и меѓународните стандарди, како и упатства за нивна имплементација.

(2) Министерството во соработка со Министерство за финансии-Бирото за јавни набавки изготвува модели на технички спецификации за набавка на мрежни и информациски системи кои ќе бидат усогласени со меѓународните стандарди.

(3) Врз основа на упатствата од ставот (1) на овој член, Министерството воспоставува и води Регистар на ИКТ-услуги, ИКТ-системи и ИКТ-производи и нивни производители со висок ризик, кои нема да се земаат во предвид, односно се исклучуваат при постапките за јавни набавки.

V. РАЗМЕНА НА ИНФОРМАЦИИ

Механизми за размена на информации за сајбер безбедност

Член 37

(1) Субјектите од членот 4 од овој закон, а по потреба и други субјекти 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 алатки за откривање сајбер напади, доколку таквото споделување на информации:

1) има за цел да спречи или открие инцидент, одговори на инцидент, закрепне од инцидент или да го ублажи неговото влијание;

2) 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;

3) помогне за развивање на техники 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, се одвива во рамките на суштинските субјекти и важните субјекти и каде што е релевантно и со нивните добавувачи или даватели на услуги.

(3) Размената на информации се врши преку однапред дефинирани поедноставени процедури и воспоставени ИКТ алатки кои ги исполнуваат стандардите за безбедна размена на податоци и информации.

(4) Суштинските субјекти и важните субјекти се должни преку надлежниот орган да го известат Министерството за нивното учество во механизмите за споделување информации за сајбер безбедноста од ставот (2) од овој член или за нивното повлекување од учеството во таквите механизми.

(5) Министерството ќе обезбеди помош за воспоставување на механизми за споделување информации за сајбер безбедност од ставот (2) од овој член, преку примена на најдобрите практики од ЕУ и НАТО.

(6) Начинот на размена на податоците од ставот (2) на овој член, како и процедурите од ставот (3) на овој член ги утврдува раководното лице на надлежниот орган, за областите и субјектите од својата надлежност.

Доброволно известување за релевантни информации

Член 38

(1) Известувања на доброволна основа до надлежниот орган, надлежниот тим за одговор на компјутерски инциденти и Министерството може да достават:

1) суштинските субјекти и важните субјекти во врска со инциденти, сајбер закани и избегнати инциденти кои не се значителни;

2) субјекти различни од субјектите од точката 1) од овој став, без оглед на тоа дали припаѓаат во опфатот на примената на овој закон, во однос на значителни инциденти, сајбер закани или избегнати инциденти.

(2) Надлежниот тим за одговор на компјутерски инциденти ги обработува известувањата од ставот (1) на овој член, во согласност со постапката утврдена во членот 33 ставовите (5), (6), (7) и (8) од овој закон.

(3) Надлежниот тим за одговор на компјутерски инциденти е должен да им даде приоритет на обработката на задолжителните известувања, пред обработката на доброволните известувања.

(4) Надлежниот тим за одговор на компјутерски инциденти е должен да проследи информации до Министерството, како единствена точка за контакт за сите известувања добиени согласно ставот (1) на овој член.

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

VI. ПРАВА НА ВРАБОТЕНИТЕ ВО ТЕЛАТА ЗА ОДГОВОР НА КОМПЈУТЕРСКИ ИНДИЦЕНТИ

Обука на вработените во тимовите за одговор на компјутерски инциденти, на офицерите за сајбер безбедност и вработените во јавниот сектор

Член 39

(1) Вработените во тимовите за одговор на компјутерски инциденти, во организациските единици за сајбер безбедност и офицерите за сајбер безбедност имаат право и должност на стручно усовршување заради ефикасно извршување на своите работни задачи.

(2) Стручното усовршување од ставот (1) на овој член, се врши преку специјализирани обуки, кои ги обезбедува работодавачот.

(3) Министерството организира и/или спроведува специјализирана обука за офицерите за сајбер безбедност, а за поминатата обука издава сертификати.

(4) Надоместокот за обуката од ставот (3) на овој член, го плаќаат работодавачите односно субјектите во кои се ангажирани офицерите за сајбер безбедност, а приходите од надоместокот се приход на Буџетот на Република Северна Македонија.

(5) Меѓусебните права и обврски на работодавачот и вработениот кој е упатен на специјализирана обука од ставот (1) на овој член, се уредуваат со писмен договор во кој се утврдува точниот датум до кој вработениот не може да побара престанок на работниот однос како и неговата материјална одговорност која ќе изнесува петкратно поголем износ од средствата потрошени за реализација на обуката, доколку по негова вина или на негово барање му престане работниот однос пред утврдениот датум.

(6) Периодот во кој вработениот не може да бара престанок на работниот однос се определува согласно износот кој работодавачот го платил за обуката, и тоа по шест месеци за секој износ еднаков на просечната нето плата во Републиката исплатена во претходната година согласно податоците на Државниот завод за статистика.

(7) Сите вработени во институциите од јавниот сектор закон се должни да поминат генеричка обука за безбедност на мрежни и информациски системи, најмалку еднаш годишно согласно закон.

(8) Раководните лица на институциите од јавниот сектор подготвуваат годишен план за специјализирани обуки за своите вработени на кои согласност дава Министерството.

(9) Програмата за специјализирана обука за офицер за сајбер безбедност од ставот (3) на овој член, начинот на нивна реализација, висината на надоместокот согласно цената на ангажираните обучувачи, бројот на обучувачите и времетраењето на обуката, како и формата содржината на сертификатот за поминатата обука ги пропишува министерот.

Додатоци на плата

Член 40

(1) Заради специфичност на работните задачи и прилагодување на пазарот на труд додаток на плата во износ од 40 % од основната плата имаат следните вработени во институциите од членот 4 ставот (1) од овој закон:

1) вработените во организациската единица за сајбер безбедност во надлежниот орган од членот 12 ставот (1) од овој закон, со завршено високо образование од областа на ИКТ, телекомуникации, безбедност;

2) вработените во надлежните органи кои ги извршуваат надлежностите од членот 17 ставот (2) од овој закон, со завршено високо образование од областа на ИКТ, телекомуникации, безбедност;

3) вработените во тимовите за одговор на компјутерски инциденти од членот 20 ставот (1) од овој закон и

4) офицерите за сајбер безбедност од членот 25 ставот (1) од овој закон.

(2) Работните места во организациската единица за сајбер безбедност во надлежниот орган од членот 12 ставот (1) од овој закон, како и работните места за лицата од ставот (1) точките 2), 3) и 4) на овој член, во институции од јавен сектор може да бидат пополнети со лица со завршено високо образование од областа на областа на ИКТ, телекомуникации, безбедност или право, кои ги исполнуваат општите и посебните услови утврдени со актот за систематизација на работни места на надлежниот орган.

VII. СПРОВЕДУВАЊЕ НА ЗАКОНОТ

Надзор над спроведување на законот

Член 41

(1) Надзор над спроведувањето на овој закон врши министерството.

(2) Стручен надзор во однос на исполнувањето на обврските утврдени со овој закон вршат надлежните органи од членот 11 од овој закон, над суштинските и важните субјекти од нивна надлежност.

(3) Доколку стручниот надзор се врши заради решавање на инциденти кои за последица имаа повреда на личните податоци надлежните органи соработуваат со надлежното тело за заштита на личните податоци.

Овластено лице за вршење на стручен надзор

Член 42

(1) Стручниот надзор од членот 41 од овој закон, го вршат вработени во надлежниот орган со завршено високо образование од областа на ИКТ, телекомуникации, безбедност или право и кои ги исполнуваат општите и посебните услови утврдени со актот за систематизација на работните места на надлежниот орган или лица од Регистар на независни ревизори за сајбер безбедност кои се ангажирани и добиле овластување за конкретен стручен надзор, доколку надлежниот орган нема човечки капацитети за вршење на конкретниот надзор.

(2) Надлежниот орган на овластеното вработено лице му издава службена легитимација, која му служи за докажување на неговото службено својство и која е должен да ја покаже при вршењето на стручниот надзорот, а на независниот ревизор му издава писмено овластување за конкретниот надзор кое му служи за докажување на неговото својство.

(3) Овластеното лице за вршење на стручниот надзор е функционално независно во изрекување на мерките согласно одредбите од овој закон, без оглед дали се работи за субјект од приватен или од јавен сектор.

(4) Формата и содржината на службената легитимација од ставот (2) на овој член, и начинот на нејзиното издавање и одземање ги пропишува министерот.

(5) Потребните стручни квалификации и посебните компетенции на овластеното лице за стручен надзор ги пропишува министерот.

Вршење на надзор кај субјект на надзорот

Член 43

За вршење на стручниот надзор овластеното лице задолжително писмено го известува субјектот на надзорот најмалку три дена пред почетокот на надзорот. Во писменото известување овластеното лице е должно да даде образложение за причините за вршење на надзор.

Обврска на субјектот на надзорот во постапката на стручен надзор

Член 44

(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 стручен надзор да му обезбеди услови неопходни за непречена работа и за утврдување на фактичката состојба.

(3) Субјектот на надзорот е должен на овластеното лице кое врши стручен надзор да му овозможи во определениот рок утврден од овластеното лице, пристап до системите, услугите, информациските средства, просториите и документите што се предмет на надзорот.

Права на субјектот на надзорот во постапката на надзор

Член 45

(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 стручниот надзор 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 46

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

(2) Овластеното лице кое го врши стручниот надзор 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 стручниот надзор 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) Записниците од стручниот надзор се класифицирани информации согласно со закон.

(6) Формата и содржината на образецот на записникот за извршениот надзор ги пропишува министерот.

Решение

Член 47

(1) Во случај на повреда на одредбите на овој закон или друг пропис донесен врз основа на овој закон констатирана со записник овластеното лице е должно во рок од 15 дена од денот на достава на записникот 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

Член 48

(1) Решението по извршен стручен надзор е конечно и извршно.

(2) Против решението од ставот (1) на овој член, субјектот на надзорот може да поведе управен спор пред надлежен суд во рок од 30 дена од денот на приемот на решението.

Стручен надзор кај суштинските субјекти

Член 49

(1) Надзорот и мерките наметнати на суштинските субјекти во однос на обврските утврдени со овој закон, треба да се ефективни и пропорционални, а притоа, земајќи ги предвид околностите на секој поединечен случај.

(2) Во врска со надзорот од ставот (1) на овој член, надлежниот орган може:

1) да изврши стручен надзор преку овластено лице на лице место и стручен надзор надвор од локацијата на суштинскиот субјект, вклучувајќи случајни проверки;

2) да му наложат на суштинскиот субјект да спроведе безбедносни редовни ревизии и ревизии со конкретна цел извршени од независен ревизор со сајбер безбедносни квалификации;

3) да спроведува вонреден надзор, во случај кога тоа е оправдано, а поради настанат значителен инцидент или прекршување на овој закон од страна на суштинскиот субјект;

4) да спроведува анализи за безбедност врз основа на објективни, недискриминаторски, праведни и транспарентни критериуми за проценка на ризикот, доколку е тоа потребно, во соработка со суштинските субјекти;

5) да бара информации неопходни за проценка на мерките за управување со сајбер безбедносни ризици што се донесени од суштинскиот субјект, вклучително и донесени и усвоени политики за сајбер безбедност;

6) да бара да му се овозможи пристап до податоци, документи и информации неопходни за извршување на стручниот надзор;

7) да бара да му се достават докази за спроведување на донесените и усвоени политики за сајбер безбедност, како што се резултатите од безбедносните ревизии извршени од независен ревизор со сајбер безбедносни квалификации и други соодветни докази.

(3) Безбедносните ревизии со конкретна цел од став (2) точка 2 на овој член, треба да се извршат врз основа на проценки на ризик утврдени од надлежниот орган за суштинскиот субјект кој е предмет на ревизија или од други достапни информации поврзани со ризикот.

(4) Резултатите од која било безбедносната ревизија со конкретна цел треба да и бидат достапни на надлежниот орган. Трошоците за безбедносната ревизија со конкретна цел спроведена од независен ревизор со сајбер безбедносни квалификации ги плаќа суштинскиот субјект кој е предмет на ревизија, освен во соодветно оправдани случаи кога надлежниот орган ќе одлучи поинаку.

(5) По исклучок од став (4) на овој член, во случаи кога субјектот веќе бил предмет на сродна ревизија во претходните шест месеци, повторна ревизија може да се наложи само доколку трошоците за истата бидат покриени од страна на надлежниот орган.

(6) Суштинските субјекти се должни на писмено барање на надлежниот орган да му ги обезбедат информациите и податоците од ставот (2) точките 5), 6) и 7) на овој член, на ниво на деталност и во рок којшто од 20 дена од денот на приемот на барањето. Надлежниот орган е должен во барањето да ги наведе причините и целта за користење на побараните информации.

Мерки кај суштинските субјекти

Член 50

(1) Надлежниот орган врз основа на извршен стручен надзор има право на суштинскиот субјект со решение да му ги изрече следните мерки:

1) писмено да го предупреди за прекршување на одредбите на овој закон;

2) 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;

3) да донесе наредба со која се бара од суштинскиот субјект да ги отстрани идентификуваните недостатоци или да престане со однесувањето кое доведува до прекршување на овој закон, како и да се откаже од повторување на тоа однесување;

4) да му нареди на суштинскиот субјект да обезбеди дека неговите мерки за управување со сајбер безбедносен ризик се усогласени со членот 30 од овој закон, или да ги исполни обврските за пријавување утврдени во членот 31 од овој закон, на одреден начин и во одреден период;

5) да му наложи да ги информира физичките или правните лица на кои им обезбедува услуга, а на кои би можела да влијае значителниот сајбер безбедносен инцидент или значајна сајбер закана, за природата на заканата, како и за сите можни заштитни или корективни мерки кои би можеле да бидат преземени од негова страна како одговор на таа закана;

6) да му нареди на суштинскиот субјект во разумен рок да ги спроведе препораките што се резултат на безбедносната ревизија;

7) да побара од суштинскиот субјект да определи вработено лице со конкретно дефинирани задачи, кое ќе ја следи и надгледува усогласеноста на суштинскиот субјект со членовите 30 и 31 од овој закон;

8) да му наложи на суштинскиот субјект на одреден начин, да објави јавно достапни податоци за сторено прекршување на овој закон;

9) да поднесе барање за поведување прекршочна постапка пред надлежен суд.

(2) Кога мерките донесени во согласност со ставот (1) точките 1), 2), 3), 4) и 5) на овој член, нема да ги дадат очекуваните резултати, надлежниот орган ќе определи рок во кој суштинскиот субјект е должен да преземат мерки за отстранување на неправилноста или да ги исполнат барањата на надлежниот орган.

(3) Доколку суштинскиот субјект не постапи во согласност со ставот (2) на овој член:

1) ќе му се изрече прекршочна санкција привремена забрана за вршење одделна дејност;

2) на одговорното физичко лице или на правниот застапник на суштинскиот субјект, ќе му се изрече прекршочна санкција забрана за вршење на професија, дејност или должност.

(4) Доколку органите на државната управа, општините, градот Скопје и општините во градот Скопје, како и другите органи на централната власт опфатени со овој закон не постапат во согласност со ставот (2) на овој член, надлежниот орган за истото ќе ја извести Владата/Собранието, односно Министерството за локална самоуправа за општините, градот Скопје и општините во градот Скопје, во рок од 30 дена од денот кога органот го примил решението од членот 47 ставот (1) од овој закон.

(5) При изрекувањето на мерките од ставот (1) или ставот (3) на овој член, надлежниот орган треба да ја има во предвид сериозноста на повредата и важноста на прекршените одредби, при што за сериозна повреда, меѓу останатото, се смета следното:

1) повторување на повредата;

2) непријавување или несправување со значителни инциденти;

3) неотстранување на недостатокот во согласност со задолжителните упатства дадени од овластеното лице;

4) попречување на ревизијата што ја побарал надлежниот орган по утврдената повреда;

5) давање на лажни или особено неточни информации во врска со мерките за управување со безбедносните ризици или обврската за пријавување утврдена во членот 31 од овој закон;

6) времетраење на повредата;

7) сите релевантни претходни повреди сторени од суштинскиот субјект;

8) 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;

9) дали повредата е направена со намера или од небрежност;

10) сите мерки кои суштинскиот субјект ги презел со цел да ја спречи или ублажи материјалната или нематеријалната штета;

11) секое почитување на одобрените кодекси на однесување или одобрените механизми на сертификација и

12) нивото на соработка на одговорните физички или правни лица со надлежниот орган.

(6) Надлежниот орган е должен детално да ги образложи изречените мерки.

(7) Надлежниот орган пред изрекување на мерките, треба да го извести суштинскиот субјект 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) Надлежниот орган е должен 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.

Стручен надзор кај важни субјекти

Член 51

(1) Надлежниот орган, кон важниот субјект презема екс постнадзорни мерки врз основа на добиен доказ, индикација или информација дека важниот субјект не работи во согласност со овој закон. Преземените мерки треба да се ефективни и пропорционални, а при тоа треба да се имаат предвид околностите за секој поединечен случај.

(2) Надлежниот орган има право од важниот субјект да бара:

1) стручен надзор на лице место и екс постстручен надзор надвор од локацијата на важните субјекти,

2) безбедносни ревизии со конкретна цел кои ги спроведува независен ревизор со сајбер безбедносни квалификации;

3) безбедносни скенирања врз основа на објективни, недискриминаторски, праведни и транспарентни критериуми за проценка на ризик, а ако е потребно во соработка со важниот субјект;

4) достава на информации потребни за екс постоценување на мерките за управување со безбедносните ризици, донесени од страна на важниот субјект, вклучувајќи ги и донесените и усвоени безбедносни политики;

5) обезбедување пристап до податоци, документи и информации потребни за извршување на надзорот;

6) доставување докази за спроведената донесена и усвоена безбедносна политика, како што се резултатите од безбедносната ревизија што ја спровел независен ревизор со сајбер безбедносни квалификации други соодветни докази.

(3) Безбедносните ревизии со конкретна цел од ставот (2) точката 2) на овој член, се базираат на проценките за ризик кои ги утврдил надлежниот орган или важниот субјект или на други достапни информации поврзани со ризикот.

(4) Резултатите од секоја безбедносна ревизија со конкретна цел му се стават на располагање на надлежниот орган.

(5) Трошоците за безбедносната ревизија со конкретна цел која ја спроведува независен ревизор со сајбер безбедносни квалификации ги сноси важниот субјект над кого е спроведена ревизијата, освен во одредени оправдани случаи, кога надлежниот орган ќе одлучи поинаку.

(6) По исклучок од ставот (5) на овој член, во случаи кога субјектот веќе бил предмет на сродна ревизија во претходните шест месеци, повторна ревизија може да се наложи само доколку трошоците за истата бидат покриени од страна на надлежниот орган.

(7) Важниот субјект е должен на писмено барање на надлежниот орган да му ги обезбедат информациите и податоците од ставот (2) точките 4), 5) или 6) на овој член, на ниво на деталност и во рок од 20 дена од денот на приемот на барањето. Надлежниот орган е должен во барањето да ги наведе причините и целта за користење на побараните информации.

Мерки кај важните субјекти

Член 52

(1) Надлежниот орган, врз основа на извршен стручен надзор има право на важните субјекти со решение да им ги изрече следните мерки:

1) писмено да го предупреди за прекршување на одредбите на овој Закон;

2) да донесе задолжителни упатства или наредби со кои од важниот субјект ќе побара да ги отстрани утврдените недостатоци или прекршувања на овој закон;

3) да му нареди на важниот субјект да престане со постапувања со кои се прекршува овој закон и да не го повторува таквото постапување;

4) да му нареди на важниот субјект да обезбеди дека неговите мерки за управување со безбедносните ризици се во согласност со обврските утврдени во членот 30 на овој закон или да ја исполни обврската за пријавување утврдена во членот 31 на овој закон, на определен начин и во определен рок;

5) да му нареди на важниот субјект да ги извести физичките или правните лица на кои им обезбедува услуги, а на кои би можела да влијае значајната 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;

6) да му нареди на важниот субјект, во разумен рок да ги спроведе препораките дадени врз основа на извршената безбедносна ревизија;

7) да му нареди на важниот субјект на определен начин да ги објави аспектите на прекршувањето на овој закон;

8) да поднесе барање за поведување на прекршочна постапка пред надлежен суд.

(2) Кога мерките донесени во согласност со ставот (1) точките 1), 2), 3), 4) и 5) на овој член, нема да ги дадат очекуваните резултати, надлежниот орган ќе определи рок во кој важниот субјект е должен да преземат мерки за отстранување на неправилноста или да ги исполнат барањата на надлежниот орган.

(3) Доколку суштинскиот субјект не постапи во согласност со ставот (2) на овој член:

1) на суштинскиот субјект ќе му се изрече прекршочна санкција привремена забрана за вршење одделна дејност;

2) на одговорното физичко лице или на правниот застапник на суштинскиот субјект, ќе му се изрече прекршочна санкција забрана за вршење на професија, дејност или должност.

(4) Важниот субјект е должен да постапи по мерките од став (1) на овој член.

Лиценца за независни ревизори за сајбер безбедност

Член 53

(1) Безбедносните ревизии со конкретна цел од членот 49 став (2) точката 2) и членот 51 став (2) точката 2) од овој закон може да вршат:

1) физичко лице – независен ревизор кој ги исполнува условите за независен ревизор и кое се стекнало со лиценца од страна на Министерството,

2) правно лице регистрирано во согласност со одредбите од Законот за трговските друштва кое има вработено независен ревизор со лиценца и

3) високо-образовна установа, научна установа, стручна установа и орган на државна управа која има тим за одговор на компјутерски инциденти.

(2) Физичко лице може да добие лиценца за независен ревизор доколку ги исполнува следните услови:

1) да е државјанин на Република Северна Македонија,

2) да има живеалиште во Република Северна Македонија,

3) да има високо образование од областа на ИКТ (диплома за завршено четиригодишно високо образование или диплома со 240 кредити според европскиот систем за трансфер на кредити (ЕКТС) или меѓународен сертификат за информациска безбедност,

4) со правосилна одлука да не му е изречна забрана за вршење професија, дејност или должност се додека траат последиците од забраната,

5) да има најмалку пет години работно искуство по дипломирањето во соодветната област за која е поднесено барањето за полагање стручен испит и

6) да има завршено обука за безбедност на мрежни и информациски системи, организирана од Министерството во траење од најмалку 60 часа.

(3) По исклучок од ставот (2) точката 6) на овој член, доктори на наука од областа на ИКТ не е потребно да имаат завршено обука од за безбедност на мрежни и информациски системи, организирана од Министерството во траење од најмалку 60 часа за да се стекнат со лиценца за независен ревизор.

(4) Обуката за независни ревизори Министерството ја спроведува најмалку двапати годишно и истата не може да трае помалку од 60 часа, за истата кандидатите кои се пријавиле на обуката плаќаат надоместок, а приходите од надоместокот се приход на Буџетот на Република Северна Македонија..

(5) Министерството јавно објавува оглас за обука на кандидати за независни ревизори на нејзината веб-страница и во најмалку два дневни весника, од кои најмалку во по еден од весниците што се издаваат на македонски јазик и во весниците што се издаваат на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

(6) За завршена обука, Министерството му издава на кандидатот за независен ревизор уверение за завршена обука.

(7) Лицето коешто ја поминало обуката може да поднесе барање за издавање на лиценца за независен ревизор до Министерството кон која се приложува:

1) доказ за завршена обука и

2) доказ за платена административна такса.

(8) Министерството на лицето коешто ги исполнува условите од ставовите (2) и (3) на овој член, му издава лиценца за независен ревизор и го запишува во Регистарот на независни ревизори, кој го води електронски и кој е јавно достапен на веб-страницата на Министерството.

(9) Лиценцата за независен ревизор се одзема, ако:

1) независниот ревизор ја загуби деловната способност, со денот на правосилноста на решението за одземена деловна способност,

2) лиценцата е издадена врз основа на неточни податоци, од денот на дознавањето,

3) со правосилна одлука е изречена забрана за вршење на професија, дејност или должност, за времето додека траат правните последици од изречената забрана, со денот на правосилноста на одлуката,

4) е осуден со правосилна судска одлука за кривично дело на безусловна казна затвор над шест месеци, за времето додека траат правните последици од осудата, од денот на правосилност на одлуката,

5) е осуден со правосилна судска одлука за кривично дело давање лажен наод, од денот на правосилност на одлуката

6) независниот ревизор сам побара да му се одземе лиценцата или

7) настапи смрт на независниот ревизор

(10) Министерството во електронска форма води Регистар на субјектите од ставот (1) на овој член, кој е јавно достапен, а во кој ги запишува сите лица кои се стекнале со сертификат.

(11) Суштинските и важните субјекти од Регистарот од ставот (10) на овој член ангажираат независни ревизори за безбедносните ревизии со конкретна цел од член 49 став (2) точка 2) и член 51 став (2) точка 2) од овој закон, водејќи сметка да не постои судир на интереси и за изборот се должни да го известат надлежниот орган.

(12) Надлежните органи од Регистарот на независни ревизори за сајбер безбедност може да ангажираат и лица за вршење на стручен надзор од членот 41 од овој закон, водејќи сметка да не постои судир на интереси.

(13) Независните ревизори се должни стручно и професионално да ги извршуваат своите овластувања определени со овој закон и да избегнуваат каков било судир на интереси, согласно со Правилникот за однесување на независните ревизори за сајбер безбедност кој го пропишува министерот.

(14) Формата и содржината на образецот на лиценцата за вештачење, начинот на нејзиното издавање и одземање, начинот на спроведување на обуката, висината на надоместокот за обуката и формата и содржината на уверението за завршена обука ги пропишува министерот.

VIII. ПРЕКРШОЧНИ ОДРЕДБИ

Прекршоци

Член 54

(1) Глоба во износ до 2% од вкупниот годишен приход на суштинскиот субјект областите од членот 4 ставовите (2) и (3) од овој закон, остварен во претходната деловна година или од вкупниот приход остварен во тековната година, доколку во таа година започнал со работа, доколку со посебен закон не е пропишана повисока глоба ако:

1) не преземе соодветни и сразмерни технички, оперативни и организациски мерки за управување со ризиците согласно со членот 32 ставовите (1) и (3) од овој закон;

2) не го извести надлежниот тим за одговор на компјутерски инциденти, за секој значаен сајбер безбедносен инцидент што има влијание врз обезбедувањето на неговите услуги и не ги достави на надлежниот тим за одговор на компјутерски инциденти сите информации што ќе му овозможат да го утврди прекуграничното влијание на инцидентот, согласно со членот 33 ставовите (1) (4) од овој закон;

3) не ги извести корисниците на неговите услуги на кои може да влијае значајниот сајбер безбедносен инцидент за сите мерки или правни средства кои тие можат да ги преземат како одговор на инцидентот согласно со членот 33 ставот (2) од овој закон;

4) не постапи во согласност со членот 33 ставот (3) точките 1), 2) и 3) од овој закон;

5) не го извести тимот за одговор на компјутерски инциденти за значајниот сајбер безбедносен инцидент, согласно со членот 31 ставот (4) од овој закон;

6) не постапи по барањето на надлежниот тим за одговор на компјутерски инциденти, согласно со членот 33 ставот (5) од овој закон или

7) суштинскиот субјект во рокот определен од страна на надлежниот орган не преземе мерки за отстранување на неправилноста или не ги исполни барањата на надлежниот орган согласно со членот 50 ставот (2) од овој закон.

(2) Глоба во износ до 1,4% од вкупниот годишен приход на важниот субјект од областите од членот 4 ставовите (2) (3) од овој закон, остварен во претходната деловна година или од вкупниот приход остварен во тековната година, доколку во таа година започнал со работа ако:

1) не преземе соодветни и сразмерни технички, оперативни и организациски мерки за управување со ризиците согласно со членот 32 ставовите (1) и (3) од овој закон;

2) не го извести надлежниот тим за одговор на компјутерски инциденти, за секој значаен сајбер безбедносен инцидент што има влијание врз обезбедувањето на неговите услуги и не ги достави на надлежниот тим за одговор на компјутерски инциденти сите информации што ќе му овозможат да го утврди прекуграничното влијание на инцидентот, согласно со членот 33 ставовите (1) и (4) од овој закон;

3) не ги извести корисниците на неговите услуги на кои може да влијае значајниот сајбер безбедносен инцидент за сите мерки или правни средства кои тие можат да ги преземат како одговор на инцидентот согласно со членот 33 ставот (2) од овој закон;

4) не постапи во согласност со членот 33 став (3) точките 1), 2) и 3) од овој закон;

5) не го извести тимот за одговор на компјутерски инциденти за значајниот сајбер безбедносен инцидент, согласно со членот 33 став (4) од овој закон;

6) не постапи по барањето на надлежниот тим за одговор на компјутерски инциденти, согласно со членот 33 ставот (5) од овој закон или

7) суштинскиот субјект во рокот определен од страна на надлежниот орган не преземе мерки за отстранување на неправилноста или не ги исполни барањата на надлежниот орган согласно со членот 52 ставот (2) од овој закон.

(3) Глоба во износ од 5000 евра во денарска противвредност ќе се изрече на раководното лице на институциите од членот 4 ставот (1) од овој закон, за прекршоците од ставот (1) на овој член.

(4) Глоба во износ до 5000 евра во денарска противвредност ќе му се изрече и на одговорното лице во суштинскиот субјект, односно во важниот субјект за прекршоците од ставот (1) на овој член.

(5) Глоба во износ до 5000 евра во денарска противвредност ќе му се изрече за прекршоците од ставот (1) на овој член на функционерот кој раководи со орган на државната управа од централната власт, општините, Градот Скопје и општините во Градот Скопје, како и другите органи на централната власт.

Други прекршоци

Член 55

(1) Глоба во износ до 10.000 евра во денарска противвредност ќе му се изрече за прекршок на суштинскиот и важниот субјект од редот на субјектите од членот 4 ставовите (2) и (3) од овој закон ако:

1) до надлежниот орган не достават известување дека ги исполнуваат условите за клучен субјект, односно важен субјект согласно со членот 8 ставот (5) од овој закон;

2) не ги достави до Министерството податоците од членот 9 ставот (3) од овој закон;

3) не достави до Министерството измена на податоците согласно членот 9 ставот (4) од овој закон;

4) не ја воспостави базата на податоци за регистрација на имиња на домени согласно членот 10 ставот (1) од овој закон;

5) не воспостават политики и постапки, вклучително и постапки за проверка, со што се обезбедува дека базата на податоци за регистрација на имиња на домени согласно членот 10 ставот (3) од овој закон.

6) јавно не ги објават податоците за регистрација, притоа водејќи сметка за заштитата на личните податоци согласно со членот 10 ставот (4) од овој закон;

7) не обезбедат пристап до одредени податоци за регистрацијата на имиња на домени согласно со членот 10 ставот (5) од овој закон;

8) не ги преземе сите неопходни, соодветни и пропорционални корективни мерки согласно со членот 32 ставот (7) од овој закон;

9) не го извести надлежниот орган за неговото учество во механизмите за споделување на информации за сајбер безбедност согласно со членот 37 ставот (4) од овој закон;

10) не овозможи непречено вршење на стручниот надзор согласно со членот 42 од овој закон;

11) не му ги даде на располагање на надлежниот орган резултатите од која било безбедносна ревизија со конкретна цел, согласно со членовите 49 ставот (4), односно членот 51 став (4) од овој закон или

12) на писмено барање на надлежниот орган не ги обезбеди информациите и податоците согласно членот 49 ставот (6), односно членот 51 ставот (6) од овој закон.

(2) Глоба во износ од 5000 евра во денарска противвредност ќе му се изрече на раководното лице на институциите од членот 4 ставот (1) од овој закон, за прекршоците од ставот (1) на овој член.

(3) Глоба во износ до 5000 евра во денарска противвредност ќе му се изрече и на одговорното лице суштинските субјекти и важните субјекти за прекршоците од ставот (1) на овој член.

(4) Глоба во износ до 5000 евра во денарска противвредност ќе му се изрече за прекршоците од ставот (1) на овој член на функционерот кој раководи со орган на државната управа од централната власт, општините, градот Скопје и општините во градот Скопје, како и другите органи на централната власт.

(5) Глоба во износ до 10.000 евра во денарска противвредност ќе му се изрече за прекршок на Единствениот регистар на врвни домени и давателите на услуги за регистрација на имиња доколку не воспостават политики и постапки за регистрација, вклучително и постапки за верификација, за да се осигурат дека базите на податоци согласно со членот 10 ставот (3) од овој закон.

Прекршочни санкции

Член 56

(1) На суштинскиот субјект за сторените прекршоци од членот 54 ставот (1) од овој закон, покрај глобата ќе му се изрече и прекршочна санкција забрана на вршење на определена дејност.

(2) Прекршочната санкција од ставот (1) на овој член не може да биде изречена за период пократок од три месеци ниту подолг од две години, од денот на правосилноста на одлуката.

(3) На одговорното лице на суштинскиот субјект за сторените прекршоци од членот 54 ставот (1) од овој закон, 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.

Надлежен орган за прекршочна постапка

Член 57

За прекршоците од членовите 54 и 55 од овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

IX. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 58

(1) Подзаконските акти кои произлегуваат од овој закон ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон.

(2) Владата на предлог на Министерството ги утврдува деталните листи од членот 7 став (1) од овој закон, во рок од дванаесет месеци од денот на влегувањето во сила на овој закон.

Член 59

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

Член 60

(1) Тимот за одговор на компјутерски инциденти за органите на извршната власт од членот 21 став (1) точката 1) од овој закон, ќе започне со работа во рок од 12 месеци од денот на влегувањето во сила на овој закон.

(2) Мрежата на тимови за одговор на компјутерски инциденти од член 22 став (1) на овој член, ќе се воспостави во рок од 12 месеци од денот на влегувањето во сила на овој закон.

Член 61

(1) Одредбите од членот 37 ставот (5) од овој закон, ќе отпочне да се применува со денот на пристапувањето на Република Северна Македонија во ЕУ.

(2) За субјектите од областите од членот 4 став (2) точки 8), 9), 10), 11), 12), 13), 14), 15) и 16) од овој закон, одредбите од овој закон ќе започнат да се применуваат со денот на пристапувањето на Република Северна Македонија во ЕУ.

Член 62

Овој закон влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“, а ќе започне да се применува од 1 јануари 2026 година.