

д-р ОЛИВЕР БАКРЕСКИ

д-р АЛЕКСАНДРА
ДЕАНОСКА-ТРЕНДАФИЛОВА

КОМЕНТАР НА ЗАКОНОТ ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

д-р ОЛИВЕР БАКРЕСКИ
д-р АЛЕКСАНДРА ДЕАНОСКА-ТРЕНДАФИЛОВА

“

КОМЕНТАР НА
ЗАКОНОТ ЗА КЛАСИФИЦИРАНИ
ИНФОРМАЦИИ

”

Скопје, 2021 година

КОМЕНТАР НА ЗАКОНОТ ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Автори:

д-р Оливер Бакрески

д-р Александра Деаноска-Трендафилова



Издавач:

©DCAF, 2021

All rights reserved

DCAF – Geneva Center for Security Sector Governance

Chemin Eugène-Rigot 2E, CH-1202 Geneva, Switzerland

©ДЦАФ, 2021

Сите права се задржани

ДЦАФ – Центар за управување со безбедносниот сектор – Женева

– Подружница Скопје

ул. Македонија бр. 11-1/2, 1000 Скопје, Република Северна Македонија

За ДЦАФ

ДЦАФ – Женевскиот центар за управување со безбедносниот сектор е посветен на подобрување на безбедноста на државите и нивниот народ во рамките на демократско управување, владеење на правото, почитување на човековите права и родова еднаквост. Од основањето во 2000 година, ДЦАФ придонесе за поодржлив мир и развој помагајќи им на државите партнери и меѓународните актери кои ги поддржуваат овие држави, да го подобрат управувањето со нивниот безбедносен сектор преку инклузивни и партиципативни реформи. Создава иновативни производи на знаење, промовира норми и добри практики, дава правни и политички совети и поддржува градење на капацитети на засегнатите страни од државниот и недржавниот безбедносен сектор.

Советот за основање на ДЦАФ е составен од претставници на околу 60 земји-членки и на Кантонот Женева. Активен во над 80 земји, ДЦАФ е меѓународно признат како еден од водечките светски центри за извонредност за управување со безбедносниот сектор (SSG) и реформи во безбедносниот сектор (SSR). DCAF се води според принципите на неутралност, непристрасност, локална сопственост, инклузивно учество и родова еднаквост. За повеќе информации посетете ја страницата www.dcaf.ch и следете нè на Твитер [@DCAF_Geneva](https://twitter.com/DCAF_Geneva).

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix

Chemin Eugène-Rigot 2E

CH-1202 Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

 Twitter [@DCAF_Geneva](https://twitter.com/DCAF_Geneva)



Kingdom of the Netherlands



Sweden
Sverige



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Swiss Agency for Development and Cooperation SDC

СОДРЖИНА

ПРЕДГОВОР.	4
ГЛАВА ПРВА	7
ОПШТИ ОДРЕДБИ.	7
Значење на изразите употребени во овој закон	11
ГЛАВА ВТОРА	17
КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ И СТЕПЕНИ НА КЛАСИФИКАЦИЈА	17
Класифицирани информации на странски држави и меѓународни организации	29
ГЛАВА ТРЕТА	31
КРИТЕРИУМИ, МЕРКИ И АКТИВНОСТИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ	31
Административна безбедност	32
Физичка безбедност	34
Безбедност на лица-корисници на класифицирани информации	36
Безбедност на комуникациско-информациски системи	37
Индустриска безбедност	40
Размена на класифицирани информации со странски држави и меѓународни организации	42
Користење на класифицирани информации	44
Постапки за издавање на безбедносни сертификати	49
Времетраење на безбедносните сертификати	57
ГЛАВА ЧЕТВРТА	66
ОРГАНИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ	66
Офицер за безбедност на класифицирани информации	66
Дирекција за безбедност на класифицирани информации	70
Регистри и контролни точки	73
ГЛАВА ПЕТТА	79
ПЛАНОВИ И ПРОГРАМИ ЗА РАБОТЕЊЕ НА ДИРЕКЦИЈАТА И ФИНАНСИРАЊЕ НА ДИРЕКЦИЈАТА.	79
ГЛАВА ШЕСТА	81
НАДЗОР	81
ГЛАВА СЕДМА	97
ПРЕКРШОЧНИ ОДРЕДБИ	97
Постапка за порамнување со издавање на прекршочен платен налог	101
ГЛАВА ОСМА	103
КАЗНЕНИ ОДРЕДБИ	103
Оддавање на класифицирани информации со степен „СТРОГО ДОВЕРЛИВО“ и „ДОВЕРЛИВО“	103
Неовластено откривање на класифицирана информација употребена во судска или друга постапка	105
ГЛАВА ДЕВЕТТА	107
ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ	107

ПРЕДГОВОР

Со воспоставувањето на законската и институционалната рамка за заштита на класифицираните информации во Република Северна Македонија, се зајакна постојниот систем за заштита на информациите од интерес за државата и се воспостави цврста основа за кредибилна соработка со меѓународните организации и странски држави во однос на прашања од чувствителен карактер поврзани со безбедноста. Регулативата за заштита на класифицираните информации е донесена со цел да се воспостави позитивна практика за заштита на националните безбедносни интереси, да се спречи нанесување штета на политиката на национална безбедност и на интересите на државата, јасно да се дефинира поделбата на надлежностите и одговорностите, да се исклучи можната злоупотреба во извршувањето на работните задачи и должности, да се овозможи ефикасна контрола и систем за санкционирање, како и за да се осигура добивање на потребниот кредибилитет во работата и во работењето.

Законската регулатива на Република Северна Македонија за заштита на класифицирани информации е во согласност со стандардите на НАТО и на ЕУ. Нејзината имплементација, како и добрите резултати од работата на Дирекцијата за безбедност на класифицирани информации, како единствен орган за спроведување на утврдената национална политика и на меѓународните стандарди за заштита на класифицираните информации и за реализирање на размената на класифицираните информации согласно воспоставените процедури, придонесуваат за подигање на степенот на безбедноста и заштитата на класифицираните информации и за унапредување на безбедносната култура кај вработените во државната администрација кои работат со такви информации. Ова го потврдува и фактот што при подготовките на Република Северна Македонија за членство во НАТО големо значење се придаваше на унапредувањето на размената на класифицирани информации како на една од привилегираните видови соработка со меѓународните организации и странски држави. Безбедноста на класифицираните информации исто така е едно од клучните прашања од Поглавјето 31 – Надворешна безбедносна и одбранбена политика (НБОП) во рамките на Националната програма за усвојување на правото на Европската Унија (НПАА).

Законот за класифицирани информации за прв пат беше донесен во март 2004 година, а потоа во согласност со потребите согледани преку неговата непосредна примена во областа која ја уредува или поради усогласување со други закони чии одредби е потребно да се имплементираат во законскиот текст, беше менуван и дополнуван неколку пати („Службен весник на Република Македонија“ број 09/04, 113/07, 145/10, 80/12, 41/14, 21/18 и 83/18). Во текот на имплементацијата на Законот беше утврдена потребата за воведување законски решенија за усогласување со постојната регулатива во други области (пр. вршењето инспекциски надзор), за регулирање на прашања што претходно не биле опфатени во регулативата (пр. користењето на класифицираните информации во судска или друга постапка), како и за воведување законска основа за донесување подзаконски акт којшто ја регулира криптозаштитата во земјата. Воедно, во согласност со интеграциските процеси на земјата во НАТО и во ЕУ, беше согледана и потреба за попрецизно утврдување на надлежностите на Дирекцијата за безбедност на класифицирани информации во доменот на размената и заштитата на класифицирани информации со меѓународните организации.

Во функција на соодветно имплементирање на прифатените меѓународни стандарди за безбедност на класифицираните информации, во текот на 2018 година во Дирекцијата за безбедност на класифицирани информации беше направена компаративна анализа на законските решенија на 12 земји членки на НАТО и на ЕУ со коишто дотогаш Владата на Република Македонија имаше потпишано билатерални спогодби за размена и заемна заштита на класифицирани информации. Врз основа на резултатите од направената анализа, од разменетите искуства со сродните служби на земјите од регионот со коишто Дирекцијата има развиено блиска соработка, како и врз основа на стекнатите искуства од научените лекции од примената на Законот од неговото донесување во 2004 година, во 2018 година беше покрената иницијатива за изработка на нов текст на закон за класифицирани информации.

Новиот Закон за класифицирани информации(*) во којшто е транспонирана Одлуката на Советот од 23 септември 2013 година во однос на правилата за безбедност за заштита на класифицирани информации на ЕУ, CELEX број 32013D0488, беше донесен кон крајот на декември 2019 година („Службен весник на Република Северна Македонија“ број 275/19), а истиот влезе во сила на 3 јануари 2020 година.

Со Законот се уредува системот за заштита на класифицирани информации во Република Северна Македонија, при што се става акцент на класифицирањето на информациите, определувањето на степените на класификација, критериумите, мерките и активностите за заштита на класифицираните информации, размената на класифицираните информации со странски држави и меѓународни организации, постапките за издавање и времетраењето на безбедносните сертификати, органите за заштита на класифицирани информации,

плановите и програмите за работење на Дирекцијата, вршењето надзор, прекршочните и казнените одредби при неовластено откривање на класифицирани информации, како и други прашања поврзани со системот за заштита на класифицирани информации.

Намерата за подетално објаснување на новините воведени со овој закон, како и желбата истиот правилно да се толкува во смисла на неговите основни идеи и вредносни определби ја нагласија потребата за изработка на коментар на Законот. Во него, покрај толкувањето на одредбите со коишто се регулираат некои од позначајните новини во Законот, должно внимание ќе се стави и на прашањата коишто укажуваат на потребата од нивно дополнително уредување со цел да не предизвикаат недоразбирања и дилеми при примената на Законот. Токму од таа причина, иако овој коментар се изработува непосредно по донесување на Законот, намерата е со оваа прва верзија да се поттикне дополнителна дискусија којашто надолната со практичните искуства од примената на Законот, несомнено ќе го унапреди квалитетот на некое следно издание. Коментарот е првенствено наменет за корисниците на класифицирани информации, но текстот, секако, ќе биде корисно четиво и за сите други лица коишто допрва ќе се обучуваат за работа со класифицирани информации, за вработените во безбедносниот сектор, како и за студентите по право и безбедност и за научните работници.

Како автори сакаме да се благодариме на поддршката на Женевскиот центар за управување со безбедносниот сектор (ДЦАФ) кој ја помогна реализацијата на овој проект, како и на сите добронамерни читатели и корисници на коментарот коишто со својата конструктивна критика на текстот на коментарот ќе придонесат во процесот на стручна анализа на одредбите содржани во Законот за класифицирани информации(*).

Авторите
Скопје, март 2021 година

ЗАКОН ЗА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ(*)¹

ГЛАВА ПРВА

ОПШТИ ОДРЕДБИ

Член 1

Со овој закон се уредуваат класификацијата на информациите, условите, критериумите, мерките и активностите што се преземаат за нивна заштита и безбедност, правата, обврските и одговорноста на создавачите и корисниците на класифицирани информации, национална и меѓународната размена, инспекцискиот надзор над спроведувањето на овој закон, како и други прашања во врска со пристапот и ракувањето со класифицирани информации.

Во рамките на првиот член начелно се уредени прашањата кои се предмет на регулирање на Законот (ratione materiae). Очигледно, овој член експлицитно ја дефинира основната цел, содржината и прашањата според кои се уредени критериумите, мерките и активностите што се преземаат за заштита и безбедност на информациите, правата, обврските и одговорноста на создавачите и корисниците на класифицирани информации, националната и меѓународната размена, инспекцискиот надзор над спроведувањето на овој закон, како и други прашања во врска со пристапот и ракувањето со класифицирани информации. Меѓутоа, содржината на овој член во голема мера зависи од правото во поширока смисла, односно од другите закони со кои се уредуваат бројни прашања поврзани со статусно-правната положба на сите физички и правни лица. Значи, прашањата кои се уредени со овој закон ја детерминираат статусно-правната положба и каузалноста на сите односи кои се јавуваат во целиот процес на спроведување на мерките и активностите до крајните реципиенти на класифицирани информации кои изрично се наброени во овој член. Јасната потреба од размена на информации е нагласена експлицитно од национално до меѓународно ниво и обратно каде очигледно е израз на јасна доминација на ваквите концепти во сите современи национални законодавства, но и во меѓународните акти кои се однесуваат на оваа материја.

Член 2

Обврска за заштита на класифицираните информации согласно со овој закон имаат сите корисници на класифицирани информации што имале пристап и/или биле запознаени со нивната содржина.

¹ Во Законот се транспонираат одредбите од Одлуката на Советот од 23 септември 2013 година во однос на правилата за безбедност за заштита на класифицирани информации на ЕУ (CELEX 32013D0488), па од таа причина истиот е означен во согласност со Одлуката за востановување на ознака на прописите на Европската Унија во подзаконските прописи со кои се врши усогласување со правото на Европската Унија („Службен весник на Република Македонија“ број 38/10).

Законот определува обврска, односно должност сите корисници на класифицирани информации што имале пристап и/или биле запознаени со нивната содржина да ја штитат содржината на информацијата. Обврската за заштита повлекува и одговорност на едно лице во ситуација кога не се почитуваат пропишаните правила или ако тоа не ги извршува или несовесно ги заштитува информациите и ако дозволи намерно или ненамерно други субјекти да бидат запознаени со содржината на информацијата која има генерална обврска да ја штити. Имајќи лапидарна природа, одредбата од членот 2 е од суштинско значење бидејќи тежината и значењето на обврската е неопходна претпоставка за совесно однесување на споменатите лица.

Обврската за заштита на класифицираните информации има особено значење во рамките на класичниот пристап во кој преовладуваат елементи на професионален однос и висок степен на безбедносна култура, што значи дека заштитата треба да се гледа низ призмата на когнитивните процеси кои пак, во основа имплицираат знаење, сознанија за безбедноста, за заштитата, за значењето на информациите итн. Тоа се вредносни судови за сензитивноста на работата и на работењето со информации кои главно вклучуваат и комбинации на вредности, стандарди и критериуми.

За да се намали потенцијална инсуфициентност на одговорно однесување, при што е нагласена заштитата на информациите, важен е самиот пристап кон овој проблем кој имплицира сложен процес внатре во самата институција/институциите и физичките лица и каква е безбедносната ориентација на корисниците која има бројни димензии кои влијаат на политичко-безбедносните процеси. Единствената релевантна интерпретација подразбира уредена демократско-безбедносна средина во која има изградена хиерархиска структура. Тука, безбедносната култура имплицира почитување на поредокот, на државата, на институцијата, на вредностите, на интересите итн. Значи, тука споменатите амбиваленции неминовно се одразуваат и на самите поединци, општествените групи и особено на општествените елити, со што се влијае на оформување на нивниот пристап и самата имплементација на тој пристап во безбедносната практика. Оттука, само општествено активен однос кон оваа проблематика ќе придонесе кон афирмација и развој на основните постулати во кои безбедносниот аспект ќе го направи неопходниот чекор да доведе до акумулација на безбедносно-културниот капитал од индивидуата до самото општество.

Фактот што обврската за заштита на класифицираните информации како што е наведено во членот 2 ја имаат сите корисници на класифицирани информации што имале пристап и/или биле запознаени со нивната содржина повлекува одговорност и е релевантно и од казнено-правен аспект, односно повлекува казнено-правна одговорност за лица и правни субјекти кои ќе направат противправно дејствие на злоупотреба и неовластено (од)давање информации и следствено, тие може да бидат одговорни за стореното дејствие со што ќе овозможат со содржината на информацијата да бидат запознаени лица кои вообичаено не треба да дојдат во допир со такви информации.

Член 3

Целта на овој закон е обезбедување на законито користење на класифицирани информации и оневозможување на секаков вид незаконит или неовластен пристап, злоупотреба и компромитирање на информациите.

Во членот 3 експлицитно е определена целта на Законот која е во насока на обезбедување законито користење на класифицираните информации и

оневозможување, спречување на секаков вид незаконит или неовластен пристап, злоупотреба и компромитирање на информациите. Целта, меѓу другото, го опишува своевидниот императив во работењето на сите правни субјекти кои имаат допирни точки и овластувања во сферата на класифицираните информации, а истите се и предизвик и обврска за сите што работат и се приврзани со институцијата која е најповикана да го раководи целиот процес и да ја обезбеди целокупната заштита на информациите, зашто може да се идентификуваат со нејзината цел и причина за постоење.

Целта која е поставена во овој закон се дефинира како одредена специфична состојба, ситуација или резултат, но постојат и механизми според кои се мери нејзиното остварување. Вака поставената цел ја дава целисходноста која треба да ја оневозможи незаконитоста, неовластениот пристап, злоупотребата и компромитираноста, што значи дека треба да се обезбеди единствен пристап во обезбедувањето, а тоа бара организациска коегзистентност.

Постигнувањето на целта значи и партиципативно учество и придонес, но и идеја како да се поттикне креативноста што во основа ќе значи иновативност, решителност, како и преземање на акција за да се овозможат промените во безбедносна смисла на зборот. Излегувањето од строгите законски рамки и услови за постапување ќе значи незаконска, неовластена примена и злоупотреба на информациите, а во некои случаи може да доведе дури и до најсериозни последици, јавни скандали и слично, што ја наметнува потребата од сериозно санкционирање на лицата сторители на незаконските дејствија. Потребно е обврските, овластувањата и функциите на одговорните тела да бидат јасно дефинирани така што ќе може работата на различните нивоа на хиерархија успешно да се надгледува и да се оценува.

Член 4

Одредбите од овој закон се применуваат на националните класифицирани информации и на класифицираните информации примени од странски држави и меѓународни организации или создадени во меѓусебна соработка, доколку со меѓународните договори ратификувани согласно со Уставот на Република Северна Македонија (во натамошниот текст: ратификуваните меѓународни договори), поинаку не е уредено.

Смислата на член 4 е определување на опсегот, односно границата до каде се протега примената на одредбите на овој закон, па, како што е наведено во член 4, одредбите не се ограничени само на националните класифицирани информации, туку и пошироко, односно и на класифицираните информации кои се примени од странски држави и меѓународни организации, како и на класифицирани информации создадени во меѓусебна соработка доколку тоа не е поинаку уредено со меѓународните договори ратификувани согласно со Уставот на Република Северна Македонија, имајќи го предвид фактот дека ратификуваните меѓународни договори стануваат дел од домашното позитивно право.

Вака поставената основа ја дава широката рамка на опфат за соработка и размена на класифицирани информации. Ова прецизирање на примената на одредбите во смисла на имплицитна забрана во поинакви ситуации ја дава рамката на примена и субјектите кои непосредно соработуваат и разменуваат

класифицирани информации во насока на обезбедување на превентивната функција заради спречување на можна злоупотреба.

Член 5

За заштитата на класифицираните информации и примената на меѓународните стандарди, за реализирање на размената на класифицирани информации согласно со ратификуваните меѓународни договори, за вршење инспекциски надзор на спроведувањето на одредбите од овој закон и другите прописи од областа на класифицираните информации, како и за вршење на други работи утврдени со овој закон, е надлежна Дирекцијата за безбедност на класифицирани информации (во натамошниот текст: Дирекција).

Во член 5 е востановена основната надлежност на Дирекцијата за безбедност на класифицирани информации, односно е апострофирано правото и обврската (од кои произлегуваат понатаму и ингеренциите) на Дирекцијата за безбедност на класифицирани информации во насока на заштита на класифицираните информации. Имено, заради специфичноста на материјата и големата важност, пред сè од безбедносен аспект, се предвидува постоење на посебна институција која ќе поддржи и одржи сеопфатен систем на заштита на информациите (што подразбира примена и на динамичен и специфичен пристап на работење кој треба да е во корелација со добро осмислена политика и стратегија која ќе овозможи севкупното дејствување и работење да е засновано на професионално, етичко, легитимно и искуствено знаење и премиси). На тоа се надоврзува и потребата од јасна синергија и дијалектика за ефикасно имплементирање на принципите на работа неопходни за успешно извршување на специфичните задачи. Особено, од раководните структури во Дирекцијата за безбедност на класифицирани информации се бара внимателно и безусловно да создадат клима за прифаќање и организирање на работните задачи навремено и на сите хиерархиски нивоа.

Во таа смисла, со цел да се обезбеди заштита на класифицираните информации и примена на меѓународните стандарди, како и за реализирање на размената на класифицирани информации согласно со ратификуваните меѓународни договори, за вршење инспекциски надзор над спроведувањето на одредбите од овој закон и другите прописи од областа на класифицираните информации, како и за вршење на други работи утврдени со овој закон, се востановува, како што наведовме погоре, надлежност на Дирекцијата. Подготвеноста за операционализација на конкретните задачи за да се обезбеди потребната заштита на информациите чија тајност треба да биде обезбедена, всушност, во најголема мера развиси од работата на Дирекцијата.

Од аспект на остварување на заштитата на класифицираните информации, Дирекцијата за безбедност на класифицирани информации мора да има доволно моќ и авторитет за да ја врши својата работа, но не во толкава мера што би се наметнала над системот или би останала надвор од секаква контрола. Оттука, нормалниот одговор на оваа дилема потенцира три аспирации: легитимност, професионализам и одговорност. Оттука, главните цели се насочени кон постојана легитимност, постојан професионализам и постојана одговорност. Сите три услови мора кумулативно да бидат исполнети за да говориме за постоење на демократско управување. Професионалното однесување и одговорноста ја поткрепуваат легитимноста, додека одговорноста ја овозможува професионалноста, а самата

легитимност го овозможува потребниот степен на професионална самостојност на Дирекцијата.

ЗНАЧЕЊЕ НА ИЗРАЗИТЕ УПОТРЕБЕНИ ВО ОВОЈ ЗАКОН

Член 6

Одделни изрази употребени во овој закон го имаат следново значење:²

1. „Информација“ е сознание кое може да биде пренесено во која било форма;³

2. „Информација од интерес за Република Северна Македонија“ е секоја информација изготвена од орган на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје, физичко или правно лице, како и од странски државен орган, односно странско физичко или правно лице, која се однесува на безбедноста и одбраната на државата, нејзиниот територијален интегритет и суверенитет, уставниот поредок, јавниот интерес и слободите и правата на човекот и граѓанинот;

3. „Класифицирана информација“ е информација од делокругот на работа на орган на државната и локалната власт основан во согласност со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или други правни лица којашто се однесува на јавната безбедност, одбраната, надворешните работи или безбедносни или разузнавачки активности на државата која во согласност со закон мора да се заштити од неовластен пристап и е обележана со соодветен степен на класификација во согласност со овој закон. Класифицирани информации може да претставуваат и документи, технички средства, машини, опрема, односно одвоени компоненти или оружје или алати што се произведени или се во процес на производство, како и доверливите пронајдоци што се однесуваат на одбраната и се од интерес на безбедноста на државата;

4. „Документ“ е секој пишан текст, нацрт или скица, репродукција, копија, фотографија, аудио, видео, магнетски, електронски, оптички или друг вид запис, во кој се содржани информации;⁴

5. „Штета“ е повреда на интересите на државата како последица од загрозување на безбедноста на класифицираните информации од интерес за Република Северна Македонија или информациите кои Република Северна Македонија е обврзана да ги заштитува во согласност со ратификуваните меѓународни договори;

6. „Безбедносен ризик“ е можност за нарушување на безбедноста на класифицираната информација;

7. „Безбедност на класифицирана информација“ е збир на активности и мерки со кои се обезбедува заштитата на класифицираните информации од неовластен пристап и неовластено ракување;

² За дефинирање на изразите од овој член се користени одредбите од следните документи: Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-COR1-12, GLOSSARY, February 2013, *Amdt. no 9* и Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Journal of the European Union L274/1).

³ Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-COR1-12, GLOSSARY, February 2013, *Amdt. no 9*, стр. 3.

⁴ Исто.

8. „Безбедносен сертификат за физичко лице“ е документ со кој се потврдува дека за физичкото лице не постои безбедносен ризик за пристап и ракување со класифицирани информации;

9. „Безбедносен сертификат за правно лице“ е документ со кој се потврдува дека за правното лице не постои безбедносен ризик и дека поседува физички или организациски капацитети за ракување со класифицирани информации и/или за чување на класифицирани информации, во согласност со закон;

10. „Дозвола за пристап до класифицирани информации“ е документ со кој се потврдува дека странското физичко или правно лице има безбедносен сертификат издаден во матичната држава и има право на пристап и користење на класифицирани информации во Република Северна Македонија;

11. „Потребно е да знае“ е принцип според кој се утврдува корисникот кој има потреба за пристап до класифицирани информации заради извршување на функцијата или на службената должност и службените овластувања, на дејноста или за спроведување на класифицирани договори;⁵

12. „Создавач на класифицирана информација“ е овластен изработувач на класифицирана информација. Создавачи на класифицирани информации се органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други физички или правни лица, што создаваат информации од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата;

13. „Дисеминација на класифицирани информации“ претставува распоредување на класифицирани информации согласно со принципот „потребно е да знае“ до лица кои поседуваат соодветен безбедносен сертификат;

14. „Корисник на класифицирана информација“ е физичко или правно лице кое има потреба за пристап до класифицирани информации заради извршување на функцијата, службената должност и службените овластувања или за спроведување на класифицирани договори и кое има безбедносен сертификат, соодветен на класификацијата на информацијата.

15. „Ракување со класифицирани информации“ е процес кој го опфаќа секое постапување со класифицираните информации во времетраење на нивното постоење. Тоа подразбира нивно создавање, евиденција, пренос, користење, распоредување, рекласификација, декласификација, архивирање и уништување.

16. „Безбедносен појас“ е простор околу објектот којшто претставува минимална оддалеченост од објектот од која можат да бидат загрозувани објектот и класифицираните информации во него;

17. „Безбедносна зона“ е простор или просторија во објектот во кој се ракува и во кој се чуваат класифицирани информации до степенот „ДРЖАВНА ТАЈНА“ и има потреба од соодветна физичка заштита;

18. „Административна зона“ е јасно определен заштитен простор што се воспоставува околу или пред безбедносните зони во коишто постојат можности за контрола на лица и возила.⁶

19. „Класифициран договор“ е секој облик на договор или договор кој

⁵ Исто, стр. 6.

⁶ Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Journal of the European Union L274/1), Annex II, PHYSICAL SECURITY, IV. Physically Protected Areas, точка 12.

произлегува од него, вклучувајќи ги и преговорите за склучување на истиот, којшто содржи или овозможува пристап до класифицирани информации;

20. „Офицер за безбедност на класифицирани информации“ е лице овластено од одговорното лице во органот на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или во правното лице кое има должност да се грижи за ефикасно и координирано извршување на правата и обврските кои произлегуваат од овој закон;

21. „Криптографска безбедност“ е компонентата на безбедноста на комуникациско-информациските системи која ја опфаќа криптографската заштита, управувањето со криптографските материјали и развојот на методи на криптографска заштита, кои се спроведуваат преку шифра, код и дигитален потпис;

22. „Криптографска заштита“ е оперативно-планска активност во системот на криптографски материјали и производи кои се користат за заштита на класифицирани информации од неовластен пристап при изработка, ракување и чување на класифицираните информации;

23. „Криптографски производ“ е софтвер, систем или уред со кој се врши криптографска заштита;

24. „Криптографски материјали (криптоматеријали)“ се криптографски алгоритми, криптографски хардверски и софтверски модули, криптоклучеви, насоките за нивна имплементација и придружната документација;⁷

25. „Безбедносна акредитација на комуникациско-информациски системи“ е процес на формално одобрување на комуникациско-информациски системи за работа до одредениот степен на класификација, во посебни безбедносни услови во неговото оперативно опкружување и на прифатливо ниво на безбедносен ризик;

26. „Процес на управување со безбедносен ризик“ е процес на идентификација, контролирање, минимизирање или елиминирање на настани што можат да влијаат врз безбедноста на една организација или на системот што таа го користи;⁸

27. „Комуникациско-информациски систем (КИС)“ е секој систем што овозможува создавање, чување, обработка, или пренос на информациите во електронска форма. Комуникациско-информацискиот систем ги вклучува сите средства потребни за негово функционирање, како инфраструктурата, организацијата, персоналот и информациските, комуникациските и други електронски ресурси.

Членот 6 од Законот претставува поимник, односно содржи дефиниции на поими кои го сочинуваат категоријалниот систем востановен во Законот за класифицирани информации(*).

Постоењето поимник, односно посебен член за „значење на изразите“ употребено во Законот е втемелена практика на законодавецот на почетокот од законскиот текст, во делот на општите одредби да ги дефинира основните термини, концепти и изрази од кои зависи правилната примена на Законот. Со тоа ќе се

⁷ Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-COR13, GLOSSARY, February 2013, *Amdt. no 9*, стр. 2; Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Journal of the European Union L274/1), Appendix A, Definitions

⁸ Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Journal of the European Union L274/1), Appendix A, Definitions

спречи во практиката да се јават различни, прешироки или воопшто неправилни толкувања; всушност, во ваквите случаи самиот законодавец, кој е најповикан во таа насока, го дава потребното толкување, па во правната литература ова претставува еден од облиците на законско, односно автентично толкување или толкување преку т.н. легални дефиниции.⁹ Во конкретниов случај, како што е нагласено, станува збор за терминологските дивергенции околу поимите кои се во директна корелација со законската материја и очигледно се во функција на појаснување на основните категории и поими со што директно ќе се придонесе за оформување на целосната слика за да се избегнат недоумици во спроведувањето на Законот. Оваа одредба е, навистина, повеќе од потребна ако се земе предвид законот кој регулира една исклучително специфична и сензитивна област.

Во поимникот на Законот за класифицирани информации(*) се дефинирани поимиповрзани со информацијата и класифицираните информации, безбедносната терминологија, субјектите кои создаваат, користат и ракуваат со информациите, безбедносната зона, термини поврзани со безбедноста на комуникациско-информациските системи итн. Значи, определени се многу термини и поими со кои понатаму оперира Законот и кои се исклучително важни за поимно разбирање на целокупната реалност определена во законскиот текст.

Практичната примена допрва ќе покаже (со оглед на фактот што овој закон е донесен на самиот крај на 2019 година) дали законодавецот пропуштил да дефинира уште некој поим кој во практиката ќе се појави како нужен.

Централните поими во овој закон, како што се: информација, информација од интерес за Република Северна Македонија и класифицирана информација, се први на листата од 27-те поими. Првата дефиниција дава претстава и теоретско објаснување за поимот информација како сознание во која било форма.

Во алинеа 4 и алинеа 5 на член 6 се дефинирани документот како форма на пишан текст, нацрт или скица, репродукција итн., во кој се содржани информации; и штетата која е повреда на интересите на државата како последица од загрозување на безбедноста на класифицираните информации од интерес за Република Северна Македонија или информациите кои Република Северна Македонија е обврзана да ги заштитува во согласност со ратификуваните меѓународни договори.

Во наредните алинеи се расчленува безбедноста низ призмата на безбедносен ризик и безбедност на класифицирани информации. Генерално, променетата природа на безбедносните ризици ја услови потребата за редефинирање на безбедноста, но наметна и усвојување на нови пристапи за безбедноста. Прифаќајќи ја ваквата реалност државите мора да се приспособат на новите околности заради заштита на националните интереси и заради гарантирање на оптималното ниво на безбедност. Адаптирањето на безбедносните ризици го изразува и високото ниво за безбедност на класифицирани информации што е збир на активности и мерки со кои се обезбедува заштитата на класифицираните информации од неовластен пристап и неовластено ракување. Ова бара генерална сеопфатна инклузија на сите субјекти што се вклучени и ја остваруваат заштитната компонента.

Во алинеите 8 и 9 кои се однесуваат на безбедносниот сертификат како документ кој потврдува дека кај физичкото или правното лице не постои ризик за пристап и ракување со класифицирани информации се прецизира дека безбедносен сертификат за физички лица, всушност, во смисла на Законот, значи издавање на документ дека физичкото лице ги исполнува условите да пристапува и ракува со класифицирани информации, додека безбедносниот сертификат за правни лица е многу прецизен во аргументацијата, односно станува збор за

⁹ Камбовски Владо, Казнено право - општ дел, Скопје, 2011, стр. 114.

правно лице кое поседува физички и организациски капацитети за ракување и/или чување на класифицирани информации. Тоа значи дека не постои ризик (закани по информациите) и нема опасност од уништување, противправно дејствување, злоупотреба и други форми на штетни дејствија.

Во алинеја 10 децидно, преку дозволата за пристап до класифицирани информации, се потврдува дека странското физичко или правно лице има безбедносен сертификат издаден во матичната држава и се определува дека има право на пристап и користење на класифицирани информации во Република Северна Македонија. Дозволата има далекусежни импликации за вршењето на дејноста, односно немањето соодветна дозвола ќе го оневозможи физичкото и правното лице да користи класифицирани информации во земјава. Доколку странското физичко или правно лице има потреба да користи класифицирани информации на Република Северна Македонија, мора за тоа да обезбеди дозвола.

Во алинеја 11 наведен е принципот „потребно е да знае“ според кој се утврдува корисникот кој има потреба за пристап до класифицирани информации заради извршување на функцијата или на службената должност и службените овластувања, на дејноста или за спроведување на класифицирани договори. Примената на овој принцип („need to know“) е исклучително важна во делот на давањето пристап до класифицирани информации од причина што поседувањето безбедносен сертификат или високиот ранг, чин или функција на лицето не подразбира директен пристап до одредени класифицирани информации.¹⁰

Во алинеја 12 се дефинира создавачот на класифицирана информација кој е овластен изработувач на класифицирана информација. Како создавачи на класифицирани информации опфатени се органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други физички или правни лица, што создаваат информации од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата. Секоја друга информација која не е создадена од создавачот на информацијата во смисла на Законот нема правна втемеленост и веродостојност и во никој случај не може да добие степен на класификација.

Во наредните алинеи се дефинира дисеминацијата, корисникот и процесот на ракување со класифицирани информации, односно распоредување на класифицираните информации до лица кои поседуваат соодветен безбедносен сертификат и постапување со класифицираните информации за времетраење на нивното постоење.

Во алинеите 16, 17 и 18 се дефинирани соодветните зони кои пропишуваат минимална оддалеченост дефинирана како безбедносен појас, просторот или просторијата во објектот во кој се ракува и се чуваат класифицираните информации определен како безбедносна зона и заштитниот простор определен како административна зона кој треба да се воспостави околу и пред безбедносните зони.

Алинеја 19 прецизира што значи „класифициран договор“, при што се подразбира дека за да се смета овој правен однос за правно валиден треба да е создаден во писмена форма и да ги исполнува сите други карактеристики предвидени со други одредби од други релевантни акти во поглед на тоа како се склучува истиот меѓу договорните страни, доколку содржи во себе или овозможува пристап до

¹⁰ Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "C", 20 November 2020, стр. C-1, точка 4.

класифицирани информации, но посебно се нагласува и тоа дека покрај договорот, може да се класифицираат и самите преговори за склучување на истиот, бидејќи и од нив може да се дојде со сознанија поврзани со класифицирани информации.

Алинеја 20 го детерминира значењето на тоа што е офицер за безбедност на класифицирани информации како лице кое има должност да се грижи за ефикасно и координирано извршување на правата и обврските кои произлегуваат од Законот и е лице овластено од одговорното лице во органот на државната власт, правно лице или друг субјект од релевантниот делокруг на субјекти определени со Законот. Алинеите 21, 22, 23 и 24 ги дефинираат поимите „криптографска безбедност“ која е компонента на комуникациско-информациските системи, што значи „криптографска заштита“ како оперативно-планска активност, потоа криптографскиот производ и криптографските материјали кои се криптографски алгоритми, криптографски хардверски и софтверски модули, крипто клучеви, насоките за нивна имплементација и придружната документација.

Алинејата 25 го објаснува поимот „безбедносна акредитација на комуникациско-информациски системи“ и законодавецот притоа објаснува дека тоа е процес на формално одобрување на комуникациско-информациски системи за работа до одредениот степен на класификација, во посебни безбедносни услови во неговото оперативно опкружување и на прифатливо ниво на безбедносен ризик; а алинеа 26 го објаснува процесот на управување со безбедносен ризик со детерминирачките елементи.

Во последната, алинеја 27 е објаснет поимот „комуникациско-информациски систем“ кој е особено важен од аспект на тоа што овозможува создавање, чување, обработка или пренос на информациите во електронска форма.

ГЛАВА ВТОРА

КЛАСИФИЦИРАЊЕ НА ИНФОРМАЦИИ И СТЕПЕНИ НА КЛАСИФИКАЦИЈА

Член 7

Со класификација на информацијата се определува степенот на заштита на информацијата кој треба да биде соодветен со степенот на штетата што би настанала за Република Северна Македонија со неовластен пристап или неовластена употреба на информацијата.

Информациите кои се предмет на класификација се однесуваат особено на: јавната безбедност; одбраната; надворешните работи; безбедносни, разузнавачки и контраразузнавачки активности на државата; системи, уреди, пронајдоци, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања и технолошки, економски и финансиски работи од значење за Република Северна Македонија.

Со член 7 е пропишано дека класификацијата на информацијата се врши со определување одреден степен на класификација и притоа е уредено дека истиот треба да биде соодветен со степенот на штетата што би настанала за Република Северна Македонија во случај кога некое лице неовластено би пристапило или неовластено би ја употребило таа информација. Значи, постои сразмерност меѓу степенот на класификација и потенцијалната штета која би настанала со нејзино некласифицирање.

Во вториот став на членот е уредено дека степен на класификација се определува за информациите коишто се однесуваат на јавната безбедност; одбраната; надворешните работи; безбедносни, разузнавачки и контраразузнавачки активности на државата; системи, уреди, пронајдоци, проекти и планови од важност за јавната безбедност, одбраната, надворешните работи; научни истражувања и технолошки, економски и финансиски работи од значење за Република Северна Македонија.

Во контекст на состојбите поврзани со глобалната здравствена пандемија со COVID-19 вирусот, се поставува прашањето за опсегот на поимот безбедност и кои сè аспекти треба тој да покрие, се поставува прашањето и за потребата за заштита на информациите коишто се однесуваат или имаат влијание на јавното здравје на населението. Во една поширока дискусија за тоа дали таквите информации треба да имаат степен на безбедносна класификација, односно дали можат да се сметаат за информации што се однесуваат на јавната безбедност, треба да се земе предвид поширокиот контекст на поимот безбедност којшто во себе го содржи и концептот за хумана или индивидуална безбедност којашто, едноставно кажано, се фокусира на безбедноста и благосостојбата на луѓето. Хуманата безбедност препознава

повеќе закани за безбедноста, меѓу кои се и заканите за здравствената безбедност на луѓето, вклучувајќи различни инфективни и паразитски болести, здравствени и социјални проблеми предизвикани од недостаток на чиста вода и загадување на воздухот, непостоење соодветна здравствена заштита и слично. Следствено на тоа, би можело да се препознае безбедносниот карактер на информациите коишто се однесуваат на здравјето и на здравствената заштита на населението и како такви да подлежат на соодветна заштита.

Во Законот за управување со кризи,¹¹ ризиците што ги загрозуваат здравјето и животот на луѓето се ставени во корелација со поимот „загрозеност на безбедноста на Републиката“.

Воедно, Националната концепција за безбедност и одбрана од 2003 година¹², во којашто се дефинирани интересите на државата, во виталните интереси со кои се унапредува безбедносната состојба и со кои се создаваат услови за подобар живот на граѓаните и функционирање на државата и општеството, меѓу другите ги вбројува и интересите за „заштита и унапредување на мирот и безбедноста, животот, здравјето, имотот и личната безбедност на граѓаните на Република Македонија“.

Следствено на ова, во контекст на глобална здравствена пандемија што може да доведе до нарушување на внатрешните состојби во државата и на нејзините односи на меѓународен план, ако притоа се земе предвид дека степенот на загрозувањето и нанесувањето штета на виталните интереси на државата влијае на одредувањето на степенот на класификација на информациите, законодавецот треба да го препознае безбедносниот карактер на информациите поврзани со здравствената заштита на луѓето и да ја уреди нивната заштита.

Член 8

Класификацијата на информациите се врши според нивната содржина.

Степенот на класификација на информацијата го определува создавачот на информацијата, а со негово писмено овластување и друго лице.

Информацијата се означува со еден од степените на класификација:

- ▶ ДРЖАВНА ТАЈНА,
- ▶ СТРОГО ДОВЕРЛИВО,
- ▶ ДОВЕРЛИВО и
- ▶ ИНТЕРНО.

Во членот 8 е уредено дека класификацијата на информациите се врши според нивната содржина и дека создавачот го определува степенот на класификација, а со негово писмено овластување, и друго лице. Тоа е општоприфатено правило во безбедносните политики за ракување со класифицирани информации на НАТО и на ЕУ, како и во безбедносните политики на нивните земји-членки, односно во националните безбедносни политики. Во овој член се утврдени и степените на класификација: ДРЖАВНА ТАЈНА, СТРОГО ДОВЕРЛИВО, ДОВЕРЛИВО и ИНТЕРНО.

¹¹ Закон за управување со кризи, „Службен весник на Република Македонија“ број 29/05, член 3, став 1, точка 1.

¹² Национална концепција за безбедност и одбрана, „Службен весник на Република Македонија“ број 5/03, поглавје I. Интереси на Република Македонија, точка 7 став 2 алинеја 1.

Со донесување на Законот за класифицирани информации во 2004 година беше направен значаен чекор напред од аспект на усогласување на степените на класификација со меѓународно прифатените степени на класификација и укинување на дотогаш постојните видови класификација.

Новиот Закон за класифицирани информации(*) го следи тоа решение, но останува да се усогласи казнено-правната заштита и евентуално решенија во други закони заради конзистентност. Имено, инкриминирано е оддавањето на државна тајна во член 317 од Кривичниот законик, но другите степени на класификација не се опфатени, додека постојат инкриминации за заштита на воена тајна и слично, што е одраз на поранешни решенија во моментов непоткрепени со основа во позитивното законодавство.¹³

Член 9

Класифицираната информација со степен „ДРЖАВНА ТАЈНА“ е информација чие неовластено откривање би предизвикало загрозување и нанесување непоправливи штети на трајните интереси на Република Северна Македонија.

Класифицираната информација со степен „СТРОГО ДОВЕРЛИВО“ е информација чие неовластено откривање би предизвикало исклучително сериозна штета за виталните интереси на Република Северна Македонија.

Класифицираната информација со степен „ДОВЕРЛИВО“ е информација чие неовластено откривање би предизвикало сериозна штета за важните интереси на Република Северна Македонија.

Класифицираната информација со степен „ИНТЕРНО“ е информација чие неовластено откривање би предизвикало штета за работењето на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, кои се од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата.

Во членот 9 поблиску се уредени степените на класификација во согласност со тежината на последиците од неовластеното откривање на содржината на информациите со секој одделен степен на класификација. Притоа, интересите на Република Северна Македонија коишто би биле загрозени со неовластеното откривање на класифицираните информации се усогласени со интересите што се дефинирани во Националната концепција за безбедност и одбрана.¹⁴

Притоа е уредено дека степенот „ДРЖАВНА ТАЈНА“ се доделува на информација чие неовластено откривање би предизвикало загрозување и нанесување непоправливи штети на трајните интереси на Република Северна Македонија; степенот „СТРОГО ДОВЕРЛИВО“ се доделува на информација чие неовластено откривање би предизвикало исклучително сериозна штета за виталните интереси на Република Северна Македонија, а степенот „ДОВЕРЛИВО“ се доделува на

¹³ В. Кривичен законик, Службен весник на Република Македонија број 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 97/17 и 248/18, членови 281, 349 и 360.

¹⁴ Национална концепција за безбедност и одбрана, „Службен весник на Република Македонија“ број 42/01 и 5/03, поглавје I. Интереси на Република Македонија, точка 7.

информација чие неовластено откривање би предизвикало сериозна штета за важните интереси на Република Северна Македонија.

Воедно е уредено дека најнискиот степен на класификација „ИНТЕРНО“ се доделува на информација чие неовластено откривање би предизвикало штета за работењето на органите на државната и локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, кои се од значење за јавната безбедност, одбраната, надворешните работи и безбедносните и разузнавачките активности на државата.

Член 10

При класифицирањето на информацијата, создавачот, односно лицето овластено од него, треба да ја означи класифицираната информација со најсоодветниот степен на класификација со кој се обезбедува потребната заштита на државните интереси и безбедноста од членот 9 од овој закон.

Определувањето на соодветниот степен на класификација на информацијата се врши врз основа на проценка за можната штета и последиците кои би произлегле од неовластениот пристап до неа.

Во член 10 законодавецот ја уредил обврската на создавачот на информацијата, односно на лицето овластено од него, да ја означи класифицираната информација со најсоодветниот степен на класификација со кој ќе се обезбеди потребната заштита на државните интереси и безбедноста дефинирани во членот 9. Притоа укажал дека определувањето на соодветниот степен на класификација на информацијата се врши врз основа на процената за можната штета и последиците кои би произлегле од неовластениот пристап до неа.

Целта на одредбите од овој член е да се намали тенденцијата на прекумерна класификација на информациите којашто потоа резултира со сериозни обврски за корисниците на класифицираните информации во смисла на ракувањето и чувањето на истите. Истовремено, тоа значи и давање поголема тежина на процесот на точна проценка на можните штети што ќе резултира со најправилен избор на степен на класификација.

Ова решение е воведено со новиот закон како резултат на сознанијата од направените анализи и стекнатите искуства од применетите практики за ракување со класифицирани информации во Република Северна Македонија кои укажуваа дека создавачите на класифицирани информации заради поголема сигурност или од недоволна упатеност честопати доделуваат поголем степен на класификација на информациите или, во ретки случаи, дури непотребно класифицираат информации. Со цел да им помогне на корисниците на класифицирани информации во одредувањето на соодветен степен на класификација на информациите, Дирекцијата за безбедност на класифицирани информации изработи Водич за одредување на степенот на класификација на информациите.¹⁵

¹⁵ Водич за одредување на степенот на класификација на информациите (достапно на: https://www.dbki.gov.mk/files/pdf_files/Vodic_zao_dreduvanje_stepen_na_Kl.pdf).

Член 11

Класифицирана информација со степен „ДРЖАВНА ТАЈНА“ определуваат: претседателот на Република Северна Македонија, претседателот на Собранието на Република Северна Македонија, претседателот на Владата на Република Северна Македонија, претседателот на Уставниот суд на Република Северна Македонија, претседателот на Врховниот суд на Република Северна Македонија, министрите во рамките на своите ресори, јавниот обвинител на Република Северна Македонија, началникот на Генералштабот на Армијата на Република Северна Македонија, директорот на Агенцијата за разузнавање, директорот на Агенцијата за национална безбедност, директорот на Оперативно-техничката агенција, директорот на Центарот за управување со кризи, директорот на Дирекцијата за безбедност на класифицирани информации, како и лица овластени од страна на горенаведените субјекти.

Ако така е определено со закон, ратификуван меѓународен договор или друг пропис, класифицирана информација со степен „ДРЖАВНА ТАЈНА“ определуваат и лицата предвидени во тие акти.

Во членот 11 се утврдени субјектите коишто, во согласност со Законот се овластени да класифицираат информации со највисокиот степен – „ДРЖАВНА ТАЈНА“. Притоа, таксативно се наведени носителите на највисоките јавни функции во државата, односно претседателот на Република Северна Македонија, претседателот на Собранието на Република Северна Македонија, претседателот на Владата на Република Северна Македонија, претседателот на Уставниот суд на Република Северна Македонија, претседателот на Врховниот суд на Република Северна Македонија, министрите во рамките на своите ресори, јавниот обвинител на Република Северна Македонија и началникот на Генералштабот на Армијата на Република Северна Македонија, како и директорите на државните органи коишто имаат надлежности во доменот на безбедноста и заштитата на државата, односно директорот на Агенцијата за разузнавање, директорот на Агенцијата за национална безбедност, директорот на Оперативно-техничката агенција, директорот на Центарот за управување со кризи и директорот на Дирекцијата за безбедност на класифицирани информации.

Оваа одредба предвидува степен „ДРЖАВНА ТАЈНА“ да можат да определуваат и други лица коишто се овластени од страна на горенаведените субјекти.

Вториот став на овој член остава можност класифицирана информација со степен „ДРЖАВНА ТАЈНА“ да определуваат и лица коишто за тоа изрично се определени со закон, ратификуван меѓународен договор или друг пропис.

Се поставува прашањето дали можноста што законодавецот ја стипулирал и со друг пропис да се определат лица кои ќе определуваат класифицирани информации со степен „ДРЖАВНА ТАЈНА“ е добро решение, бидејќи тоа всушност би значело и со подзаконски акти кои многу полесно се носат (не поминуваат ни процедура за донесување закони) и почесто и полесно потенцијално се менуваат, да се прошири делокругот на лица кои би ги класифицирале информациите со највисокиот степен на класификација.

Законодавецот не ги определил субјектите коишто се овластени да класифицираат информации со степен „СТРОГО ДОВЕРЛИВО“ и „ДОВЕРЛИВО“, но во согласност со позитивните прописи за организација и работа на органите на државната управа се подразбира дека тоа е одговорното лице во субјектот или од него овластено лице за потпишување акти, решавање определени прашања или

вршење други работи од надлежност на органот.¹⁶

Член 12

Информациите со чие откривање би се намалила ефикасноста на работењето на органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, добиваат ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“.

Ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“ не претставува степен на класификација, но до ваквите информации не е дозволен слободен пристап.

Начинот на чување и ракување со информациите за ограничена употреба со уредба поблиску ги уредува Владата на Република Северна Македонија.

Со членот 12 се дефинира доделувањето на ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“ на информациите со чие откривање би се намалила ефикасноста на работењето на органите на државната и на локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје. Како што е уредено со вториот став на овој член, ознаката не претставува степен на класификација, но го ограничува јавниот пристап до таквите информации.

Имено, ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“ се доделува на информациите коишто се користат за службени цели и иако не наметнува потреба од строги мерки за ракување и чување на таквите информации, сепак укажува на потребна заштита од нивно објавување во јавноста. Имено, со ова јасно се делимитираат ваквите информации од оние до кои што може да биде дозволен слободен пристап.¹⁷

Во безбедносната политика на НАТО таквите информации се означени како UNCLASSIFIED, а во ЕУ такви се информациите со ознака LIMITE. Притоа, во безбедносните политики и на НАТО и на ЕУ се нагласува дека ознаките не претставуваат степен на класификација туку ознака за распределување на информациите којашто подразбира ракување со таквите информации од страна на лица во рамките на организацијата за службени цели.

Заради специфичниот карактер на информациите со ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“ во третиот став на овој член е предвидено Владата на Република Северна Македонија со уредба поблиску да ги уреди начинот на чување и ракување со таквите информации.

Член 13

Ако во една информација се опфатени податоци за повеќе степени на класификација, создавачот е должен да го определи степенот на класификација на секој од нив посебно.

Целината на информацијата се класифицира според највисокиот степен на класификација, а на насловната страна на материјалот се означуваат другите

¹⁶ Закон за организација и работа на органите на државната управа, „Службен весник на Република Македонија“ број 58/00, 44/02, 82/08, 167/10, 51/11 и „Службен весник на Република Северна Македонија“ број 96/19, 110/19, член 47 и член 52.

¹⁷ За тоа кои информации може да се сметаат за информации до кои е дозволен слободен пристап, в. Закон за слободен пристап до информации од јавен карактер, „Службен весник на Република Северна Македонија“, број 101/19.

делови со степени на класификација коишто припаѓаат кон информацијата.

Ако дел од документот содржи класифицирана информација со повисок степен на класификација, тој дел може да се издвои како посебен документ со соодветен степен на класификација.

Фуснотите нема да бидат класифицирани освен ако содржат или откриваат класифицирани информации.

Заради избегнување на безбедносен ризик употребата на фусноти треба да се сведе на минимум.

Во членот 13 е уреден начинот на класификација на една информација која што е составена од делови коишто носат различен степен на класификација.

Одредбите од членот укажуваат на должноста на создавачот да го определи степенот на класификација на секој дел од информацијата посебно – одделно, а целината на информацијата да ја класифицира според највисокиот степен на класификација. Притоа, покрај највисокиот степен со којшто ја класифицира информацијата, создавачот е должен на насловната страна на материјалот да ги означи другите делови со степени на класификација коишто припаѓаат кон информацијата. Со тоа ќе биде јасно за идните ракувачи со класифицираната информација, зависно од највисокиот степен, како се постапува со целата информација, а и дека нејзината содржина е различна во поглед на класификацијата.

Во третиот став на овој член е утврдена можноста дел од документот којшто содржи класифицирана информација со повисок степен на класификација да може да се издвои како посебен документ со соодветен степен на класификација. Имено, доколку е потребно да се применат строги мерки за заштита само за еден дел од класифицираната информација, со неговото издвојување во посебен документ се овозможува полесно ракување со преостанатите делови од класифицираната информација коишто воопшто немаат или имаат понизок степен на класификација.

Во практиката, при работа со националните класифицирани информации ретко се случува издвојувањето на делови од класифицирана информација како посебен документ, но тоа е вообичаена практика при работа со класифицирани информации на НАТО.¹⁸

Во овој член е уредена и употребата на фусноти, при што се посочува дека тие по правило не треба да бидат класифицирани освен ако содржат или откриваат класифицирани информации, а заради избегнување на безбедносен ризик, одредбата од петтиот став на овој член укажува дека нивната употреба треба да се сведе на минимум.

Заради фактот дека фуснотите претставуваат референци, односно секогаш се поврзани со основниот текст, практично е тешко да се изведе целата заштита во практика доколку текстот е класифициран, а самата фуснота кон него не е, или ако хипотетички има различни степени на класификација на текстот од фуснотата. Оттука, прагматична е насоката дадена во последниот став на овој член за избегнување на употребата на фусноти во класифицираните информации.

Член 14

¹⁸ Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "E", 20 November 2020, стр. E-2, точка 12.

Создавачот на класифицираната информација задолжително го означува на видно место степенот на нејзината класификација, согласно со овој закон.

Во членот 14 законодавецот ја предвидел обврската на создавачот на класифицираната информација степенот на нејзината класификација задолжително да го означи на видно место. Тоа е важно од аспект на побрза и полесна забележливост на фактот дека се работи за класифицирана информација и за тоа за кој степен се работи, со што би се превенирале случаите на небрежен пристап.

Означувањето на класифицираната информација подетално е уредено во подзаконски акт во којшто се пропишани мерките од доменот на административната безбедност на класифицираните информации.

Член 15

Ако информацијата не била означена со степен на класификација, а создавачот не може да се утврди или престанал да постои, класифицирањето на информацијата го врши правниот следбеник на создавачот.

Ако не може да се утврди ниту правниот следбеник од ставот 1 на овој член, означувањето на степенот на класифицираната информација го врши Дирекцијата.

Во случај кога информацијата не била означена со степен на класификација, а создавачот не може да се утврди или престанал да постои, законодавецот во членот 15 предвидел дека класифицирањето на информацијата го врши правниот следбеник на создавачот, а доколку не може да се утврди ниту правниот следбеник, законодавецот утврдил дека означувањето на степенот на класифицираната информација го врши Дирекцијата за безбедност на класифицирани информации.

Основата за оправданоста на ваквото решение на законодавецот лежи во членот 5 од Општите одредби во којшто Дирекцијата е препознаена како надлежен орган за спроведување на безбедносната политика во однос на заштитата на класифицираните информации и извршување работи уредени со овој закон, а целта е секогаш кога има потреба да се класифицира одредена информација да постои решение за тоа кој ќе биде овластен субјект во случај на неможност за утврдување или во случај на актуелно непостоење на создавачот на информацијата.

Законодавецот тука не ја предвидел улогата на Дирекцијата во случај кога е потребно да се рекласифицира или да се декласифицира класифицирана информација чијшто создавач не може да се утврди или престанал да постои.

Член 16

Со рекласификација се врши промена на степенот на класификацијата на информацијата.

Промена на степенот на класификација врши создавачот, а со негово писмено овластување и друго лице.

За промената на степенот на класификација на информацијата задолжително се известуваат корисниците на информацијата.

Начинот на промена на степенот на класификација на информацијата со уредба поблиску го уредува Владата на Република Северна Македонија.

Во членот 16 всушност се дефинира поимот рекласификација и е уредена постапката за рекласификација, односно промената на степенот на класификацијата на информацијата, којашто ја врши создавачот на информацијата или од него овластено лице. Притоа, законодавецот не укажува прецизно во која насока треба да се одвива промената, односно дека промената на степенот на класификацијата на информацијата треба да оди од повисок кон понизок степен на класификација, што всушност е намерата со постапката за рекласификација. Не е логично информација што е означена со понизок степен на класификација, и како таква била достапна на одреден круг на корисници, дополнително да се заштитува со повисок степен на класификација, а со тоа и со дополнителни мерки за заштита и ограничувања во пристапот.

Во третиот став од членот е утврдена обврската за промената да се известат сите корисници на класифицираната информација. Ваквата обврска е дадена со цел да се обезбеди соодветна заштита на класифицираната информација, особено ако е подигнат степенот на заштита, но исто така и да се избегне употребата на поголеми ресурси од потребното за таа цел или воопшто, доколку е даден понизок степен на класификација.

Одредбата од четвртиот став на овој член предвидува Владата на Република Северна Македонија со уредба поблиску да го уреди начинот на промена на степенот на класификација на информацијата, со што се дава можност за подетално уредување на постапката и операционализација на оваа одредба и процедура во подзаконски акт. Начинот на промена на степенот на класификација на информацијата е предмет на уредување во подзаконскиот акт во којшто се пропишани мерките од доменот на административната безбедност на класифицираните информации.

Член 17

Класификацијата на информацијата престанува:

- на датумот означен на документот,
- со случување на определен настан наведен во документот,
- со истекување на временскиот период означен на документот и
- со декласификација.

Во членот 17 законодавецот ги утврдува начините на кои може да престане, односно да заврши класификацијата на една информација, па утврдува дека класификацијата на информацијата престанува на датумот што е означен на документот, со случување на настанот на којшто се однесува документот, со истекување на временскиот период означен на документот и со декласификација.

Всушност, тоа се неколкуте начини на кои престанува класификацијата, а не кумулативно поставени услови кои треба да се исполнат за престанок на класификацијата. Имено, кај определени информации може да се наведе точен датум кога класификацијата ќе престане, но кај други тоа не е можно затоа што се врзани со настан за кој не може однапред да се знае кога ќе се случи, кај трети ќе се определи временски период, а кај некои ќе се изврши декласификација.

Со уредување на престанокот на класификацијата на информацијата се дава можност истата да стане достапна на јавноста заради тоа што не постои повеќе опасност да биде загрозен или повреден определен интерес на државата,

а дополнително со тоа да се заштедат ресурси што би биле наменети за нејзина натамошна заштита. Достапноста за јавноста подразбира особено достапност на информацијата за научни цели, за истражувања и анализи.

Член 18

Со декласификација се врши промена од класифицирана информација во информација која е некласифицирана.

Декласификацијата од ставот 1 на овој член ја врши создавачот на информацијата или од него овластено лице, за што задолжително ги известува корисниците на информацијата.

Начинот на декласификација на информацијата со уредба поблиску го уредува Владата на Република Северна Македонија.

Во членот 18 е уредена постапката за декласификација на класифицираната информација со која што истата станува некласифицирана. Тоа е всушност еден од повеќето начини на кои класификацијата на една информација престанува.

По правило, промена на степенот на класифицираната информација може да направи создавачот или од него овластено лице, па следствено на тоа законодавецот уредува дека и самата декласификација ја врши создавачот на информацијата или од него овластено лице. Како и во случај на постапката за рекласификација на класифицираната информација, одредбата од вториот став на овој член предвидува корисниците задолжително да бидат известени за декласифицираната информација. Со цел подетално уредување на постапката за декласификација, во третиот став на овој член е уредено Владата на Република Северна Македонија со уредба поблиску да го уреди начинот на декласификација на информацијата. Ова е предмет на уредување во подзаконскиот акт во којшто се пропишани мерките од доменот на административната безбедност на класифицираните информации.

Практиката покажува дека постапката за декласификација не се спроведува често, но познати се искуства од работата со класифицирани информации во НАТО, каде што постои посебен Комитет преку којшто се спроведува декласификацијата на класифицираните информации на НАТО.¹⁹

За потребите на судските постапки (поточно кривичната постапка), кај нас често се декласифицираат доказите кои се обезбедени со употреба на посебни истражни мерки (ПИМ) а кои претходно, по правило, се класифицираат. Со ова *de facto* тие стануваат некласифицирани информации, па заради спречување на слободен пристап, односно ограничување на пристапот до нив се случува да им се додели ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“. Сепак, оваа ознака не е степен на класификација. Сметаме дека се потребни дополнителни дискусии и обуки во овој домен на сите релевантни субјекти, затоа што тука легитимно се поставуваат неколку прашања: прво, дали оваа ознака, на пример, сама по себе е доволен основ за исклучување на јавноста и, второ, дали има потреба од декласификација на сите претходно класифицирани информации во овие случаи (кривични постапки), кога законот предвидува тие да може да се користат како класифицирани со исклучување на јавноста?

За ова, правосудните органи, но и создавачите на класифицирани информации за потребите на кривичната правда, особено треба да ги имаат предвид одредбите

¹⁹ ARCHIVES COMMITTEE, Directive on the Public Disclosure of NATO Information, AC/324-D(2014)0010-REV2, 16 January 2018

од членовите 63 и 104 од Законот за класифицирани информации(*) и член 354 од Законот за кривичната постапка.

Член 19

Создавачот на класифицираната информација означува временски период или настан по кој информацијата може да биде рекласифицирана или декласифицирана.

Временскиот период или настанот по кој класифицираната информација може да биде рекласифицирана или декласифицирана не може да надминат период од десет години, освен во случај кога на класифицираната информација ѝ е потребна подолготрајна заштита утврдена со закон.

Во членот 19 акцентот е ставен на обврската на создавачот на класифицираната информација да го означи временскиот период или настан по кој информацијата може да биде рекласифицирана или декласифицирана, при што утврдува дека истите не можат да надминат период од десет години, освен во случај кога на класифицираната информација ѝ е потребна подолготрајна заштита утврдена со закон.

Целта на оваа одредба е да се даде насока на создавачите на класифицирани информации за потребата од преиспитување на нивната одлука и определување на временски максимум за претходнонаведеното.

Член 20

Класифицираната информација со степенот „ДРЖАВНА ТАЈНА“ создавачот ја разгледува и оценува во период не подолг од десет години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицираната информација со степенот „СТРОГО ДОВЕРЛИВО“ се разгледува и оценува во период не подолг од пет години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицираната информација со степенот „ДОВЕРЛИВО“ се разгледува и оценува во период не подолг од три години за да се оцени потребата од натамошно задржување на класификацијата.

Класифицираната информација со степенот „ИНТЕРНО“ се разгледува и оценува во период не подолг од две години за да се оцени потребата од натамошно задржување на класификацијата.

Со член 20 се допрецизира одредбата од претходниот член и се утврдува временскиот период според степенот на класификација за којшто создавачот разгледува и оценува одредена класифицирана информација со цел утврдување на потребата од натамошно задржување на постојниот степен на класификација.

Така законодавецот уредува дека за класифицираната информација со степенот „ДРЖАВНА ТАЈНА“ тој период не е подолг од десет години, за класифицираната информација со степенот „СТРОГО ДОВЕРЛИВО“ не е подолг од пет години, за класифицираната информација со степенот „ДОВЕРЛИВО“ не е подолг од три години, а за класифицираната информација со степенот „ИНТЕРНО“ тој период не е подолг од две години. Но, понатаму во прекршочните одредби, законодавецот

не предвидува одговорност за создавачот доколку тој не ја разгледа и оцени потребата од натамошно задржување на класификацијата на информацијата во определениот рок.

Оценувањето на потребата за задржување на степенот е предвидено со цел да се намалат мерките за заштита или да се овозможи пристап до информацијата којашто нема потреба повеќе да се заштитува. Со тоа ќе се овозможи поголема економичност во искористување на ресурсите и поголема транспарентност во работата на државните органи и институции.

Член 21

Ако со класифицираната информација се прикрива пречекорување на овластување, злоупотреба на функцијата или некое друго незаконско дејствие, односно казниво дело, таквата информација нема да се смета за класифицирана.

На лицата кои ќе ја пријават информацијата од ставот 1 на овој член до надлежен орган согласно со Законот за заштита на укажувачи, им се гарантира заштита согласно со закон.

Со цел да се оневозможи зад класифицирана информација да се прикрие пречекорување на овластување, злоупотреба на функцијата или некое друго незаконско дејствие, односно казниво дело, во членот 21 е уредено дека таквата информација нема да се смета за класифицирана.

Имено, хипотетички можно е лице кое е овластено да доделува степен на класификација на информациите, да го злоупотреби таквото овластување со цел да прикрие определено противправно постапување, па, оттука, со овој член се превенира таквата заштита на информациите преку класификација да биде употребена во незаконски и нелегитимни цели.

Во споредба со Законот за класифицирани информации од 2004 година, во овој закон е воведена и одредба за заштита на лицата што ќе пријават класифицирана информација со која се прикрива незаконско дејствие, односно нивната заштита е гарантирана со Законот за заштита на укажувачите²⁰ како нов механизам за борба против корупцијата и криминалот.

²⁰ Закон за заштита на укажувачите, „Службен весник на Република Македонија“ број 196/15 и 35/18.

КЛАСИФИЦИРАНИ ИНФОРМАЦИИ НА СТРАНСКИ ДРЖАВИ И МЕЃУНАРОДНИ ОРГАНИЗАЦИИ

Член 22

Класифицираните информации од странски држави или меѓународни организации со кои Република Северна Македонија има склучено меѓународни договори или на кои Република Северна Македонија им пристапила, го задржуваат степенот на класификација што се користи во таа држава или меѓународна организација.

Во членот 22 е дефинирано дека странските информации коишто се отстапени на користење на Република Северна Македонија, а припаѓаат на странски држави или на меѓународни организации со коишто склучила меѓународни договори или на коишто им пристапила, го задржуваат оригиналниот степен на класификација, односно степенот што се користи во таа држава или меѓународна организација.

Преку оваа одредба се нагласува усогласеноста на националните стандарди за обезбедување заштита на класифицирани информации со меѓународно прифатените стандарди и воедно се потврдува определбата на државата за обезбедување подеднаква заштита на странските класифицирани информации како и за националните класифицирани информации што го носат истиот степен на класификација. Во случај на промена во системот на класификација на информациите во некоја странска држава со којашто Република Северна Македонија има склучено меѓународен договор, со оваа одредба од Законот се овозможува континуитет во заштитата на разменетите информации.²¹

Член 23

Дисеминација на странските класифицирани информации се врши согласно со принципот „потребно е да знае“ и поседување на соодветен безбедносен сертификат.

Начинот на определување на корисниците и вршењето на дисеминација на добиените странски класифицирани информации со уредба поблиску ги уредува Владата на Република Северна Македонија.

Во членот 23 е уредена дисеминацијата, односно распоредувањето на странските класифицирани информации до лица кои поседуваат соодветен безбедносен сертификат и во согласност со принципот „потребно е да знае“. Тоа значи дека не е доволно определено лице да има само соодветен безбедносен сертификат, бидејќи во таков случај странските класифицирани информации би се распоредувале до сите лица што поседуваат безбедносен сертификат со соодветниот степен на класификација. Напротив, со постапување во согласност со принципот „потребно е да знае“ („need to know“), ваквите (странски) класифицирани информации ќе се распоредат само до оние лица кои навистина е потребно да ја знаат содржината на соодветната информација.

²¹ Франција пред извесно време ја промени законската рамка за заштита на тајноста на информациите од значење за националната безбедност со којашто е предвидено наместо три степени на класификација од 1 јули 2021 година да се применува систем со два степени на класификација. Следствено на тоа, Спогодбата меѓу Владата на Република Македонија и Владата на Република Франција за размена и заемна заштита на класифицирани информации, потпишана во Скопје на 5 јули 2010 година, ќе треба да биде предмет на соодветни измени во согласност со предвидената процедура за таа цел.

Дисеминацијата на класифицирани информации како поим за прв пат се воведува во овој закон заради неговата општоприфатена примена во кругот на корисниците на класифицираните информации.

Вториот став на овој член предвидува Владата на Република Северна Македонија со уредба понатаму подетално да ги уреди начинот на определување на корисниците и вршењето на дисеминација на добиените странски класифицирани информации. Оваа материја, поконкретно, е предмет на уредување во подзаконскиот акт во којшто се пропишани мерките од доменот на административната безбедност на класифицираните информации.

ГЛАВА ТРЕТА

КРИТЕРИУМИ, МЕРКИ И АКТИВНОСТИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 24

За заштита на класифицираните информации, се преземаат мерки и активности за административна, физичка и индустриска безбедност, безбедност на комуникациско-информациски системи, како и за безбедност на лица-корисници на класифицирани информации.

Третата глава од Законот се фокусира на критериумите, мерките и активностите за заштита на класифицираните информации. Како резултат на тоа, во членот 24 се дефинирани домените во коишто се применуваат мерките и активностите, односно доменот на административната безбедност, на физичката безбедност, на индустриската безбедност, на безбедноста на комуникациско-информациските системи, како и доменот на безбедноста на лица-корисници на класифицирани информации.

Ваквото дефинирање на мерките и активностите е усогласено со меѓународно-прифатените стандарди за заштита на класифицирани информации.

Член 25

Критериуми кои особено се земаат предвид при утврдувањето на мерките за заштита на класифицираните информации се:

- ▶ степенот на класификација,
- ▶ обемот и формата на класифицираната информација и
- ▶ процената на ризикот за безбедноста на класифицираната информација.

Во членот 25 се дефинирани минималните критериуми кои се земаат предвид при утврдувањето на мерките за заштита на класифицираните информации. Самиот израз „кои особено се земаат предвид“, значи дека при утврдување на мерки за заштита треба да се земат предвид што повеќе критериуми релевантни за конкретната информација, но наведените се задолжителни за разгледување.

Првиот критериум е степенот на класификација од којшто понатаму зависи обемот и сериозноста на мерките и активностите што ќе бидат применети за заштита на класифицираните информации. По правило, повисок степен на класификација подразбира построги мерки за заштита, а со тоа и ангажирање поголеми ресурси.

Обемот и формата на класифицираната информација е следниот критериум што се зема предвид при утврдувањето на мерките за заштита на класифицираните

информации. Доколку класифицираната информација има голем „габарит“, е во форма на машина или друг уред и сл., корисникот на таквата класифицирана информација треба да обезбеди соодветни простории за чување, како и мерки за заштита. Доколку пак станува збор за класифицирана информација во електронска форма, корисникот на истата ќе треба да преземе соодветни мерки за заштита на комуникациско-информациските системи во коишто таквата информација се обработува и чува.

Процената на ризикот за безбедноста на класифицираната информација е третиот и не помалку важен критериум при утврдувањето на мерките за заштита на класифицираните информации. Таа претставува сеопфатна анализа на сите фактори што би можеле да ја нарушат безбедноста на класифицираната информација чиишто резултати понатаму укажуваат на обемот и степенот на заштита што треба да се обезбеди за таа информација.

АДМИНИСТРАТИВНА БЕЗБЕДНОСТ

Член 26

Мерки и активности за административна безбедност се:

- ▶ определување на степенот на класификација и обележување на класифицираната информација,
- ▶ прием и евиденција на класифицираната информација,
- ▶ определување начин за чување, ракување и контрола на класифицираната информација,
- ▶ репродукција, преводи и извадоци на класифицираната информација и одредување на бројот на примероците и корисниците,
- ▶ дисеминација на класифицирани информации,
- ▶ пренос на класифицирани информации,
- ▶ отстранување и уништување на класифицираната информација.

Мерките и активностите за административна безбедност со уредба поблиску ги уредува Владата на Република Северна Македонија.

Во членот 26 се наведени мерките и активностите за административна безбедност, односно за безбедност на информациите како што се нарекува во директивите и актите на НАТО и на ЕУ.²²

Првата алинеја од став 1 на овој член се однесува на определувањето на степенот на класификација и нејзиното соодветно обележување. При определувањето на степенот на класификацијата се земаат предвид показатели кои поблиску укажуваат на степенот на евентуалната штета што би настанала за Република Северна Македонија или за странска земја или меѓународна организација со неовластен пристап до класифицираната информација или со нејзина неовластена употреба. По утврдување на степенот на класификација, создавачот на класифицираната

²² За определување на степенот на класификација и обележување на класифицираните информации, прием и евиденција на класифицираните информации, рекласификација и декласификација на класифицираните информации, пренос и чување на класифицираните информации, изработка на преводи, копии и слично, в. Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, Enclosure "E", 20 November 2020; Council Decision of 23 September 2013 on the security rules for protecting EU classified information 32013D0488 (Official Journal of the European Union L274/1), Annex III)

информација треба соодветно да ја обележи со цел истата да ја добие соодветната заштита.

Втората алинеја се однесува на приемот и евиденцијата на класифицираната информација коишто се вршат во согласност со постојните правила за канцелариско и архивско работење и претставуваат важен чекор во заштитата на информацијата бидејќи уредната евиденција на информацијата и „следењето“ на нејзиното движење е еден од предусловите за обезбедување соодветна заштита.

Третата алинеја од став 1 на овој член се однесува на определувањето на начинот за чување, ракување и контрола на класифицираната информација. Начинот на којшто класифицираната информација ќе се чува, со неа ќе се ракува и истата ќе се контролира зависи од степенот на класификација на таа информација и од нејзиниот обем и форма.

Репродуцирањето на класифицираната информација и правењето преводи и извадоци од истата, како и одредувањето на бројот на примероците и на корисниците се следните мерки и активности за административна безбедност наведени во овој член. Меѓународно прифатениот стандард во овој случај е дека сите репродукции, преводи и копии ги носат истите обележја и ја имаат истата заштита како и оригиналната класифицирана информација, а со цел да се овозможи нивна соодветна заштита и контрола, потребно е нивниот број да се ограничи на бројот потребен за извршување на службените задачи, а нивните корисници соодветно да се евидентираат.

Петтата алинеја се однесува на дисеминацијата на класифицираната информација, односно нејзиното распределување до крајните корисници, што подразбира доставување на класифицираната информација до лица коишто имаат соодветен безбедносен сертификат согласно принципот „потребно е да знае“. Следствено на тоа се уредува и преносот на класифицираната информација, при што се води сметка и за начинот на пакување на истата, според нејзиниот степен на класификација.

Отстранувањето и уништувањето на класифицираната информација го претставуваат последниот чекор од нејзиниот „животен циклус“ и истиот се спроведува во согласност со постојните национални правила за канцелариско и архивско работење и со регулативите на НАТО и на ЕУ за ракување со нивните класифицирани информации.

Вториот став на овој член предвидува Владата на Република Северна Македонија со уредба понатаму подетално да ги уреди мерките и активностите за административна безбедност на класифицирани информации.

ФИЗИЧКА БЕЗБЕДНОСТ

Член 27

Физичката безбедност се остварува со примена на физички и технички заштитни мерки со цел да се спречи неовластен пристап до класифицирани информации.

Мерките за физичка безбедност треба да спречат прикриен или насилан упад од неовластено лице, да одвратат, спречат и детектираат неовластени активности, како и да овозможат поделба на персоналот во нивниот пристап до класифицирани информации согласно со принципот „потребно е да знае“.

Мерките за физичка безбедност се применуваат во објекти, згради, канцеларии, простории и други локации во кои се ракува, се чуваат или електронски се обработуваат класифицирани информации.

Просториите во кои се чуваат класифицирани информации со степен „ДОВЕРЛИВО“ и повисоко, се воспоставаат како безбедносни зони.

За заштита на класифицирани информации со степен „ДОВЕРЛИВО“ и повисоко се користи опрема, системи или други технички средства кои исполнуваат минимални стандарди, кои ги пропишува директорот на Дирекцијата.

Во првиот став од членот 27 е уредено дека физичката безбедност се остварува со примена на физички и технички заштитни мерки со цел да се спречи неовластен пристап до класифицирани информации.

Понатаму, одредбите од членот укажуваат на резултатите што треба да се постигнат со примена на мерките за физичка безбедност, а тоа се спречување на прикриен или насилан упад од неовластено лице, одвраќање, спречување и детектирање неовластени активности, како и овозможување поделба на персоналот во нивниот пристап до класифицирани информации во согласност со принципот „потребно е да знае“.

Третиот став од членот укажува на сеопфатноста на примената на мерките за физичка безбедност, односно на нивната примена на сите локации, објекти, згради, канцеларии и простории, на коишто се ракува, во коишто се чуваат или електронски се обработуваат класифицирани информации.

Во последните два става од членот е нагласено воспоставувањето на безбедносни зони во просториите во коишто се чуваат класифицирани информации со степен „ДОВЕРЛИВО“ и повисоко, како и користењето на опрема, системи или други технички средства за заштита на таквите информации. Законодавецот, оттука, смета дека како безбедносни зони треба да се востановат просториите за класифицираните информации со степени „ДОВЕРЛИВО“, „СТРОГО ДОВЕРЛИВО“ И „ДРЖАВНА ТАЈНА“, односно за оние степени за кои едно лице за да може да ракува со нив треба да поседува соодветен безбедносен сертификат. Оттука, оваа одредба е исклучувачка во спротивниот правец, односно *argumentum a contrario* просториите во кои се чуваат класифицираните информации со степен „ИНТЕРНО“ не се востановуваат како безбедносни зони.

Притоа е уредено дека претходно споменатата опрема, системи и средства

треба да исполнуваат минимални стандарди коишто ги пропишува директорот на Дирекцијата. Во основа, пропишувањето на тие стандарди се заснова на меѓународно-прифатените стандарди на НАТО и на ЕУ, односно на листите на препорачните производи кои ги исполнуваат пропишаните стандарди на тие меѓународни организации за заштита на класифицираните информации.

Член 28

Мерки и активности за физичка безбедност се:

- ▶ проценка за можно нарушување на безбедноста на класифицираната информација,
- ▶ определување на безбедносен појас околу објектот,
- ▶ определување на безбедносни и административни зони,
- ▶ организирање на физичка заштита и примена на технички средства за обезбедување на објекти и простории во кои се наоѓаат класифицирани информации,
- ▶ контрола на влез, движење и излез на лица и возила за пренос на класифицирани информации и
- ▶ физичко обезбедување при пренесување на класифицирани информации надвор од безбедносните зони.

Мерките и активностите за физичка безбедност со уредба поблиску ги уредува Владата на Република Северна Македонија.

Вочленот 28 акцентот е ставен на мерките и активностите за физичка безбедност при што не случајно на прво место е ставена процената за можно нарушување на безбедноста на класифицираната информација. Резултатите од процената на можноста за загрозување на безбедноста на класифицираните информации и на изворите од каде може да потекне таа, даваат солидна основа за определување на мерките и активностите за физичка безбедност за заштита на класифицираните информации. Тука, пред сè се мисли на определување на безбедносен појас околу даден објект, на определување на безбедносни и административни зони во даден објект, како и на организирање на физичката заштита и примената на технички средства за обезбедување на објекти и простории во кои се наоѓаат класифицирани информации.

Мерките и активностите за физичка безбедност опфаќаат, покрај претходно наведеното, и обезбедување контрола на влез, движење и излез на лица и возила за пренос на класифицирани информации, како и физичко обезбедување при пренесување на класифицирани информации надвор од безбедносните зони. Имајќи предвид дека безбедносното опкружување и изворите на закани постојано се менуваат, а технологијата брзо напредува, во предвидените мерки и активности за физичка безбедност на класифицирани информации треба да се остави можност за надградување и дополнување.

Со вториот став на овој член се дава основа за понатамошно поминувањето на определување на идентификуваните мерки и активности за физичка безбедност на класифицирани информации во уредба што ќе ја донесе Владата на Република Северна Македонија.

БЕЗБЕДНОСТ НА ЛИЦА-КОРИСНИЦИ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 29

Мерки и активности за безбедност на лица-корисници на класифицирани информации се:

- ▶ определување на офицер за безбедност на класифицирани информации,
- ▶ безбедносна проверка,
- ▶ издавање на безбедносен сертификат,
- ▶ издавање на дозвола за пристап до класифицирани информации и
- ▶ проверка и оценување на способноста за постапување со класифицирани информации.

Мерките и активностите за безбедност на лица корисници на класифицирани информации со уредба поблиску ги уредува Владата на Република Северна Македонија.

Мерките и активностите за безбедност на лица корисници на класифицирани информации таксативно се наведени во членот 29 за потоа подетално да бидат уредени подолу во Законот.

Определувањето офицер за безбедност на класифицирани информации и неговите обврски детално се разработени во Глава четврта од овој закон. Офицерите за безбедност на класифицирани информации претставуваат клучни лица од персоналот за одржливост, спроведување и надзор над безбедносните политики за работа со класифицирани информации во секој од релевантните органи на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правните лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други правни лица, каде што се ракува и се чуваат класифицирани информации.

Заедно со безбедносната проверка на лицата со цел издавање безбедносен сертификат за пристап до класифицирани информации, издавањето на безбедносен сертификат, издавањето на дозвола на странски физички и правни лица за пристап до класифицирани информации на Република Северна Македонија, како и проверката и оценувањето на способноста за постапување со класифицирани информации како мерки и активности за безбедност на лица-корисници на класифицирани информации, законодавецот предвидел поблиску да бидат уредени со уредба што ја донесува Владата на Република Северна Македонија.

БЕЗБЕДНОСТ НА КОМУНИКАЦИСКО-ИНФОРМАЦИСКИ СИСТЕМИ

Член 30

Безбедност на комуникациско-информациски системи е примена на безбедносни мерки за заштита на комуникациските, информациските и другите електронски системи и на класифицираните информации кои се создаваат, чуваат, обработуваат или пренесуваат во овие системи, со цел да се обезбеди нивна доверливост, интегритет, достапност, автентичност и неотповикливост.

Заради обезбедување на целите од ставот 1 на овој член се имплементира соодветен систем на безбедносни мерки за административна и физичка безбедност, безбедност на комуникациско-информациски системи, како и за безбедност на лица-корисници на класифицирани информации, со цел создавање на безбедносна околина во која функционираат комуникациските, информациските или другите електронски системи.

Системот на безбедносни мерки на комуникациско-информациските системи мора да се заснова на процес за управување со безбедносен ризик.

Во членот 30 законодавецот ја дефинира безбедноста на комуникациско-информациските системи (КИС), при што утврдува дека истата претставува примена на безбедносни мерки за заштита на комуникациските, информациските и другите електронски системи и на класифицираните информации кои се создаваат, чуваат, обработуваат или пренесуваат во овие системи, со цел да се обезбеди нивна доверливост, интегритет, достапност, автентичност и неотповикливост.

Во вториот став на овој член се нагласува потребата од имплементирање на сеопфатен систем на безбедносни мерки за административна и за физичка безбедност, за безбедност на КИС, како и за безбедност на лица корисници на класифицирани информации, со цел создавање на безбедносна околина во која функционираат комуникациските, информациските или другите електронски системи. Сотоа законодавецот укажува на комплексноста на мерките и активностите што се потребни за да се постигне безбедноста на КИС и води кон подигнување на безбедносната свест кај корисниците на класифицирани информации при ракувањето со истите и нивното чување во електронска форма.

Од таа причина во третиот став на овој член законодавецот укажува дека системот на безбедносни мерки на КИС мора да се заснова врз процес на управување со безбедносен ризик. Ако се земе предвид дека управувањето со безбедносен ризик веќе е дефинирано како процес на идентификација, контролирање, минимизирање или елиминирање на настани што можат да влијаат врз безбедноста на една организација или на системот што таа го користи, може да се заклучи дека законодавецот уште еднаш ја нагласува комплексноста на оваа материја и потребата од одржување високо ниво на безбедносна свест за променливото безбедносно опкружување и брзиот развој на технологијата, особено на информатичката технологија и експанзијата на компјутерскиот криминал.

Член 31

Мерки и активности за безбедност на комуникациско-информациски системи се:

- ▶ акредитација на комуникациско-информациски системи и процеси,
- ▶ процена за можно нарушување на безбедноста на класифицираната информација со неовластено навлегување во комуникациско-информацискиот систем во кој се чуваат, обработуваат и пренесуваат класифицирани информации,
- ▶ утврдување на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма,
- ▶ заштита при создавање, чување, обработка и пренос на класифицирани информации во комуникациско-информациски системи,
- ▶ криптографска безбедност на комуникациски, информациски и други електронски системи преку кои се создаваат, чуваат, обработуваат со криптозаштита и пренесуваат класифицирани информации,
- ▶ заштита од компромитирачко електромагнетно зрачење,
- ▶ определување на зони и простории заштитени од компромитирачко електромагнетно зрачење и
- ▶ инсталирање на уреди за чување на класифицирани информации.

Мерките и активностите за безбедност на комуникациско-информациски системи со уредба поблиску ги уредува Владата на Република Северна Македонија.

Мерките и активностите за безбедност на комуникациско-информациските системи (КИС) таксативно се наведени во членот 31, при што законодавецот предвидел и нивно поблиско уредување со уредба на Владата на Република Северна Македонија. При набројувањето на мерките и активностите за безбедност на КИС, законодавецот ја наведува акредитацијата на КИС и процесите за работа на истите и со тоа укажува на потребата од формално одобрување на КИС за работа до одредениот степен на класификација. Формалното одобрување на КИС како надлежност на Дирекцијата за безбедност на класифицирани информации е уредено подолу во овој закон, во член 69 став 2 алинеја 9.

Како следна мерка за безбедност на КИС е наведена процената за можното нарушување на безбедноста на класифицираната информација со неовластено навлегување во КИС во кој се чуваат, обработуваат и пренесуваат класифицирани информации. Целта на таквата процена е да се утврди ризикот, да се процени ризикот кој не може да се избегне, да се оценат ранливоста и заканите, како и да се утврдат последиците од реализација на одредени закани.

Третата алинеја се однесува на утврдувањето на методи и безбедносни процедури за прием, обработка, пренос, чување и архивирање на класифицирани информации во електронска форма. Тоа е сеопфатна постапка при којашто треба да се води сметка за примена на соодветните мерки и активности од доменот на административната безбедност при приемот, обработката и преносот на класифицираните информации, потоа од доменот на физичката безбедност во однос на определувањето на безбедносните зони во коишто се лоцирани КИС зависно од степенот на класифицираните информации што се обработуваат во нив, како и мерки и активности од доменот на безбедноста на лица-корисници на класифицирани информации согласно кои пристап до КИС во кој се обработуваат класифицирани информации може да има само корисник кој има соодветен безбедносен сертификат на степенот на класификација на КИС и е соодветно

запознаен со обврските што произлегуваат од безбедносно-оперативните процедури за КИС.

Понатаму, законодавецот укажува на мерките за заштита при создавање, чување, обработка и пренос на класифицирани информации во КИС, на криптографската безбедност на комуникациски, информациски и други електронски системи преку кои се создаваат, чуваат, обработуваат со криптозаштита и пренесуваат класифицирани информации, како и на заштита од компромитирачко електромагнетно зрачење и определување на зони и простории заштитени од компромитирачко електромагнетно зрачење. Мерките за заштита од компромитирачко електромагнетно зрачење подразбираат технички мерења со коишто се определуваат зони во објектите во коишто се лоцирани КИС и следствено на добиените резултати се определуваат соодветни мерки за заштита од аспект на физичката безбедност.

Како последна мерка за безбедност на КИС законодавецот го наведува инсталирањето на уреди за чување на класифицирани информации, што подразбира истите да бидат инсталирани од стручни и овластени лица.

Член 32

Мерки и активности за криптографска безбедност се:

- ▶ планирање, организација и имплементација на криптографска безбедност,
- ▶ евалуација и одобрување на криптоматеријали и криптопроизводи,
- ▶ изработка и развој на криптографски алгоритми и производи,
- ▶ планирање, организација и управување со криптоматеријали,
- ▶ примена на мерки и процедури за евиденција, безбедно ракување, чување и дистрибуција на криптоматеријали и криптопроизводи,
- ▶ обука на лица за работа со криптоматеријали и криптопроизводи,
- ▶ контрола на имплементација на мерките и активностите за криптографска безбедност и на начинот на употреба на криптографските материјали и производи.

Мерките и активностите за криптографска безбедност со уредба поблиску ги уредува Владата на Република Северна Македонија.

Како една од мерките и активностите за безбедност на комуникациско-информациските системи е и криптографската безбедност. Во членот 32 таксативно се наведени мерките и активностите за криптографска безбедност, при што законодавецот предвидел и нивно поблиско уредување со уредба на Владата на Република Северна Македонија. Ова не претпоставува дека досега оваа материја воопшто не била уредена, туку дека постојната Уредба, донесена во 1995 година и класифицирана со степен „ДРЖАВНА ТАЈНА“, треба да се замени со нова уредба во којашто ќе се рефлектираат моменталните текови во доменот на криптографската заштита и со којашто јасно ќе се уредат односите меѓу сите носители на криптографската заштита во државата.

Земајќи предвид дека законодавецот ја дефинира криптографската безбедност како оперативно-планска активност во системот на криптографски материјали и производи кои се користат за заштита на класифицирани

информации од неовластен пристап при изработка, ракување и чување на класифицираните информации, сите наведени мерки и активности посочуваат на комплексна материја за чијашто имплементација е потребен технички образован и соодветно обучен кадар. Законодавецот препознал неколку мерки и активности за криптографска безбедност коишто сами по себе претставуваат посебни процеси што вклучуваат повеќе активности. Такви процеси се планирањето, организацијата и имплементацијата на криптографска безбедност; евалуацијата и одобрувањето на криптоматеријалите и криптопроизводите што се користат за обезбедување криптографска заштита; изработката и развојот на криптографски алгоритми и производи; планирањето, организацијата и управувањето со криптоматеријали; примената на мерки и процедури за евиденција, безбедно ракување, чување и дистрибуција на криптоматеријали и криптопроизводи; обуката на лица за работа со криптоматеријали и криптопроизводи, како и вршењето на контрола на имплементација на мерките и активностите за криптографска безбедност и на начинот на употреба на криптографските материјали и производи.

Заради специфичната природа на материјата, донесувањето на посебен подзаконски акт со којшто ќе се уредат односите меѓу органите на државната управа коишто имаат надлежности во доменот на криптографската заштита е од исклучителна важност за Република Северна Македонија.

Член 33

Пренос на класифицирани информации преку комуникациски системи надвор од безбедносните зони се врши исклучиво со примена на криптографска заштита.

Во овој член законодавецот пропишува дека преносот на класифицирани информации преку комуникациски системи надвор од безбедносните зони се врши исклучиво со примена на криптографска заштита и притоа не предвидел ограничување во степенот на класификација на информациите во однос на електронскиот пренос. Тоа подразбира дека класифицирани информации од сите степени на класификација можат да се пренесуваат по електронски пат со задолжителна примена на криптографска заштита.

ИНДУСТРИСКА БЕЗБЕДНОСТ

Член 34

Мерките за индустриска безбедност се применуваат со цел обезбедување заштита на класифицираните информации од страна на договарачите и субјектите вклучени во преговорите пред склучување на договор и во текот на реализација на класифицираниот договор.

Со мерките за индустриска безбедност се обезбедува заштита на класифицираните информации при транспорт и при воспоставување на процедури за посета на физички и правни лица на објекти каде што се ракува со класифицирани информации.

За пристап и ракување со класифицирани информации при реализирање на

класифицирани договори, транспорт на класифицирани информации и посети на објекти каде што се ракува со класифицирани информации, физичките и правните лица од ставовите 1 и 2 на овој член треба да поседуваат соодветен безбедносен сертификат или дозвола за пристап до класифицирани информации.

За потребата за класифицирање на договор и фазите коишто претходат на склучувањето на договорот, вклучувајќи го и јавниот повик за учество во јавни набавки, правното лице треба да обезбеди мислење од офицерот за безбедност на класифицирани информации на субјектот што го распишува јавниот повик.

Мерките и активностите за индустриска безбедност ги опфаќаат мерките и активностите од членовите 26 став 1, 28 став 1, 29 став 1, 31 став 1 и 32 став 1 од овој закон.

Мерките и активностите за индустриска безбедност со уредба поблиску ги уредува Владата на Република Северна Македонија.

Во членот 34 законодавецот уредува дека мерките и активностите за индустриска безбедност се применуваат со цел обезбедување заштита на класифицираните информации од страна на договарачите и субјектите вклучени во преговорите пред склучување на договор и во текот на реализација на класифицираниот договор. Тоа значи заштита која ги опфаќа сите фази, дури и оние кои претходат на самото склучување на договорот. Тоа е оправдано од причина што дури и во тие фази може да се користат и разменуваат информации што се и/или треба да бидат заштитени.

Дополнително, се пропишува дека мерките за индустриска безбедност обезбедуваат заштита на класифицираните информации при транспорт и при воспоставување на процедури за посета на физички и правни лица на објекти каде што се ракува со класифицирани информации. Притоа законодавецот укажува на поврзаноста на индустриската безбедност со мерките и активностите за безбедност на лица корисници на класифицирани информации со тоа што предвидел дека за пристап и ракување со класифицирани информации при реализирање на класифицираните договори, при транспортот на класифицирани информации и при посети на објекти каде што се ракува со класифицирани информации, физичките и правните лица треба да поседуваат соодветен безбедносен сертификат или дозвола за пристап до класифицирани информации.

Во четвртиот став на овој член е уредено дека при класифицирање на договор и фазите што претходат на склучувањето на договорот, вклучувајќи го и јавниот повик за учество во јавни набавки, правното лице треба да обезбеди мислење од офицерот за безбедност на класифицирани информации на субјектот што го распишува јавниот повик.

Во овој член законодавецот таксативно не ги наведува мерките и активностите за индустриска безбедност како што тоа претходно го прави со останатите мерки и активности од причина што индустриската безбедност ги опфаќа сите пропишани мерки и активности од доменот на административната безбедност, безбедноста на лица корисници на класифицирани информации, физичката безбедност и безбедноста на КИС.

Таквата сеопфатност на мерките и активностите за индустриска безбедност законодавецот предвидел поблиску да се уреди со уредба на Владата на Република Северна Македонија.

РАЗМЕНА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ СО СТРАНСКИ ДРЖАВИ И МЕЃУНАРОДНИ ОРГАНИЗАЦИИ

Член 35

Класифицирана информација на странска држава или меѓународна организација е информација којашто надлежниот орган на странската држава или меѓународната организација ја отстапил на Република Северна Македонија со обврска да се обезбеди нејзина заштита.

Со класифицираните информации примени од странска држава или меѓународна организација се постапува на начин којшто е предвиден со ратификуван меѓународен договор.

Ако меѓународниот договор од ставот 2 на овој член не содржи одредби за начинот на постапување со класифицираните информации, се постапува согласно со одредбите од овој закон.

Во првиот став од член 35 законодавецот ја дефинира класифицираната информација на странска држава или меѓународна организација како информација којашто надлежниот орган на странската држава или меѓународната организација ја отстапил на Република Северна Македонија со обврска да се обезбеди нејзина заштита.

Следствено на тоа, во вториот став се препознава обврската на корисниците на класифицирани информации во земјата за постапување со таквите информации на начин којшто е предвиден со ратификуван меѓународен договор. А доколку договорот не содржи одредби за начинот на постапување со класифицираните информации, законодавецот предвидел дека ќе се применуваат одредбите од овој закон. Со тоа, пред сè се исклучува примената на соодветните одредби од овој закон во случај кога со ратификуваниот меѓународен договор е утврден начинот на постапување со ваквите информации. Примената на нашето домашно законодавство доаѓа предвид кога меѓународниот договор не предвидел одредби за начинот на постапување.

Со прифаќање на вакво решение се демонстрира сериозниот однос кон заштитата на класифицираните информации и усогласеноста на националното законодавство со пропишаните меѓународни стандарди и мерки на заштита на класифицирани информации.

Член 36

Во случај на воена, вонредна или кризна состојба во Република Северна Македонија, по барање на надлежните органи согласно со Уставот на Република Северна Македонија и со закон, Дирекцијата може да врши размена на класифицирани информации со странски држави и меѓународни организации со кои не се склучени меѓународни договори по претходна согласност од страна на Владата на Република Северна Македонија, ако е тоа во интерес на Република Северна Македонија.

По завршување на воената, вонредната или кризната состојба од ставот 1 на овој член, Дирекцијата доставува извештај до Владата на Република Северна

Македонија за разменетите класифицирани информации со странски држави и меѓународни организации со кои не се склучени меѓународни договори.

Членот 36 содржи одредби со коишто за прв пат досега се уредува постапувањето на Дирекцијата за безбедност на класифицирани информации во однос на размената на класифицирани информации со странски држави и меѓународни организации со кои не се склучени меѓународни договори во случај на воена, вонредна или кризна состојба во Република Северна Македонија.

Значи, се работи за исклучителен случај (размена на класифицирани информации со странски држави и меѓународни организации во отсуство на соодветен меѓународен договор) во исклучителни околности (вонредна, воена или кризна состојба).

Имено, првиот став од членот пропишува дека Дирекцијата може да врши размена на класифицирани информации во таков случај, ако е тоа во интерес на Република Северна Македонија, по барање на надлежните органи, во согласност со Уставот на Република Северна Македонија и со закон и по претходна согласност од страна на Владата на Република Северна Македонија. Во вториот став на овој член законодавецот ја превидел обврската на Дирекцијата по завршување на воената, вонредната или кризната состојба во земјата до Владата да достави извештај за разменетите класифицирани информации со странските држави и меѓународни организации со кои не се склучени меѓународни договори.

Со ваквото решение законодавецот ги уредува односите и обврските на Дирекцијата во контекст на горенаведеното а во случај на воена, вонредна или кризна состојба во Република Северна Македонија со нагласување дека истите се реализираат ако е тоа во интерес на државата.

Член 37

Согласно со преземените обврски од ратификуваните меѓународни договори, Дирекцијата овозможува вршење контрола на овластени претставници на странски држави и меѓународни организации, на начинот на користење и заштита на класифицираните информации што од нив се отстапени на користење во Република Северна Македонија.

Контрола на начинот на користење и заштита на доставените класифицирани информации од Република Северна Македонија до странските држави и меѓународните организации врши Дирекцијата согласно со овој закон и ратификуваните меѓународни договори.

Одредбата од овој член е своевиден континуум на одредбата од член 35 и во неа законодавецот ги препознава преземените обврски од ратификуваните меѓународни договори како основа за уредување на контролата на начинот на користење и заштита на разменетите класифицирани информации меѓу Република Северна Македонија и други странски држави и меѓународни организации. Притоа е изразено начелото на рециприцитет.

Следствено на тоа, предвидел дека овластени претставници на странски држави и меѓународни организации можат да вршат контрола на начинот на користење и заштита на класифицираните информации коишто од нив се отстапени на користење во Република Северна Македонија, додека во однос на националните класифицирани информации што се доставени од Република Северна Македонија

до нив, законодавецот предвидел контролата на начинот на којшто тие информации се користат и заштитуваат да ја врши Дирекцијата за безбедност на класифицирани информации.

КОРИСТЕЊЕ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 38

Орган на државната и локалната власт основан согласно со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или физичко или правно лице во Република Северна Македонија кое има безбедносен сертификат или странски државен орган, институција или странско физичко или правно лице кое има безбедносен сертификат на матичната држава и дозвола за пристап до класифицирани информации издадена од Дирекцијата, може да биде корисник на класифицирани информации согласно со принципот „потребно е да знае“.

Во членот 38 законодавецот пропишува кој може да биде корисник на класифицирани информации при што ја нагласува неопходноста од согласност со принципот „потребно е да знае“. Притоа, предвидел дека орган на државната и на локалната власт основан во согласност со Уставот на Република Северна Македонија и со закон, правно лице основано од Републиката или од општините, градот Скопје и општините во градот Скопје или физичко или правно лице во Република Северна Македонија, треба да поседува безбедносен сертификат, додека странски државен орган, институција или странско физичко или правно лице треба да поседува безбедносен сертификат на матичната држава и дозвола за пристап до класифицирани информации издадена од Дирекцијата. Со други зборови, законодавецот предвидува два кумулативни услови што треба едно лице (физичко или правно) да ги исполнува за да биде корисник на класифицирани информации, а тоа се: 1. поседување на соодветен безбедносен сертификат/безбедносен сертификат и дозвола за пристап (за странско физичко или правно лице) и 2. да може во конкретниот случај да се примени принципот „потребно е да знае“.

Ваквото решение уште еднаш го афирмира гореспоменатиот принцип кој е одамна познат и применуван во безбедносната теорија и практика и апострофиран во многу НАТО документи, но и оневозможува теоретски секое лице со соодветен безбедносен сертификат да има пристап до сите класифицирани информации со соодветниот степен. На тој начин, тајноста на информациите е дополнително обезбедена, а пристапот до нив ограничен само на лицата кои навистина имаат потреба да ја знаат содржината на конкретните информации заради извршување на нивните функции, задачи и овластувања.

Законодавецот тука (а ниту на друго место во Законот) не ги предвидел условите коишто е потребно да се исполнат за издавање на дозволата за пристап до класифицирани информации од страна на Дирекцијата.

Член 39

За извршување на работните задачи, на лицата кои ракуваат со класифицирани информации во органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, како и на други правни и физички лица им се издава безбедносен сертификат согласно со

принципот „потребно е да знае“.

Безбедносен сертификат се издава за пристап до соодветен степен на класифицирани информации.

За издавање на безбедносен сертификат за пристап до соодветен степен на класифицирани информации, заинтересираното физичко или правно лице поднесува писмено барање до Дирекцијата.

Барањето за издавање на безбедносен сертификат од ставот 3 на овој член се поднесува преку офицер за безбедност на класифицирани информации во правното лице.

Постапката за издавање на безбедносен сертификат за лицата вработени во Дирекцијата се спроведува преку офицерот за безбедност на класифицирани информации во Дирекцијата.

Безбедносен сертификат од ставот 2 на овој член издава директорот на Дирекцијата врз основа на претходно спроведена безбедносна проверка и оценка за постоење или непостоење на безбедносен ризик за ракување со класифицирани информации.

Членот 39 се фокусира на низа прашања поврзани со безбедносниот сертификат како неопходен предуслов за пристап до класифицирани информации на корисниците на класифицираните информации.

Притоа, во првиот став, законодавецот пропишува дека безбедносниот сертификат се издава на лицата кои ракуваат со класифицирани информации за извршување на нивните работни задачи во согласност со принципот „потребно е да знае“, а во вториот став уредува дека безбедносниот сертификат се издава за пристап до соодветен степен на класифицирани информации. Тоа подразбира дека степенот на класификација на безбедносниот сертификат треба да соодветствува, односно да биде најмалку еднаков на степенот на класификација на информациите до којшто корисникот има потреба за пристап. Тоа не го ограничува корисникот да има пристап до информација со понизок степен на класификација од степенот на класификација на безбедносниот сертификат што го поседува, но не дозволува пристап до информација со повисок степен на класификација од оној на безбедносниот сертификат. Со други зборови, безбедносен сертификат за повисок степен на класификација ги опфаќа и пониските степени, но не и повисоките.

Понатаму, законодавецот уредува дека заинтересираното физичко или правно лице треба да поднесе писмено барање до Дирекцијата за да може да започне постапката за издавање безбедносен сертификат и притоа пропишува дека барањето се поднесува преку офицер за безбедност на класифицирани информации во правното лице. Определувањето офицер за безбедност на класифицирани информации, како еден од клучните елементи на системот за заштита на класифицирани информации којшто е воведен со цел да се овозможи ефикасно и координирано извршување на правата и обврските кои се однесуваат на класифицираните информации, законодавецот подетално го уредил од член 65 до член 68 од овој закон.

За вработените во Дирекцијата за безбедност на класифицирани информации, во петтиот став на овој член е пропишано дека постапката за издавање безбедносен

сертификат се спроведува преку офицерот за безбедност на класифицирани информации во Дирекцијата.

Тоа значи дека „комуникацијата“ во поглед на барањето за издавање на безбедносен сертификат на определено лице се одвива преку офицерите за безбедност, односно офицерот за безбедност на правното лице каде што работи заинтересираното лице го препраќа барањето до Дирекцијата заради натамошно постапување.

Одредбата од последниот став на овој член уредува дека безбедносниот сертификат го издава директорот на Дирекцијата врз основа на претходно спроведена безбедносна проверка и оценка за постоење или непостоење на безбедносен ризик за ракување со класифицирани информации.

Издавањето на безбедносен сертификат на лица корисници на класифицирани информации подетално е уредено во подзаконски акт.²³

Член 40

Безбедносен сертификат за пристап и користење на класифицирани информации од сите степени, без претходна безбедносна проверка, заради непречено вршење на функцијата од денот на изборот до крајот на мандатот, добиваат: претседателот на Република Северна Македонија, претседателот на Собранието на Република Северна Македонија, претседателот на Владата на Република Северна Македонија, замениците на претседателот на Владата на Република Северна Македонија, претседателот на Уставниот суд на Република Северна Македонија и претседателот на Врховниот суд на Република Северна Македонија.

Во членот 40 е пропишан исклучок од одредбата од претходниот член, односно таксативно се наведени лицата коишто заради непречено вршење на функцијата од денот на изборот до крајот на мандатот добиваат безбедносен сертификат за пристап и користење на класифицирани информации од сите степени без претходна безбедносна проверка. Законодавецот, како што рековме, таксативно ги наведува носителите на највисоките јавни функции во државата, и тоа: претседателот на Република Северна Македонија, претседателот на Собранието на Република Северна Македонија, претседателот на Владата на Република Северна Македонија, замениците на претседателот на Владата на Република Северна Македонија, претседателот на Уставниот суд на Република Северна Македонија и претседателот на Врховниот суд на Република Северна Македонија.

Оваа листа на исклучоци е изработена во согласност со постојните пропишани меѓународни стандарди коишто се однесуваат на постапката за издавање безбедносни сертификати за пристап до класифицирани информации на носители на високи државни функции. Законот во врска со ова прашање е доста рестриктивен споредено со легислативата на други странски држави, но искуствата покажуваат дека меѓународните фактори позитивно гледаат на кратката листа на исклучоци бидејќи големиот број исклучоци може да претставува и поголем безбедносен ризик по класифицираните информации.

Член 41

²³ Уредба за безбедност на лица-корисници на класифицирани информации (Службен весник на Република Македонија број 82/04). Во тек е постапка за донесување на нова Уредба за безбедност на лица-корисници на класифицирани информации.

Безбедносен сертификат се издава на физичко лице кое ги исполнува следниве услови:

- ▶ да е државјанин на Република Северна Македонија,
- ▶ за безбедносен сертификат со степен „ДРЖАВНА ТАЈНА“ да не е државјанин и на друга држава,
- ▶ за безбедносен сертификат со степен „СТРОГО ДОВЕРЛИВО“ да не е државјанин на држава која не е членка на НАТО,
- ▶ да постои оправдана потреба за користење на класифицирани информации согласно со принципот „потребно е да знае“,
- ▶ да не постојат безбедносни пречки за пристап и ракување со класифицирани информации што се утврдува со оперативна проверка,
- ▶ физичкото лице да има деловна способност,
- ▶ лицето да наполнило 18 години, а за користење на класифицирани информации означени со степен „ДРЖАВНА ТАЈНА“ да наполнило 21 година,
- ▶ да не му е изречена санкција забрана за вршење на професија, дејност или должност,
- ▶ да поседува уверение за неосудуваност, не постаро од шест месеци,
- ▶ од оперативната проверка за лицата наведени во безбедносниот прашалник да не произлегува постоење на безбедносни пречки за пристап и ракување со класифицирани информации.

Пред издавање на сертификатот, лицето мора да се обучи за ракување со класифицирани информации.

Во членот 41 законодавецот ги дефинира условите за издавање безбедносен сертификат на физичко лице.

Притоа, во првата алинеја утврдува дека физичкото лице треба да е државјанин на Република Северна Македонија, но понатаму во втората алинеја уредува дека за безбедносен сертификат со степен „ДРЖАВНА ТАЈНА“ лицето не треба да има двојно државјанство, односно да не е државјанин и на друга држава, додека во третата алинеја прецизира дека за безбедносен сертификат со степен „СТРОГО ДОВЕРЛИВО“ физичкото лице не треба да е државјанин на држава која не е членка на НАТО. Во овие две алинеи законодавецот го дефинира ставот околу поседувањето на двојното државјанство при ракување со информации со повисок степен на класификација. Имено, на лица со двојно државјанство, нема да им биде издаден безбедносен сертификат за највисокиот степен на класификација по ниеден исклучок, додека за понискиот степен – „СТРОГО ДОВЕРЛИВО“, по исклучок, може да се издаде безбедносен сертификат за овој степен на лица со двојно државјанство, но само на оние лица чие друго државјанство е на држава членка на НАТО.

Понатаму, следат другите услови што треба да ги исполни физичкото лице за да добие безбедносен сертификат, односно да постои оправдана потреба за користење на класифицирани информации во согласност со принципот „потребно е да знае“, да не постојат безбедносни пречки за пристап и ракување со класифицирани информации што се утврдува со оперативна проверка, физичкото лице да има деловна способност, да наполнило 18 години, а за користење на класифицирани

информации означени со степен „ДРЖАВНА ТАЈНА“ да наполнило 21 година, да не му е изречена санкција забрана за вршење на професија, дејност или должност, да поседува уверение за неосудуваност коешто не е постаро од шест месеци и од оперативната проверка за лицата наведени во безбедносниот прашалник да не произлегува постоење на безбедносни пречки за пристап и ракување со класифицирани информации (лица од неговото семејство и сл.).

Во вториот став од овој член законодавецот предвидел дека пред издавање на сертификатот, лицето мора да се обучи за ракување со класифицирани информации, но притоа не ги уредил условите, односно не предвидел за каква обука станува збор и кој ја спроведува. Од таа причина членот треба да се дополни со одредби коишто дополнително ќе го уредат и издавањето на сертификат или друг вид документ како потврда за завршената обука, како и да го уреди времетраењето, односно времето на важење на таквиот документ.

Член 42

Безбедносен сертификат се издава на правно лице кое ги исполнува следниве услови:

- ▶ да е регистрирано во Република Северна Македонија,
- ▶ да постои оправдана потреба за пристап и ракување со класифицирани информации согласно со принципот „потребно е да знае“,
- ▶ да не му е изречена санкција-забрана за вршење на дејност,
- ▶ да има обезбедено услови за физичка безбедност, административна безбедност и/или безбедност на комуникациско-информациски системи, доколку тоа го бараат условите од класифицираниот договор,
- ▶ да има обезбедено безбедносен сертификат за офицерот за безбедност на класифицирани информации во правното лице,
- ▶ да е финансиски и економски стабилно и
- ▶ да не постојат безбедносни пречки за ракување со класифицирани информации што се утврдува со оперативна проверка.

Финансиската и економската стабилност од ставот 1 алинеја б на овој член се утврдува со следниве документи што не треба да бидат постари од шест месеци:

- ▶ извод од регистрацијата на дејноста,
- ▶ документ за бонитет од надлежен орган,
- ▶ доказ од надлежен орган дека не е отворена постапка за стечај или ликвидација,
- ▶ доказ од надлежен орган дека со пресуда не му е изречена мерка на безбедност- забрана на вршење на дејности,
- ▶ потврда од надлежен орган за платени даноци, придонеси и други јавни давачки.

Во член 42 законодавецот ги уредува условите за издавање безбедносен сертификат на правно лице. Притоа таксативно набројува дека: правното лице треба да е регистрирано во Република Северна Македонија, да постои оправдана потреба за пристап и ракување со класифицирани информации во согласност со принципот „потребно е да знае“, да не му е изречена санкција – забрана за вршење на дејност, да има обезбедено услови за физичка безбедност, административна безбедност и/

или безбедност на комуникациско-информациски системи доколку тоа го бараат условите од класифицираниот договор, да има обезбедено безбедносен сертификат за офицерот за безбедност на класифицирани информации во правното лице, да е финансиски и економски стабилно и да не постојат безбедносни пречки за ракување со класифицирани информации, што се утврдува со оперативна проверка. Тука е потребно да се нагласи дека исполнетоста на пропишаните услови од страна на правното лице, Дирекцијата ја проверува со свои експертски тимови, додека самата оперативна проверка ја спроведува надлежен орган, односно Агенцијата за национална безбедност.

Понатаму, законодавецот подетално ги уредува доказите со коишто се утврдува финансиската и економската стабилност на правното лице, односно документите што треба да се приложат кон барањето за безбедносен сертификат како доказ за финансиската и економската стабилност на правното лице и коишто не треба да бидат постари од шест месеци. Притоа, законодавецот предвидел дека правното лице треба да приложи извод од регистрацијата на дејноста, документ за бонитет од надлежен орган, доказ од надлежен орган дека не е отворена постапка за стечај или ликвидација, доказ од надлежен орган дека со пресуда не му е изречена мерка на безбедност – забрана на вршење дејност, како и потврда од надлежен орган за платени даноци, придонеси и други јавни давачки.

Член 43

Правното лице се смета за способно да обезбеди заштита на класифицирани информации доколку обезбеди услови за спроведување на мерките и активностите за заштита на класифицирани информации определени со овој закон.

Со одредбата од член 43, која е општа и упатувачка по својот карактер, законодавецот уредува дека правното лице се смета за способно да обезбеди заштита на класифицирани информации доколку ги обезбеди условите за спроведување на мерките и активностите за заштита на класифицирани информации определени со овој закон. Тоа подразбира исполнување на мерките и активностите од доменот на административната безбедност, безбедноста на лица корисници на класифицирани информации, физичката безбедност, индустриската безбедност и безбедноста на комуникациско-информациски системи, зависно од делокругот на работата и потребата и обемот на пристапот до класифицираните информации. Споменатите домени на безбедност се уредени во други одредби од овој закон.

ПОСТАПКИ ЗА ИЗДАВАЊЕ НА БЕЗБЕДНОСНИ СЕРТИФИКАТИ

Член 44

Исполнувањето на условите за издавање на безбедносен сертификат се утврдува преку безбедносна проверка.

Безбедносната проверка од ставот 1 на овој член се врши врз основа на претходна писмена согласност од физичкото или правното лице кое поднело барање за издавање на безбедносниот сертификат, којашто е составен дел на барањето од членот 39 став 3 од овој закон.

Ако физичкото или правното лице во текот на постапката писмено ја повлече

својата согласност за проверка, повторна постапка за безбедносна проверка не може да се спроведе пред истекот на една година од денот на повлекувањето на согласноста.

Во член 44 е уредено дека исполнувањето на условите за издавање на безбедносен сертификат се утврдува преку безбедносна проверка за којашто физичкото или правното лице кое поднело барање за издавање на безбедносниот сертификат претходно дава писмена согласност за спроведување. Ваквата согласност е логичен услов затоа што безбедносната проверка опфаќа дејствија кои длабоко навлегуваат во сферата на приватноста и опфаќаат и сензитивни лични податоци. Оттука, лицето има право во текот на постапката, да ја повлече согласноста. Но, тоа предизвикува и одредена консеквенција, имено, во случај ако физичкото или правното лице во текот на постапката писмено ја повлече својата согласност за проверка, законодавецот предвидел дека повторна постапка за безбедносна проверка не може да се спроведе пред истекот на една година од денот на повлекувањето на согласноста.

Член 45

Безбедносна проверка се спроведува пред издавање на безбедносен сертификат на правни и физички лица за пристап и ракување на класифицирани информации, со цел да се утврди постоење или непостоење на безбедносен ризик.

Безбедносната проверка започнува по поднесување на барањето од членот 39 став 3 од овој закон, до Дирекцијата.

Пополнетите податоци од безбедносниот прашалник претставуваат дел од содржината на безбедносната проверка.

Формата и содржината на обрасците на безбедносниот прашалник од ставот 1 на овој член ги пропишува директорот на Дирекцијата, а по претходна координација со надлежните служби кои се задолжени за реализација на оперативни безбедносните проверки.

Законодавецот подетално ја уредува безбедносната проверка во членот 45, при што предвидува дека истата се спроведува пред издавање на безбедносен сертификат на правни и физички лица за пристап и ракување на класифицирани информации, со цел да се утврди постоење или непостоење на безбедносен ризик, и почнува со самото доставување барање до Дирекцијата. Понатаму, законодавецот уредува дека дел од постапката за издавање безбедносен сертификат претставуваат пополнетите податоци од безбедносниот прашалник, чијашто форма и содржина ги пропишува директорот на Дирекцијата. Законодавецот предвидел да се пропише содржината и формата на обрасците на безбедносниот прашалник, но не прецизира за колку и какви обрасци станува збор. Врз основа на другите одредби од законот и досегашната практика, може да се заклучи дека се пропишуваат одделни обрасци за различните степени на класификација (зависно од барањето) и зависно од тоа дали се работи за физичко или правно лице.

Член 46

Пополнетиот прашалник за безбедносна проверка се означува со ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“.

Податоците од пополнетиот безбедносен прашалник од ставот 1 на овој член се користат за целите на проверката и со нив се постапува согласно со закон.

Во член 46 законодавецот предвидел дека пополнетиот прашалник за безбедносна проверка се означува со ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“ што подразбира дека прашалникот не може да биде достапен на јавноста и се користи само за службени потреби, со почитување на одредбите од Законот за заштита на личните податоци.²⁴ Со ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА“ се ограничува дистрибуцијата на безбедносниот прашалник и се укажува дека истиот ќе се користи само за целите за коишто е наменет, односно за потребите на безбедносната проверка. Во таа насока е и одредбата од вториот став на овој член со која се уредува дека податоците од пополнетиот безбедносен прашалник се користат за целите на проверката и со нив се постапува во согласност со закон. Тоа значи дека, на пример, личните податоци се штитат во согласност со прописите за заштита на лични податоци итн.

Член 47

За користење на класифицирани информации означени со степенот „ИНТЕРНО“ не се врши безбедносна проверка и не се издава безбедносен сертификат.

Физичкото или одговорното лице во правното лице се информира за обврската за заштита на класифицираните информации од ставот 1 на овој член што му се дадени на увид, односно ракување.

Во член 47 законодавецот предвидел дека за користење класифицирани информации означени со степенот „ИНТЕРНО“ не се врши безбедносна проверка и не се издава безбедносен сертификат, туку физичкото лице или одговорното лице во правното лице се информира за обврската за заштита на класифицираните информации што им се дадени на увид, односно на ракување. Тоа подразбира т.н. безбедносен брифинг што го спроведува овластено лице во органот, односно офицерот за безбедност на класифицирани информации со којшто лицето се информира за безбедносните мерки и процедури и неговите обврски при ракувањето и чувањето на класифицираните информации. Најмалку еднаш годишно, а по потреба и почесто, од страна на офицерот за безбедност на класифицирани информации, корисниците на класифицирани информации повторно се информираат за нивните обврски кои произлегуваат од Законот за класифицирани информации(*). По првичното и повторното запознавање со нивните обврски, корисниците на класифицираните информации потпишуваат изјава со која потврдуваат дека целосно ги разбрале одредбите од Законот.

Доколку се повредат правилата за ракување и заштита на овие информации, лицето треба да биде предмет на соодветна одговорност и санкционирање, зависно од тоа дали се работи за полесна повреда, прекршок или пак, друго незаконско постапување или злоупотреба извршена со умисла која би се третираше како кривично дело. Иако се работи за најнизок степен на класификација, треба да се

²⁴ Закон за заштита на личните податоци, „Службен весник на Република Северна Македонија“ број 42/20.

истакне дека и така класифицираните информации треба да се предмет на заштита и со нив треба да се ракува со сериозност и одговорност.

Член 48

Во зависност од степенот на класифицираната информација за која е поднесено барање за издавање безбедносен сертификат за физичко лице, се врши безбедносна проверка соодветна на степенот на класифицираната информација и тоа:

- а) од прв степен за информација класифицирана „ДОВЕРЛИВО“;
- б) од втор степен за информација класифицирана „СТРОГО ДОВЕРЛИВО“ и
- в) од трет степен за информација класифицирана „ДРЖАВНА ТАЈНА“.

Во член 48 законодавецот определува три степени на безбедносна проверка за физичко лице кои се соодветни на степенот на класифицираната информација за која е поднесено барање за издавање безбедносен сертификат. Како резултат на тоа, законодавецот предвидува: безбедносна проверка од прв степен за информација класифицирана со степен „ДОВЕРЛИВО“, безбедносна проверка од втор степен за информација класифицирана со степен „СТРОГО ДОВЕРЛИВО“ и безбедносна проверка од трет степен за информација класифицирана со степен „ДРЖАВНА ТАЈНА“.

Различните степени на безбедносна проверка подетално се уредени во следните членови од законот.

Член 49

Со безбедносна проверка од прв степен се проверува:

- ▶ идентитетот на лицето (врз основа на приложена писмена документација) и оперативната проверка на податоците за лицето од надлежен орган,
- ▶ возраста од најмалку 18 години,
- ▶ државјанството на Република Северна Македонија,
- ▶ деловната способност на лицето (врз основа на уверение од надлежен орган) и
- ▶ постоење на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето (утврдени со спроведување на оперативна проверка од страна на надлежен орган).

Во однос на безбедносната проверка од прв степен,²⁵ во член 49 законодавецот предвидел дека се проверуваат: идентитетот на лицето (врз основа на приложена писмена документација) и оперативната проверка на податоците за лицето од надлежен орган, возраста од најмалку 18 години, државјанството на Република Северна Македонија, деловната способност на лицето (врз основа на уверение од надлежен орган) и постоење на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето (утврдени со спроведување на оперативна проверка од страна на надлежен орган).

Аналогно на проверката на деловната способност на лицето врз основа на уверение од надлежен орган, законодавецот тука не предвидел проверка на

²⁵ Ова е подетално уредено во подзаконски акт, односно во Уредбата за безбедност на лица –корисници на класифицирани информации („Службен весник на Република Македонија“ број 82/04). Во тек е постапка за донесување нова Уредба за безбедност на лица –корисници на класифицирани информации.

неосудуваноста на лицето врз основа на уверението за неосудуваност, не постаро од шест месеци, чиешто поседување како услов за добивање безбедносен сертификат е пропишано во член 41 став 1 алинеја 9. Но, секако треба да се има предвид дека неосудуваноста на лицето се проверува и во текот на оперативната проверка.

Член 50

Со безбедносна проверка од втор степен се проверува:

- ▶ идентитетот на лицето (врз основа на приложена писмена документација и оперативна проверка на податоците за лицето од страна на надлежен орган),
- ▶ возраста од најмалку 18 години,
- ▶ државјанството на Република Северна Македонија,
- ▶ деловната способност на лицето (врз основа на уверение од надлежен орган) и
- ▶ постоењето на безбедносен ризик или пречки за пристап и ракување со класифицирани информации кај лицето - барател на безбедносен сертификат и кај лицата наведени во безбедносниот прашалник (со спроведување на оперативната проверка од страна на надлежен орган),
- ▶ лицето да нема државјанство на друга држава која не е членка на НАТО.

Во член 50 законодавецот, имајќи ја предвид Одлуката на Уставниот суд на Република Македонија од 20 април 2011 година, предвидел поширок опсег на безбедносната проверка од втор степен со што покрај проверката на лицето-барател на безбедносен сертификат, оперативната проверка вклучува и проверка на лицата наведени во безбедносниот прашалник.²⁶ Така, со безбедносната проверка од втор степен се проверува: идентитетот на лицето (врз основа на приложена писмена документација) и оперативната проверка на податоците за лицето од надлежен орган, возраста од најмалку 18 години, државјанството на Република Северна Македонија, деловната способност на лицето (врз основа на уверение од надлежен орган), постоењето на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето (утврдени со спроведување на оперативна проверка од страна на надлежен орган) и лицето да нема државјанство на друга држава која не е членка на НАТО, што исто така се проверува со оперативната проверка.

И во овој член законодавецот не предвидел безбедносноста проверка да вклучи проверка и на неосудуваноста на лицето врз основа на уверението за неосудуваност, не постаро од шест месеци, чиешто поседување како услов за добивање безбедносен сертификат е пропишано во член 41 став 1 алинеја 9, како што ја предвидел проверката на деловната способност на лицето врз основа на

²⁶ По поднесена иницијатива, на седницата одржана на 20 април 2012 година, Уставниот суд на Република Македонија донесе Одлука (У.бр.209/2010) („Службен весник на Република Македонија“ број 61/11) за укинување на член 7 став 2 алинеи 2 и 3 од Уредбата за безбедност на лица корисници на класифицирани информации („Службен весник на Република Македонија“ број 82/04) којшто содржеше одредби дека постоењето на безбедносен ризик за лицето за кое се бара издавање на соодветен безбедносен сертификат, се утврдува врз основа на спроведена оперативна безбедносна проверка за кандидатот, неговите деца и брачниот другар, за проверки од втор степен, а за проверките од трет степен, врз основа на спроведена оперативна безбедносна проверка за кандидатот, неговите деца, брачниот другар, родителите и за другите лица со кои тој живее во иста семејна заедница. Во Образложението на Уставниот суд за таквата Одлука стои дека во отсуство на законска регулатива која утврдува дека оперативната безбедносна проверка треба да ги опфати и наведените лица, истото не може да се регулира со подзаконски акт којшто го донесува Владата. Имајќи го ова предвид при изработката на новиот текст на Законот за класифицирани информации, законодавецот предвидел со оперативната проверка од втор степен да бидат опфатени и лицата коишто кандидатот за безбедносен сертификат ги навел во безбедносниот прашалник, како генерален поим кој ги вклучува родителите, брачниот другар и членовите на потесното семејството, како и лицата постари од 18 години што живеат во истото семејство и родителите на брачниот другар за коишто постојат посебни рубрики во безбедносниот прашалник.

уверение од надлежен орган. Но, како што наведовме и во коментарот на член 49, неосудуваноста на лицето се проверува во текот на оперативната проверка.

Член 51

Со безбедносна проверка од трет степен се проверува:

- ▶ идентитетот на лицето (врз основа на приложена писмена документација и оперативна проверка на податоците за лицето од страна на надлежен орган),
- ▶ возраста од најмалку 21 година,
- ▶ државјанството на Република Северна Македонија,
- ▶ деловната способност на лицето (врз основа на уверение од надлежен орган) и
- ▶ постоењето на безбедносен ризик или пречки за пристап и ракување со класифицирани информации кај лицето барател на безбедносен сертификат и кај лицата наведени во безбедносниот прашалник (со спроведување на оперативната проверка од страна на надлежен орган),
- ▶ утврдување на способноста на лицето за ракување со класифицирани информации преку реализација на интервју од страна на овластено лице од надлежните служби кои ги вршат оперативни безбедносните проверки,
- ▶ лицето да нема државјанство на друга држава.

Опсегот на безбедносната проверка од трет степен законодавецот го предвидел во член 51. Притоа утврдил дека се проверува: идентитетот на лицето – врз основа на приложена писмена документација и оперативната проверка на податоците за лицето од надлежен орган, возраста од најмалку 21 година, државјанството на Република Северна Македонија, деловната способност на лицето барател на безбедносен сертификат и кај лицата наведени во безбедносниот прашалник²⁷ (врз основа на уверение од надлежен орган), постоењето на безбедносни пречки за пристап и ракување со класифицирани информации кај лицето (утврдени со спроведување на оперативна проверка од страна на надлежен орган), утврдување на способноста на лицето за ракување со класифицирани информации преку реализација на интервју од страна на овластено лице од надлежните служби кои ги вршат оперативни безбедносните проверки и лицето да нема државјанство на друга држава.

Утврдувањето на способноста на лицето за ракување со класифицирани информации преку реализација на интервју од страна на надлежните служби е новина воведена со овој закон. Претходната практика вклучуваше разговор/интервју со лицето – барател на безбедносен сертификат со степен „ДРЖАВНА ТАЈНА“ од страна на директорот на Дирекцијата за безбедност на класифицирани информации по оценета потреба доколку треба да се разјаснат одредени сонанија добиени со оперативната проверка за лицето.

Во поглед на неосудуваноста, таа се проверува во текот на оперативната проверка, а законодавецот тука не предвидел проверка на неосудуваноста на лицето врз основа на уверението за неосудуваност, не постаро од шест месеци, што самото лице го доставува и чиешто поседување е услов за добивање безбедносен сертификат согласно член 41 став 1 алинеја 9.

²⁷ Во контекст на Одлуката на Уставниот суд – У.бр.209/2010 (в. претходна фуснота), законодавецот предвидел со оперативната проверка од трет степен да бидат опфатени и лицата коишто кандидатот за безбедносен сертификат ги навел во безбедносниот прашалник.

Член 52

На барање на Дирекцијата, оперативните проверки за постоење на безбедносни пречки за пристап и ракување со класифицирани информации ги вршат:

- ▶ Агенцијата за национална безбедност за сите физички и правни лица, освен за лицата утврдени во алинејата 2 на овој став и
- ▶ надлежните служби на Министерството за одбрана за сите вработени во Министерството за одбрана и Армијата на Република Северна Македонија.

Во членот 52 се идентификувани безбедносните служби коишто на барање од Дирекцијата ги вршат оперативните проверки за постоење на безбедносни пречки за пристап и ракување со класифицирани информации.

Притоа е уредено дека Агенцијата за национална безбедност ги врши оперативните проверки за сите физички и правни лица, освен за лицата вработени во Министерството за одбрана и Армијата на Република Северна Македонија, за коишто оперативните проверки ги вршат надлежните служби на Министерството за одбрана за сите вработени во Министерството за одбрана и Армијата на Република Северна Македонија.

Во случај на проверка на лица вработени во Агенцијата за разузнавање или дипломати, односно лица кои престојувале и работеле во странство, Агенцијата за разузнавање може да достави информации за засегнатите лица до надлежните служби при што тие информации ќе бидат земени предвид во рамки на вкупната безбедносна проверка.²⁸

Член 53

Постапката за спроведување на безбедносна проверка трае најмногу до:

- ▶ четири месеци за безбедносната проверка од прв степен за физички лица,
- ▶ шест месеци за безбедносната проверка од втор степен за физички лица,
- ▶ шест месеци за безбедносната проверка од трет степен за физички лица и
- ▶ шест месеци за безбедносна проверка за правно лице.

По исклучок од ставот 1 на овој член, постапката за безбедносна проверка од трет степен за лицата назначени во надзорните тела кои вршат надзор над спроведувањето на мерките за следење на комуникациите, како и за ангажираните акредитирани национални и меѓународни технички експерти од тие тела, согласно со Законот за следење на комуникациите, трае еден месец од денот на поднесување на барањето.

По исклучок од ставот 1 на овој член, постапката за безбедносна проверка од втор степен за лицата пред засновање на работен однос во Оперативно-техничката агенција, согласно со Законот за Оперативно-техничка агенција, трае еден месец од денот на поднесување на барањето.

²⁸ Закон за Агенцијата за разузнавање, „Службен весник на Република Северна Македонија“ број 21/21, член 83.

Во членот 53 законодавецот ги предвидел роковите за постапката на безбедносна проверка и притоа утврдил дека постапката за безбедносна проверка од прв степен за физички лица трае најмногу до четири месеци, додека истата трае најмногу до шест месеци за безбедносната проверка од втор степен за физички лица, за безбедносната проверка од трет степен за физички лица и за безбедносната проверка за правно лице.

Законодавецот предвидел и исклучоци, па така утврдил дека рокот на постапката за безбедносната проверка од трет степен за лицата назначени во надзорните тела кои вршат надзор над спроведувањето на мерките за следење на комуникациите, како и за ангажираните акредитирани национални и меѓународни технички експерти од тие тела, во согласност со Законот за следење на комуникациите, трае еден месец од денот на поднесување на барањето. Втор исклучок е и постапката за безбедносна проверка од втор степен за лицата пред засновање на работен однос во Оперативно-техничката агенција, согласно со Законот за Оперативно-техничката агенција,²⁹ за којашто законодавецот утврдил дека трае еден месец од денот на поднесување на барањето. Во исклучоците, законодавецот не ја предвидел постапката за безбедносна проверка од трет степен за вработените во Оперативно-техничката агенција.

Се работи за предвидување на побрзи постапки (спроведени во пократки рокови) за одредени категории лица каде што е потребно побрзо да биде завршена процедурата, односно отсуството на вакво решение би можело да доведе до блокирање на работата во овие исклучително важни сфери.

²⁹ Закон за Оперативно-техничка агенција, „Службен весник на Република Македонија“ број 71/18 и „Службен весник на Република Северна Македонија“ број 98/19, член 17, ставови 4 и 6.

ВРЕМЕТРАЕЊЕ НА БЕЗБЕДНОСНИТЕ СЕРТИФИКАТИ

Член 54

Безбедносниот сертификат издаден за информација класифицирана со степен „ДРЖАВНА ТАЈНА“ важи пет години.

Безбедносниот сертификат издаден за информација класифицирана со степен „СТРОГО ДОВЕРЛИВО“ важи десет години.

Безбедносниот сертификат издаден за информација класифицирана со степен „ДОВЕРЛИВО“ важи десет години.

Содржината и формата на образецот на безбедносните сертификати од ставовите 1, 2 и 3 на овој член ги пропишува директорот на Дирекцијата.

Во членот 54 законодавецот ја предвидел важноста на безбедносните сертификати. Притоа утврдил различно времетраење на безбедносните сертификати издадени за различни степени на класификација. Така, безбедносниот сертификат издаден за информација класифицирана со степен „ДРЖАВНА ТАЈНА“ важи пет години, а за информација класифицирана со степен „СТРОГО ДОВЕРЛИВО“ и со степен „ДОВЕРЛИВО“ важи десет години. Со одредба во четвртиот став на овој член, законодавецот предвидел содржината и формата на образецот на безбедносните сертификати да ги пропише директорот на Дирекцијата.

Законодавецот не предвидел важност на безбедносниот сертификат во времетраење на некоја активност или вршење служба, на пример заминување во мисија и сл. Тоа е од причина што во таков случај се почитува принципот „потребно е да знае“, па иако лицето добило безбедносен сертификат со важност од 10 години, по престанокот на потребата за истиот, односно по завршување на активната или на мисијата за чијашто цел бил издаден, важноста на безбедносниот сертификат ќе истече согласно член 60 став 1 алинеја 2 од овој закон.

Член 55

Корисникот на класифицирани информации е должен да поднесе ново барање за продолжување на важноста на безбедносниот сертификат најдоцна шест месеци пред денот на истекот на неговата важност.

За физичкото и правното лице кое поднесува барање за продолжување на важноста на безбедносниот сертификат, се врши повторна безбедносна проверка согласно со овој закон соодветна на степенот на класифицираните информации што му се отстапуваат на користење.

Во членот 55 законодавецот ја уредил обврската на корисникот на класифицирани информации да поднесе ново барање за продолжување на важноста на безбедносниот сертификат најдоцна шест месеци пред денот на истекот на неговата важност. Целта на ваквата обврска е да се спречи своевиден вакуум кој би настанал доколку лицето чека да истече важноста на безбедносниот сертификат, пред да побара нејзино продолжување, имајќи предвид, пред сè дека Законот не предвидува можност за издавање привремен безбедносен сертификат.

Со оглед на фактот што продолжувањето претпоставува спроведување на нова соодветна безбедносна проверка, јасно е дека тој процес треба порано да почне. Оттука, овој рок од шест месеци е усогласен со роковите за времетраење на постапката за безбедносна проверка дефинирани погоре во членот 53.

Во вториот став на овој член законодавецот укажува дека со барањето за продолжување на важноста на безбедносниот сертификат, за физичкото и правното лице кое го поднесува барањето се врши повторна безбедносна проверка соодветна на степенот на класифицираните информации што му се отстапуваат на користење. Еднаш спроведената безбедносна проверка не значи дека се добиени податоци кои не се менуваат, па оттука, секое лице кое има пристап до класифицирани информации, би требало периодично да е предмет на соодветна контрола (а по соодветни индиции и почесто), па законодавецот предвидел обврска за повторна безбедносна проверка при секое барање за продолжување на важноста на сертификатот.

Член 56

Ако се утврди дека физичкото или правното лице не постапува со класифицираните информации согласно со овој закон или повеќе не е исполнет некој од условите врз основа на кои е издаден безбедносниот сертификат, директорот на Дирекцијата донесува решение за одземање на безбедносниот сертификат и пред истекот на неговото важење.

Во решението од ставот 1 на овој член не се дава образложение за причините за одземање на безбедносниот сертификат.

Против решението од ставот 1 на овој член за одземање на безбедносниот сертификат и пред истекот на неговата важност, лицето има право на жалба до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен во однос на постапката за одземање на безбедносниот сертификат.

Во член 56 е уредена постапката за одземање на безбедносниот сертификат и пред истекот на неговото важење од страна на директорот на Дирекцијата во случај ако се утврди дека физичкото или правното лице не постапува со класифицираните информации во согласност со Законот или повеќе не е исполнет некој од условите врз основа на кои е издаден безбедносниот сертификат. Тоа го утврдува офицерот за безбедност на класифицирани информации во органот во кој е вработено физичкото лице или инспекторот за безбедност на класифицирани информации, кој може да изврши надзор врз работата на физичкото, односно правното лице со класифицираните информации. Законодавецот предвидел за тоа директорот на Дирекцијата да донесе решение за одземање на безбедносниот сертификат во коешто не се дава образложение за причините за одземање на безбедносниот сертификат.³⁰ Причините заради кои не се дава образложение, законодавецот веројатно ги гледа во можноста со самото образложение да се откријат информации

³⁰ По поднесена иницијатива, на седницата одржана на 21 септември 2005 година, Уставниот суд на Република Македонија донесе Решение (У.бр.213/2004) дека не се поведува постапка за оценување на уставноста на член 54 став 2 и член 55 став 2 од Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/04) коишто содржеа одредби дека не се дава образложение за причините за престанокот на важноста на безбедносниот сертификат. Во образложението на Уставниот суд за таквото решение стои дека „со оглед на тоа што безбедносниот сертификат не претставува класичен управен акт со кој се решаваат индивидуалните права на граѓаните, туку за право на пристап и користење на класифицирани информации за пристап до една специфична материја – област како што е безбедноста на одбраната на државата, Судот утврди дека не може да се постави прашањето за согласноста на оспорените законски одредби со Уставот на Република Македонија“.

кои би требало да останат тајни во тој момент.

Сепак, во третиот став од членот законодавецот го уредил правото на лицето да го обжали таквото решение пред Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен во однос на постапката за одземање на безбедносниот сертификат. Тоа подразбира дека Државната комисија првенствено го разгледува начинот на спроведување на постапката за неговото одземање, и по правило, не навлегува во причините за одземање на сертификатот. Сепак, доколку членовите на Комисијата дојдат до сознание за содржината на некоја класифицирана информација во текот на самата постапка, обврзани се за чување во тајност на таквата информација во согласност со член 104 од овој закон.

Член 57

Директорот на Дирекцијата може да донесе решение за одбивање на барањето за издавање на безбедносен сертификат за физички и правни лица ако не се исполнети условите од овој закон.

Во решението од ставот 1 на овој член не се дава образложение за причините за одбивање на барањето за издавање на безбедносен сертификат.

Против решението од ставот 1 на овој член лицето чие барање е одбиено може да поднесе жалба до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен во однос на постапката за издавање на безбедносниот сертификат.

Во член 57 законодавецот ја уредил и можноста директорот на Дирекцијата да може да донесе решение за одбивање на барањето за издавање на безбедносен сертификат за физички и правни лица ако не се исполнети условите што се пропишани со овој закон. И во тоа решение не е предвидено да се даде образложение за одбивањето на барањето, а лицето има право истото да го обжали пред Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен во однос на постапката за издавање на безбедносниот сертификат.

Одбивањето на барањето за издавање на безбедносен сертификат, како што може да се заклучи, иако е необразложено, не е дискрециона одлука без основа, односно тоа е резултат на неисполнетост на законските услови, но најчесто причините за одбивање во конкретен случај треба да останат тајни зашто, на пример, се предмет на истрага или претставуваат детектирани ризици или закани кои треба да бидат соодветно третирани, па оттука и потребата да не се изнесуваат во образложение.

Член 58

Жалбата од членот 56 став 3 и членот 57 став 3 од овој закон се поднесува во рок од 15 дена од денот на приемот на решението, до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен.

Решението по жалбата од ставот 1 на овој член, донесено од Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен, е конечно.

Во првиот став на член 58 законодавецот го утврдува рокот од 15 дена за поднесување на жалбата до Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен, додека во вториот став уредува дека решението што го донесува Државната комисија за одлучување во управна постапка и постапка од работен однос во втор степен е конечно.

Гореспоменатата Комисија е основана со Законот за основање на Државна комисија за одлучување во управна постапка и постапка од работен однос во втор степен.³¹ Против нејзиното решение, во согласност со член 10 став 1 од Законот за основање на Државна комисија за одлучување во управна постапка и постапка од работен однос во втор степен, може да се покрене управен спор пред надлежен суд.

Член 59

Барање за повторно издавање на безбедносен сертификат со ист или повисок степен може да се поднесе:

- ▶ по истекот на една година од правосилноста или конечноста на решението за одбивање на барањето за издавање на безбедносен сертификат и
- ▶ по истекот на три години од правосилноста или конечноста на решението за одземање на безбедносниот сертификат пред истекот на важноста.
- ▶ При повторно издавање на безбедносен сертификат за лицата од ставот 1 на овој член, безбедносниот сертификат важи една година.

Во член 59 законодавецот ги дефинира роковите кога може да се поднесе барање за повторно издавање на безбедносен сертификат со ист или повисок степен кога едно лице било одбиено во поглед на барањето да му биде издаден безбедносен сертификат или кога имало добиено сертификат, но тој му бил одземен. Притоа, зависно од причината поради која е донесено „негативното“ решение, законодавецот предвидел различни рокови, па така утврдува дека истото може да се поднесе по истекот на една година од правосилноста или конечноста на решението за одбивање на барањето за издавање на безбедносен сертификат и по истекот на три години од правосилноста или конечноста на решението за одземање на безбедносниот сертификат пред истекот на важноста. Причината за утврдување различен временски рок кога лицето може да поднесе барање за повторно издавање на безбедносен сертификат со ист или повисок степен лежи во поголемата сериозност на причините заради коишто се донесува решението за одземање на безбедносниот сертификат.

Во случај на позитивен одговор, предвидено е издадениот сертификат да има важност од една година. Ова од причини што иако во моментот е утврдено дека се исполнети условите за издавање на безбедносен сертификат, причините заради кои лицето претходно било одбиено или му бил одземен сертификатот остануваат да „висат“ во воздухот како индиција дека тоа лице може да претставува своевиден потенцијален ризик, па важноста на сертификатот е пократка од онаа според основното решение, што значи повторна безбедносна проверка доколку по истекот на важноста на тој сертификат од една година, лицето побара нејзино продолжување. Имајќи го предвид фактот дека лицето треба да побара продолжување барем 6 месеци пред истекот на важноста, тоа значи дека следната безбедносна проверка би започнала веќе по шест месеци од издавањето на сертификатот од член 59, став 2.

³¹ Закон за основање на Државна комисија за одлучување во управна постапка и постапка од работен однос во втор степен, „Службен весник на Република Македонија“ број 51/11, 148/13, 41/14, 130/14, 53/16 и 11/18.

Член 60

Безбедносниот сертификат престанува да важи со истекот на рокот на неговата важност, како и во случај на:

- ▶ престанок на функцијата на лицата од членот 40 од овој закон,
- ▶ престанок на потребата за пристап до класифицирани информации согласно со принципот „потребно е да знае“,
- ▶ намалена ментална способност за постапување со класифицирани информации утврдена од надлежна медицинска установа,
- ▶ смрт на физичкото лице или престанок на правното лице.

Во случаите од ставот 1 алинеи 1, 2, 3 и 4 на овој член, офицерот за безбедност на класифицирани информации ги враќа безбедносните сертификати за физички и/или правни лица во Дирекцијата во рок од 15 дена од констатирањето на истите.

Во член 60 е уредено кога престанува да важи безбедносниот сертификат. Притоа, покрај главната основа за престанување на важност, а тоа е по истекување на предвидениот рок, законодавецот предвидел уште неколку случаи.

Првиот се однесува на лицата коишто во согласност со Законот добиваат безбедносен сертификат за пристап и користење на класифицирани информации од сите степени, без претходна безбедносна проверка, заради непречено вршење на функцијата од денот на изборот до крајот на мандатот (член 40). Така, по завршување на нивната функција, односно на крајот на мандатот престанува да важи и безбедносниот сертификат што им бил издаден за вршење на должностите.

Вториот случај се однесува на престанок на потребата за пристап до класифицирани информации во согласност со принципот „потребно е да знае“. Тоа подразбира дека лицето кое во даден момент имало потреба за пристап до класифицирани информации заради извршување работни задачи за кои бил потребен пристап до класифицирани информации, во случај на негово прераспореѓување на работно место за коешто не е потребен пристап до класифицирани информации повеќе нема потреба од безбедносен сертификат и со тоа престанува да важи безбедносниот сертификат кога за тоа лице бил исполнет принципот „потребно е да знае“. Истото важи и кога лицето преминува на работна позиција од една во друга институција бидејќи и во тој случај може да престане да важи принципот „потребно е да знае“ врз основа на кој бил издаден безбедносниот сертификат.

Законодавецот предвидел важноста на безбедносниот сертификат да престане и во случај на намалена ментална способност за постапување со класифицирани информации утврдена од надлежна медицинска установа. Овој случај не е подетално уреден во Законот, кој не содржи одредби со кои би се уредил начинот на утврдување на намалената способност кај лицето коешто поседува важечки безбедносен сертификат или постапката за добивање мислење од надлежна медицинска установа. Дадената одредба од Законот претпоставува дека во случај на сознание за постоење безбедносен ризик по класифицираните информации заради намалена ментална способност на лицето што ракува со нив потврдена од надлежна медицинска институција, издадениот безбедносен сертификат ќе престане да важи.

Последниот случај во којшто е предвидено да престане да важи безбедносниот сертификат е смрт на физичкото лице или престанок на правното лице.

Во последниот став од овој член е уредена обврската на офицерот за безбедност на класифицирани информации да ги врати безбедносните сертификати за физички и/или правни лица во Дирекцијата во рок од 15 дена од констатирањето на престанокот на важноста на истите.

Член 61

Дозволата за пристап до класифицирани информации престанува да важи:

- ▶ со истекот на рокот на важноста наведен во дозволата,
- ▶ со извршување на задачата за која била издадена,
- ▶ ако потребата од издавањето на дозволата престанала да постои или е изменета и
- ▶ ако се утврди дека правното и физичкото лице не постапува со класифицираните информации согласно со закон.

Во член 61 е уреден престанокот на важноста на дозволата за пристап до класифицирани информации, при што законодавецот предвидел истата да престане да важи со истекот на рокот на важноста наведен во дозволата, со извршување на задачата за која била издадена, во случај ако потребата од издавањето на дозволата престанала да постои или е изменета и ако се утврди дека правното и физичкото лице не постапуваат со класифицираните информации во согласност со Законот. Всушност, преку инспекциски надзор од страна на инспекторот за безбедност на класифицирани информации, се утврдува дека правното и физичкото лице не постапуваат со класифицираните информации во согласност со Законот.

Дозвола за пристап до класифицирани информации, всушност, во согласност со член 6, став 1, алинеја 10, е документ со кој се потврдува дека странското физичко или правно лице има безбедносен сертификат издаден во матичната држава и има право на пристап и користење на класифицирани информации во Република Северна Македонија, па врз основа на овој член (61), посредно доаѓаме до сознание дека таа се издава на странски лица на кои истата им е потребна, односно има потреба тие да имаат пристап до класифицирани информации во нашата држава, односно тоа е поврзано со некаква задача и сл. Оттука, престанокот на постоење на ваквите основи, како и непостапувањето со класифицираните информации во согласност со Законот е основа за престанок на важноста на дозволата за пристап.

Со престанок на важноста на дозволата за пристап не престанува важноста на безбедносниот сертификат издаден во матичната држава, но тој сам по себе не е доволен за тоа странското физичко или правно лице да има пристап до класифицирани информации, така што дозволата за пристап претставува *conditio sine qua non* („услов без кој не се може“).

Член 62

Обврската за заштита на тајноста на класифицираните информации продолжува и по истекот на важноста на безбедносниот сертификат.

Во член 62 е уредена обврската за заштита на тајноста на класифицираните информации и по истекот на важноста на безбедносниот сертификат. Оваа одредба подразбира дека корисникот на класифицирани информации има обврска истите да ги заштитува и по престанок на неговата потреба за пристап до класифицираните информации во согласност со принципот „потребно е да знае“, односно сите сознанија во врска со нив да ги чува како тајна.

Повредата на оваа обврска зависно од околностите може да претставува и одредено кривично дело.

Член 63

За потребите на судска постапка или постапка пред друг надлежен орган во која се користат класифицирани информации, субјектите во постапката е потребно да поседуваат безбедносен сертификат.

Постапката од ставот 1 на овој член се води во присуство на лицето за чиешто права, обврски или одговорност се одлучува во нејзини рамки и кога лицето нема безбедносен сертификат.

Лицето од ставот 2 на овој член е одговорно за исполнување на обврската за заштита на класифицираните информации согласно со овој закон.

Во постапката од ставот 1 на овој член, јавноста е исклучена.

Во случај кога создавачот на класифицираната информација не ја доставил класифицираната информација во постапката од ставот 1 на овој член, судот односно надлежниот орган е должен во рок од 15 дена од приемот на класифицираната информација да го информира создавачот и Дирекцијата за нејзиното користење во постапката.

Во член 63 е уредена потребата за поседување безбедносен сертификат од страна на субјектите/лицата коишто учествуваат во судска постапка или постапка пред друг надлежен орган во која се користат класифицирани информации.

Со цел почитување на правото на одбрана, коешто е едно од основните права на обвинетиот и тоа е уставно загарантиран принцип (член 12 од Уставот), законодавецот предвидел постапката да се води пред лицето за чија што одговорност се одлучува во нејзини рамки и кога лицето нема безбедносен сертификат. Но, во делот на судските постапки ова не е ограничено само на кривичната постапка, туку се однесува на каква било судска постапка каде што се одлучува и за права и обврски на едно лице (на пример, граѓански спор, работен спор), а не само за одговорност. Дополнително, опфатени се и други постапки што се водат пред надлежни органи. Користењето на класифицирани информации во каква било постапка не треба *per se* да е основа за нејзина декласификација, туку нејзината заштита законодавецот и натаму ја обезбедува со предвидувањето на одговорност за лицето во поглед на исполнување на обврската за заштита на класифицираните информации во согласност со овој закон. Тоа значи дека сите субјекти и лица што поседуваат безбедносен сертификат, како и лицата што се дел од постапката, а не поседуваат таков сертификат, врз основа на одредбите од овој закон се обврзани на заштита на класифицираните информации, односно на нивната тајност.

Заради остварување на претходно стипулираната заштита на класифицираните информации коишто се користат во различни судски или други постапки пред надлежни државни органи, во четвртиот став законодавецот уредил дека јавноста е исклучена во постапките во кои се користат класифицирани информации, со цел да се ограничи пристапот до класифицираните информации од страна на неовластени лица, односно поширок круг на лица.

Со цел да ја уреди ситуацијата кога создавачот на класифицираната

информација не ја доставил класифицираната информација во постапката, законодавецот предвидел судот, односно надлежниот орган да има должност во рок од 15 дена од приемот на класифицираната информација да го информира создавачот и Дирекцијата за безбедност на класифицирани информации за нејзиното користење во постапката.

Прашањето за користење класифицирани информации во судска постапка или постапка пред друг надлежен орган за прв пат се уредува во овој закон, иако и членот 354 од Законот за кривичната постапка предвидува можност за исклучување на јавноста, меѓу другото и заради чување на „државна, воена, службена или важна деловна тајна“.³² Како што може да забележиме, во Законот за кривичната постапка сè уште се користи стара терминологија, иако уште од 2004 година со Законот за класифицирани информации се предвидени четирите степени на класификација „државна тајна“, „строго доверливо“, „доверливо“ и „интерно“. Несомнено е потребно да се усогласат ваквите решенија и да се обезбеди конзистентност на релевантното законодавство.

Како што наведовме и погоре во овој коментар, честа е појавата на доделување на степен на класификација на докази обезбедени со употреба на посебни истражни мерки (ПИМ). Тие потоа најчесто се декласифицираат и се обележуваат со ознаката „ЗА ОГРАНИЧЕНА УПОТРЕБА (судска постапка)“.

Уште еднаш нагласуваме дека доколку има потреба од натамошна заштита на информацијата, таа нема потреба да се декласифицира, туку може како таква (класифицирана) да биде дел од постапката со исклучување на јавноста.

Доколку создавачот на информацијата смета дека треба да ја декласифицира, тоа првенствено значи дека таа ќе се употребува во постапка каде јавноста не е исклучена. Оттука е јасно дека за овие прашања се потребни дискусии и обуки во кои ќе бидат вклучени сите релевантни субјекти. Не треба да се заборави дека класифицирањето на ПИ-мерките (особено со највисоките степени „ДРЖАВНА ТАЈНА“ или „СТРОГО ДОВЕРЛИВО“) подразбира и исполнување на строги услови за заштита од секаков вид, вклучувајќи и криптографска заштита, доколку информацијата се пренесува електронски, строги правила за копии, репродукции итн. Создавачите на класифицирани информации треба да ги имаат предвид сите законски услови, а се препорачува и да се земат предвид и поконкретните насоки и примери дадени во Водичот за одредување на степенот на класификација на информациите на Дирекцијата за безбедност за класифицирани информации, особено ако создавачот има дилеми околу степенот на класификација кој треба да го одреди и консеквенциите кои произлегуваат од тоа.

Член 64

Дирекцијата води евиденција за издадените безбедносни сертификати и за пополнетите безбедносни прашалници.

Дирекцијата води посебна евиденција за издадените дозволи за пристап до класифицирани информации во Република Северна Македонија.

Содржината, формата и начинот на водење на евиденциите од ставовите 1 и 2 на овој член, ги пропишува директорот на Дирекцијата.

³² Закон за кривичната постапка, „Службен весник на Република Македонија“, број 150/10, 100/12, 142/16 и 198/18.

Во член 64 е уредена обврската на Дирекцијата за безбедност на класифицирани информации да води евиденција за издадените безбедносни сертификати и за пополнетите безбедносни прашалници, како и посебна евиденција за издадените дозволи за пристап до класифицирани информации во Република Северна Македонија. Дозволите за пристап до класифицирани информации се предмет на посебна евиденција бидејќи тие се издаваат на странски физички или правни лица кои веќе поседуваат безбедносен сертификат од матичната држава.

Законодавецот предвидел содржината, формата и начинот на водење на таквите евиденции да ги пропише директорот на Дирекцијата со подзаконски акт.

ГЛАВА ЧЕТВРТА

ОРГАНИ ЗА ЗАШТИТА НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

ОФИЦЕР ЗА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 65

Органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други правни лица, се должни да создадат услови неопходни за заштита на класифицирани информации и да преземат мерки за елиминирање на негативните последици ако дојде до откривање на класифицираните информации.

За ефикасно и координирано извршување на правата и обврските кои се однесуваат на класифицираните информации, во субјектите од ставот 1 на овој член се определува офицер за безбедност на класифицирани информации.

Во член 65 законодавецот ја уредува обврската на органите на државната и локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други правни лица, да создадат услови неопходни за заштита на класифицирани информации и да преземат мерки за елиминирање на негативните последици ако дојде до откривање на класифицираните информации. Во рамки на таа нивна должност, законодавецот предвидел дека наведените субјекти треба да определат офицер за безбедност на класифицирани информации којшто ќе овозможи ефикасно и координирано извршување на правата и обврските кои се однесуваат на класифицираните информации.

Мрежата на офицери за безбедност на класифицирани информации претставува важен сегмент од системот на заштита на класифицирани информации бидејќи офицерите за безбедност на класифицирани информации се сметаат за клучен персонал за одржливост, спроведување и надзор над безбедносните политики за работа со класифицирани информации во секој од релевантните субјекти каде се ракува и се чуваат класифицирани информации.

Член 66

Одговорното лице во субјектите од членот 65 став 1 од овој закон определува еден или повеќе офицери за безбедност на класифицирани информации, во зависност од бројот и обемот на класифицираните информации со кои се ракува во субјектот.

По исклучок од ставот 1 на овој член, во зависност од бројот и обемот на класифицирани информации, одговорното лице во субјектот може да ги врши работите на офицер за безбедност на класифицирани информации.

Офицерот за безбедност на класифицирани информации е должен да изготвува и поднесува квартални извештаи за својата работа и за состојбата со класифицираните информации директно до одговорното лице, освен во случајот од ставот 2 на овој член.

Доколку во субјектот се определени повеќе офицери за безбедност на класифицирани информации, одговорното лице определува еден од нив за координација со Дирекцијата.

Во член 66 законодавецот предвидел дека одговорното лице во субјектите во коишто се ракува и се чуваат класифицирани информации, односно во субјектите наведени во претходниот член, ќе определи еден или повеќе офицери за безбедност на класифицирани информации, во зависност од бројот и обемот на класифицираните информации со кои се ракува во субјектот.

Дополнителна основа за определување повеќе офицери за безбедност на класифицирани информации во еден субјект, којшто законодавецот не го идентификувал, би можела да биде и големиот број вработени коишто имаат потреба од пристап до класифицирани информации бидејќи тоа претпоставува и зголемен обем на задачи и активности за офицерот за безбедност. Токму искуствата покажуваат дека големите корисници на класифицирани информации, односно субјекти со голем број вработени каде се ракува и се чуваат голем број класифицирани информации, има потреба од повеќе офицери за безбедност на класифицирани информации.

Од друга страна, законодавецот предвидел и исклучок во којшто, во зависност од бројот и обемот на класифицирани информации, одговорното лице во субјектот може да ги врши работите на офицер за безбедност на класифицирани информации.

Понатаму во истиот член, законодавецот ја уредил обврската на офицерот за безбедност на класифицирани информации да изготвува и поднесува квартални извештаи за својата работа и за состојбата со класифицираните информации директно до одговорното лице. Притоа е уредено дека таа обврска не се однесува на офицерот за безбедност на класифицирани информации којшто истовремено е и одговорно лице во субјектот.

За подобра координација на работата на субјектот во делот на заштитата на класифицираните информации со Дирекцијата за безбедност на класифицирани информации, законодавецот уредил дека доколку во субјектот се определени повеќе офицери за безбедност на класифицирани информации, одговорното лице треба да определи еден од нив за координација со Дирекцијата.

Член 67

Офицерот за безбедност на класифицирани информации може да биде определен доколку ги исполнува следниве услови:

- ▶ да е државјанин на Република Северна Македонија,
- ▶ да не е државјанин на друга држава,
- ▶ да му е одобрен пристап до соодветно ниво на класифицирани

- информации според условите и постапката утврдени со закон,
- ▶ да има поминато обука за офицер за безбедност на класифицирани информации,
 - ▶ да поседува соодветен безбедносен сертификат.

Во член 67 се уредени условите што треба да ги исполни едно лице за да биде определено за офицер за безбедност на класифицирани информации. Имено, потребно е лицето да е државјанин на Република Северна Македонија, да не е државјанин на друга држава, да му е одобрен пристап до соодветно ниво на класифицирани информации според условите и постапката утврдени со закон, да има поминато обука за офицер за безбедност на класифицирани информации и да поседува соодветен безбедносен сертификат. Законодавецот тука не го прецизира степенот на безбедносниот сертификат што треба да го поседува офицерот за безбедност на класифицирани информации, но се претпоставува дека тоа е степенот кој соодветствува на степенот на класифицирани информации со кои се ракува во рамки на субјектот.

Обуката за офицер за безбедност на класифицирани информации законодавецот не ја уредува подетално, односно не посочува кој ја спроведува истата и каков доказ офицерот за безбедност би требало да прикаже во потврда на поминатата обука. Останува обврска на законодавецот во иднина да ја пополни оваа правна празнина, односно да ја доуреди материјата за ова прашање.

Член 68

Офицерот за безбедност на класифицирани информации е должен:

- ▶ да се грижи за спроведување на одредбите од овој закон и на ратификуваните меѓународни договори во врска со безбедноста на класифицираните информации во субјектот,
- ▶ квартално да ги проверува евиденциите и протокот на материјалите и документите,
- ▶ да се грижи за правилно и навремено спроведување на архивирањето и ништењето на класифицирани информации,
- ▶ да ја спроведе постапката за доставување барања за издавање на безбедносен сертификат во рамките на субјектот и да води евиденција на лицата за кои е спроведена постапка,
- ▶ да ја извести Дирекцијата за истекот на безбедносните сертификати, престанок на работењето или прераспоредување на корисниците на класифицирани информации,
- ▶ да ја извести Дирекцијата за потребата за промена на степенот на безбедносниот сертификат,
- ▶ да ја известува Дирекцијата, во писмена форма за секоја промена на податоците во безбедносниот прашалник или промена на условите за добивање на безбедносен сертификат за кои знаел или можел да знае дека настанала,
- ▶ да ги евидентира случаите на неовластен пристап до класифицирани информации или нивно компромитирање и на преземени дејствија и веднаш да ја извести Дирекцијата за таков случај и дејствие,
- ▶ да ги информира корисниците на класифицирани информации најмалку

еднаш годишно за правата и обврските при ракување со класифицирани информации,

- да обезбедува стручна помош при класификацијата на информацијата во субјектот,
- да организира обука за корисниците на класифицирани информации во субјектот за заштита на класифицирани информации.

За работите од ставот 1 на овој член, офицерот за безбедност на класифицирани информации изработува годишен план за работа, кој го доставува до одговорното лице на одобрување. Во случај кога одговорното лице ги врши работите на офицер за безбедност на класифицирани информации, тој го изработува годишниот план за работа.

Во член 68 законодавецот ги уредил должностите на офицерот за безбедност на класифицирани информации и притоа таксативно ги набројал. Предвидел дека офицерот за безбедност треба да се грижи за спроведување на одредбите од овој закон и на ратификуваните меѓународни договори во врска со безбедноста на класифицираните информации во субјектот. Тоа подразбира дека офицерот за безбедност на класифицирани информации е во директна комуникација со Дирекцијата за безбедност на класифицирани информации во однос на мерките и активностите коишто субјектот ги презема за заштита на класифицираните информации. Покрај генералната обврска на офицерот за безбедност на класифицирани информации за спроведување на одредбите од Законот, законодавецот понатаму предвидува одделни поконкретни должности и обврски. Притоа тој уредува дека офицерот треба квартално да ги проверува евиденциите и протокот на материјалите и документите, да се грижи за правилно и навремено спроведување на архивирањето и ништењето на класифицирани информации, да ја спроведе постапката за доставување барања за издавање на безбедносен сертификат во рамките на субјектот и да води евиденција на лицата за кои е спроведена постапка, да ја извести Дирекцијата за истекот на безбедносните сертификати, престанок на работењето или прераспоредување на корисниците на класифицирани информации, да ја извести Дирекцијата за потребата за промена на степенот на безбедносниот сертификат, да ја известува Дирекцијата, во писмена форма за секоја промена на податоците во безбедносниот прашалник или промена на условите за добивање на безбедносен сертификат за кои знаел или можел да знае дека настанала, да ги евидентира случаите на неовластен пристап до класифицирани информации или нивно компромитирање и на преземени дејствија и веднаш да ја извести Дирекцијата за таков случај и дејствие, да ги информира корисниците на класифицирани информации најмалку еднаш годишно за правата и обврските при ракување со класифицирани информации, да обезбедува стручна помош при класификацијата на информацијата во субјектот, да организира обука за корисниците на класифицирани информации во субјектот за заштита на класифицирани информации.

Во вториот став од членот законодавецот предвидел офицерот за безбедност на класифицирани информации да изработува годишен план за работа во којшто ќе бидат опфатени активностите што треба да ги исполни во согласност со дадените обврски и којшто го одобрува одговорното лице. Законодавецот го уредил и случајот кога одговорното лице ги врши работите на офицер за безбедност на класифицирани информации и притоа уредил дека тој самиот го изработува годишниот план за работа.

Неисполнувањето на должностите од страна на офицерот за безбедност стипулирани со овој член може да претставува прекршок, а умисленото и намерното пропуштање на вршење на неговите должности со цел да се предизвика определена штетна последица може дури да претставува и кривично дело, зависно од околностите на случајот, штетните последици итн.

ДИРЕКЦИЈА ЗА БЕЗБЕДНОСТ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ

Член 69

Дирекцијата е самостоен орган на државната управа со својство на правно лице.

Дирекцијата:

- ▶ обезбедува континуирано спроведување на меѓународните стандарди и нормативи во преземањето на мерките и активностите за заштита на класифицираните информации,
- ▶ врши координација на активностите во обезбедувањето заштита на класифицираните информации со државните органи и институциите кои вршат размена на класифицирани информации со странски држави и меѓународни организации,
- ▶ ги подготвува, организира, спроведува и го следи спроведувањето на мерките и активностите за обезбедување заштита на класифицирани информации кои на Република Северна Македонија ѝ се отстапени на користење од странски држави и меѓународни организации,
- ▶ презема активности за заштита на класифицирани информации отстапени од Република Северна Македонија на странски држави и меѓународни организации,
- ▶ учествува во изготвување на планови и програми на Република Северна Македонија за членство во меѓународни организации од областа за обезбедување заштита на класифицираните информации,
- ▶ планира и остварува меѓународна соработка за заштита и размена на класифицираните информации,
- ▶ предлага мерки за унапредување на заштитата на класифицирани информации,
- ▶ покренува иницијативи за склучување меѓународни договори со странски држави и меѓународни организации од областа на размената на класифицирани информации,
- ▶ врши акредитација на комуникациско-информациски системи и процеси,
- ▶ организира и спроведува обуки за безбедност на класифицирани информации,
- ▶ врши инспекциски надзор над спроведувањето на одредбите од овој закон и
- ▶ врши други работи утврдени со закон.

За своето работење Дирекцијата донесува годишен план, а подготвува и извештај кој го усвојува Владата на Република Северна Македонија.

Во член 69 е уреден статусот на Дирекцијата за безбедност на класифицирани информации како самостоен орган на државната управа со својство на правно лице. Таа како самостоен орган беше формирана во 2004 година по донесувањето на Законот за класифицирани информации истата година и е континуитет на поранешниот Национален безбедносен авторитет во НАТО контекст како стручна служба на Владата.³³

Во продолжение таксативно се уредени надлежностите на Дирекцијата, при што таа: обезбедува континуирано спроведување на меѓународните стандарди и нормативи во преземањето на мерките и активностите за заштита на класифицираните информации; врши координација на активностите во обезбедувањето заштита на класифицираните информации со државните органи и институциите кои вршат размена на класифицирани информации со странски држави и меѓународни организации; ги подготвува, организира, спроведува и го следи спроведувањето на мерките и активностите за обезбедување заштита на класифицирани информации кои на Република Северна Македонија ѝ се отстапени на користење од странски држави и меѓународни организации; презема активности за заштита на класифицирани информации отстапени од Република Северна Македонија на странски држави и меѓународни организации; учествува во изготвувањена планови и програми на Република Северна Македонија за членство во меѓународни организации од областа за обезбедување заштита на класифицираните информации; планира и остварува меѓународна соработка за заштита и размена на класифицираните информации; предлага мерки за унапредување на заштитата на класифицирани информации; покренува иницијативи за склучување меѓународни договори со странски држави и меѓународни организации од областа на размената на класифицирани информации; врши акредитација на комуникациско-информациски системи и процеси; организира и спроведува обуки за безбедност на класифицирани информации; врши инспекциски надзор над спроведувањето на одредбите од овој закон и врши други работи утврдени со закон.

Законодвецот предвидел Дирекцијата за своето работење да донесува годишен план и да подготвува извештај кој го усвојува Владата на Република Северна Македонија. Следствено на тоа, по донесување на годишниот план истиот се објавува на официјалната веб-страница на Дирекцијата, а извештајот се доставува до Владата за разгледување и усвојување.

Член 70

Во размената и заштитата на класифицирани информации со НАТО и со Европската Унија, Дирекцијата ги врши задачите за:

- ▶ координација и спроведување на безбедносните политики на НАТО и на Европската Унија во Република Северна Македонија, со цел обезбедување соодветно ниво на заштита на класифицираните информации согласно со ратификуваните меѓународни договори,
- ▶ безбедност на комуникациите за избор, управување и одржување на криптографската опрема за пренос, обработка и чување на класифицираните информации,
- ▶ спроведување безбедносна акредитација на комуникациско-

³³ Дирекција за безбедност на класифицирани информации, Историјат, достапно на: <https://www.dbki.gov.mk/?q=node/129>

информациските системи и процесите во кои се користат класифицирани информации,

- преземање мерки и активности за заштита на комуникациско-информациските системи од компромитирачко електромагнетно зрачење.

Во член 70 подетално се уредени задачите на Дирекцијата за безбедност на класифицирани информации во однос на размената и заштитата на класифицирани информации со НАТО и со Европската Унија во коишто се препознаваат улогите кои ги има Дирекцијата во однос на соработката со тие меѓународни организации.

Имено, како највисоко тело во државата во делот на заштитата на класифицираните информации, преку вршењето координација и спроведување на безбедносните политики на НАТО и на Европската Унија во Република Северна Македонија, со цел обезбедување соодветно ниво на заштита на класифицираните информации во согласност со ратификуваните меѓународни договори, Дирекцијата се препознава како Национален безбедносен авторитет (орган) за спроведување на политиката во делот на размената и заштитата на класифицираните информации со меѓународните организации. Преку извршување на задачите за безбедност на комуникациите за избор, управување и одржување на криптографската опрема за пренос, обработка и чување на класифицираните информации, Дирекцијата се препознава како Национално тело за безбедносна комуникација на комуникациско-информациски системи. Извршувајќи ги задачите за спроведување безбедносна акредитација на комуникациско-информациските системи и процесите во кои се користат класифицирани информации, Дирекцијата ја има улогата на Национално тело за акредитација на комуникациско-информациски системи, а преку преземање мерки и активности за заштита на комуникациско-информациските системи од компромитирачко електромагнетно зрачење, Дирекцијата се препознава како Национално тело за заштита од компромитирачко електромагнетно зрачење.³⁴

Член 71

Во размената и заштитата на класифицирани информации со НАТО Министерството за одбрана и Армијата на Република Северна Македонија управува со материјалите за криптографска заштита на класифицирани информации и безбедно ракување, чување, дистрибуција и евиденција на криптоматеријалите.

Во делот на управувањето со материјалите за криптографска безбедност на класифицирани информации и безбедното ракување, чување, дистрибуција и евиденција на криптоматеријалите, Дирекцијата врши надзор над имплементација на мерките што ги спроведува надлежниот орган.

Во член 71 е уредена надлежноста на Министерството за одбрана и Армијата на Република Северна Македонија во размената и заштитата на класифицирани информации со НАТО за управување со материјалите за криптографска заштита на класифицирани информации и безбедно ракување, чување, дистрибуција и евиденција на криптоматеријалите.

Во вториот став од членот законодавецот ја предвидел надлежноста на Дирекцијата за безбедност на класифицирани информации да врши надзор над имплементацијата на мерките што ги спроведува надлежниот орган во делот на управувањето со материјалите за криптографска безбедност на класифицирани

³⁴ B. Security Within the North Atlantic Treaty Organization (NATO) C-M(2002)49-REV1, 20 November 2020

информации и безбедното ракување, чување, дистрибуција и евиденција на криптоматеријалите. Надзорната улога на Дирекцијата е во насока на нејзината надлежност за следење на примената на важечката законска регулатива и за континуирано спроведување на меѓународните стандарди и нормативи во преземањето на мерките и активностите за заштита на класифицираните информации, додека надлежните субјекти ја имаат надлежноста за вршење на оперативната работа.

РЕГИСТРИ И КОНТРОЛНИ ТОЧКИ

Член 72

За вршење на работи од надлежност на Дирекцијата со НАТО класифицирани информации, класифицирани информации на Европската Унија и други странски класифицирани информации се воспоставуваат регистар, подрегистри и контролни точки.

Регистарот се воспоставува во Дирекцијата, а подрегистри и контролни точки се воспоставуваат во органите на државната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката и други правни лица, во коишто се ракува и се чуваат НАТО класифицирани информации, класифицирани информации на Европската Унија и други странски класифицирани информации.

Од подрегистрите и контролните точки од ставот 1 на овој член се доставуваат информации потребни за извршување на работите на Дирекцијата и се врши размена на класифицирани информации со странство.

На барање на корисниците на класифицирани информации Дирекцијата дава согласност за исполнување на условите за воспоставување подрегистри и контролни точки.

Размената на класифицирани информации меѓу Република Северна Македонија и странски држави и меѓународни организации се врши преку Дирекцијата, ако со закон, ратификуван меѓународен договор или друг аранжман поинаку не е уредено.

Во член 72 е уредено воспоставувањето на регистарскиот систем за вршење на работи од надлежност на Дирекцијата за безбедност на класифицирани информации со НАТО класифицирани информации, класифицирани информации на Европската Унија и други странски класифицирани информации. Истиот е составен од регистар којшто е востановен во Дирекцијата за безбедност на класифицирани информации и подрегистри и контролни точки коишто се воспоставуваат во субјектите во коишто се ракува и се чуваат НАТО класифицирани информации, класифицирани информации на Европската Унија и други странски класифицирани информации.

Во третиот став на овој член законодавецот предвидел дека од подрегистрите и контролните точки се доставуваат информации потребни за извршување на работите на Дирекцијата и се врши размена на класифицирани информации со

странство. Законодавецот ја уредил и постапката за воспоставување подрегистри и контролни точки со тоа што предвидел дека истите се воспоставуваат по добиена согласност од Дирекцијата за исполнување на условите потребни за воспоставување подрегистри и контролни точки по добиено барање од корисниците на класифицирани информации. Притоа, во овој член подетално не е предвидено кои се условите што треба да се исполнат за воспоставување подрегистри и контролни точки. Во насока на подетално уредување на ова прашање, законодавецот треба истите да ги пропише или да даде законски основ тоа да се направи со подзаконски акт.

Во последниот став на овој член е уредено дека размената на класифицирани информации меѓу Република Северна Македонија и странски држави и меѓународни организации се врши преку Дирекцијата, ако со закон, ратификуван меѓународен договор или друг аранжман поинаку не е уредено.

Мрежата на подрегистри овозможува соодветно распоредување на странските класифицирани информации до корисниците и водење контрола за нивното движење во субјектите во коишто истите се воспоставени. Во согласност со ратификувани меѓународни договори, регистарот, подрегистрите и контролните точки се предмет на надзор од страна на надлежните служби на НАТО и на ЕУ (член 37 став 1 од овој закон).

Член 73

Дирекцијата ги известува надлежните органи на странските држави и меѓународни организации за безбедноста на разменетите класифицирани информации и од нив прима известувања за безбедноста на класифицираните информации кои им се отстапени од Република Северна Македонија, согласно со ратификуваните меѓународни договори.

Во член 73 законодавецот ја уредил соработката меѓу Дирекцијата за безбедност на класифицирани информации и надлежните органи на странските држави и меѓународни организации, којашто се темели на ратификувани меѓународни договори за заемно известување за безбедноста на разменетите класифицирани информации.

Член 74

На барање на Дирекцијата, органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други правни и физички лица ѝ даваат информации кои се потребни за извршување на работите од нејзина надлежност.

Во член 74 законодавецот ја уредил обврската на органите на државната и на локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје и други правни и физички лица на барање на Дирекцијата за безбедност на класифицирани информации да ѝ даваат информации кои се потребни за извршување на работите од нејзина надлежност. Оваа соработка на Дирекцијата со субјектите особено доаѓа до израз во рамки на безбедносната проверка на физичките и на правните лица коишто бараат да им се издаде безбедносен сертификат.

Член 75

Со Дирекцијата за безбедност на класифицирани информации раководи директор кој го именува и разрешува Владата на Република Северна Македонија.

Директорот се именува со мандат од четири години.

Директорот има заменик, кој го именува и разрешува Владата на Република Северна Македонија за време од четири години. Заменик директорот го заменува директорот во случај кога тој е отсутен или кога поради болест и други причини не е во можност да ја врши својата функција со сите негови овластувања и одговорности во раководењето.

За именување на директор и заменик директор се објавува јавен оглас во три дневни весници кои се издаваат на целата територија на Република Северна Македонија од кои еден се издава на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

За директор и заменик директор на Дирекцијата може да биде именувано лице кое ги исполнува следниве услови:

- 1) да е државјанин на Република Северна Македонија;
- 2) да нема државјанство на друга држава;
- 3) со правосилна судска пресуда да не му е изречена казна забрана завршење на професија, дејност или должност;
- 4) да има стекнати 240 кредити според ЕКТС или VII/1 степен на образование;
- 5) да има најмалку пет години работно искуство;
- 6) да поседува еден од следниве меѓународно признати сертификати или уверенија за активно познавање на англискиот јазик не постар од пет години:
 - ▶ ТОЕФЕЛ ИБТ најмалку 74 бода,
 - ▶ ИЕЛТС (IELTS) - најмалку 6 бода,
 - ▶ ИЛЕЦ (ILEC) (Cambridge English: Legal) - најмалку B2 (B2) ниво,
 - ▶ ФЦЕ (FCE) (Cambridge English: First) - положен,
 - ▶ БУЛАТС (BULATS) - најмалку 60 бода или
 - ▶ АПТИС (APTIS) - најмалку ниво B2 (B2) и
- 7) да поседува безбедносен сертификат со степен „ДРЖАВНА ТАЈНА“.

На директорот и заменик директорот на Дирекцијата му престанува функцијата пред истекот на мандатот за кој е именуван:

- ▶ ако поднесе оставка,
- ▶ по лично барање,
- ▶ поради исполнување услови за старосна пензија утврдени со закон, со право на продолжување согласно со прописите за работни односи,

- ▶ поради смрт,
- ▶ ако со правосилна судска одлука е осуден на казна затвор од над шест месеци.

Владата на Република Северна Македонија ги разрешува директорот и заменик директорот на Дирекцијата ако е исполнет еден од следниве услови:

- ▶ ако се утврди дека не исполнува еден од условите утврдени во членот 74 став 5 од овој закон,
- ▶ ако одбие да поднесе изјава за имотна состојба и интереси согласно со закон или ако податоците содржани во изјавата се неистинити и
- ▶ очигледно ги прекрши правилата за судир на интереси, односно изземање во ситуации во кои директорот знаел или требало да знае за постоење на некоја од основите за судир на интереси, односно изземање предвидено со закон.

Во член 75 законодавецот уредил дека со Дирекцијата раководи директор. Него го именува и разрешува Владата на Република Северна Македонија со мандат од четири години. За прв пат со овој закон, законодавецот предвидува и заменик на директорот којшто е задолжен да го заменува директорот во случај кога тој е отсутен или кога поради болест и други причини не е во можност да ја врши својата функција со сите негови овластувања и одговорности во раководењето. И заменик-директорот го именува и разрешува Владата на Република Северна Македонија со мандат од четири години.

Со овој член е пропишана и постапката за избор на директор и заменик-директор која започнува со објавување јавен оглас во три дневни весници кои се издаваат на целата територија на Република Северна Македонија од кои еден се издава на јазикот што го зборуваат најмалку 20% од граѓаните кои зборуваат службен јазик различен од македонскиот јазик.

Пропишани се и условите коишто и двајцата функционери треба да ги исполнат за да бидат избрани за позициите директор и заменик-директор, и тоа лицето: да е државјанин на Република Северна Македонија; да нема државјанство на друга држава; со правосилна судска пресуда да не му е изречена казна забрана за вршење на професија, дејност или должност; да има стекнати 240 кредити според ЕКТС или VII/1 степен на образование; да има најмалку пет години работно искуство; да поседува еден од наведените меѓународно признати сертификати или уверенија за активно познавање на англискиот јазик не постар од пет години: ТОЕФЕЛ ИБТ – најмалку 74 бода, ИЕЛТС (IELTS) – најмалку 6 бода, ИЛЕЦ (ILEC) (Cambridge English: Legal) – најмалку Б2 (B2) ниво, ФЦЕ (FCE) (Cambridge English: First) – положен, БУЛАТС (BULATS) – најмалку 60 бода или АПТИС (APTIS) – најмалку ниво Б2 (B2) и да поседува безбедносен сертификат со степен „ДРЖАВНА ТАЈНА“.

Во овој член законодавецот ги предвидел и условите кога на директорот и заменик-директорот на Дирекцијата му престанува функцијата пред истекот на мандатот за кој е именуван, односно: ако поднесе оставка по лично барање, поради исполнување услови за старосна пензија утврдени со закон, со право на продолжување во согласност со прописите за работни односи, поради смрт и ако со правосилна судска одлука е осуден на казна затвор од над шест месеци. Уредени се и условите според кои, ако е исполнет еден од нив, Владата на Република Северна Македонија ги разрешува директорот и заменик-директорот на Дирекцијата. Имено, директорот и заменик-директорот на Дирекцијата може да биде разрешени ако се утврди дека не исполнуваат еден од условите утврдени во членот 75 став 4 од овој закон (*тука во Законот е направена техничка грешка – став 5*), ако

одбие да поднесе изјава за имотна состојба и интереси во согласност со закон или ако податоците содржани во изјавата се неистинити и очигледно ги прекршил правилата за судир на интереси, односно изземање во ситуации во кои директорот знаел или требало да знае за постоење на некоја од основите за судир на интереси, односно изземање предвидено со закон. Последните две основи всушност се индикации за коруптивно дејствување кои сами по себе прават функционерот да не е достоин за вршењето на оваа многу важна функција.

Член 76

Вработените во Дирекцијата се административни државни службеници. Во однос на нивните права и одговорности од работен однос се применуваат одредбите од Законот за административни службеници.

Вработените во Дирекцијата се упатуваат на работа во постојаните мисии на Република Северна Македонија при НАТО и ЕУ, согласно со потпишана спогодба за заедничка соработка со Министерството за надворешни работи.

За време на упатувањето, вработените се здобиваат со звање согласно со одредбите од Законот за надворешни работи.

Вработените во Дирекцијата треба да поседуваат соодветен безбедносен сертификат за пристап до класифицирани информации. Степенот на безбедносниот сертификат се утврдува со правилникот за систематизација на работните места во Дирекцијата.

Вработениот во Дирекцијата на кој за време на работниот однос нема да му биде продолжена важноста на безбедносниот сертификат или во текот на проверката ќе се утврди дека не може да добие безбедносен сертификат поради постоење безбедносен ризик за пристап и ракување со класифицирани информации, трајно се презема во друг државен орган или институција, на работно место на исто ниво за кое ги исполнува општите и посебни услови пропишани во актот за систематизација на другата институција.

Преземањето се врши врз основа на спогодба којашто ја потпишуваат раководните лица на двете институции.

На вработениот што се презема му престанува работниот однос доколку не го потпише новиот договор за работа во рок од 15 дена од датумот на кој му е доставен.

Вработените во Дирекцијата имаат службена легитимација која ја издава директорот на Дирекцијата.

Образецот на службената легитимација и начинот на нејзино издавање ги пропишува директорот на Дирекцијата.

Одредбите од член 76 се однесуваат на вработните во Дирекцијата за безбедност на класифицирани информации. Законодавецот пропишал дека вработените во Дирекцијата имаат статус на административни државни службеници, па согласно таквиот статус, пропишал дека за нивните права и одговорности од работен однос

се применуваат одредбите од Законот за административни службеници.³⁵ Со ваквиот статус, вработените во Дирекцијата остануваат единствени во рамките на државните органи што имаат надлежности во безбедносниот сектор коишто немаат статус на лица со посебни должности и овластувања.³⁶ Таквиот статус на вработените во Дирекцијата, за жал, претставува причина за зголемен одлив на персонал во други институции и директно влијае на нејзините кадровски капацитети за спроведување на законските надлежности.

Во вториот став од овој член законодавецот предвидел дека вработените во Дирекцијата се упатуваат на работа во постојаните мисии на Република Северна Македонија при НАТО и ЕУ, во согласност со потпишана спогодба за заедничка соработка со Министерството за надворешни работи и притоа, за време на упатувањето, се здобиваат со звање во согласност со одредбите од Законот за надворешни работи.

Со овој член се уредува и условот вработените во Дирекцијата да поседуваат соодветен безбедносен сертификат за пристап до класифицирани информации, којшто се утврдува со Правилникот за систематизација на работните места во Дирекцијата. Ова прашање е уредено на ваков начин од причина што сите вработени во Дирекцијата немаат потреба од пристап до класифицирани информации со ист степен на класификација, како што немаат иста потреба за пристап до класифицирани информации на НАТО и/или на ЕУ.

Законодавецот во петтиот став на овој член ја предвидел и постапката во случај кога на вработен во Дирекцијата за време на работниот однос нема да му биде продолжена важноста на безбедносниот сертификат или во текот на проверката ќе се утврди дека не може да добие безбедносен сертификат поради постоење безбедносен ризик за пристап и ракување со класифицирани информации. Во таков случај, законодавецот предвидел дека вработениот трајно се презема во друг државен орган или институција, на работно место на исто ниво за кое ги исполнува општите и посебни услови пропишани во актот за систематизација на другата институција. Преземањето на вработениот во друга институција е уредено да биде врз основа на спогодба којашто ја потпишуваат раководните лица на двете институции. Доколку вработениот што се презема не го потпише новиот договор за работа во рок од 15 дена од датумот на кој му е доставен му престанува работниот однос. Ова решение е усогласено со важечката законска регулатива за мобилност на административните службеници.³⁷

За вработените во Дирекцијата законодавецот предвидел да имаат службена легитимација која ја издава директорот на Дирекцијата и чијшто образец и начин на нејзино издавање ги пропишува во подзаконски акт. Предвидениот Правилник за образецот на службената легитимација на вработените лица во Дирекцијата за безбедност на класифицирани информации и за начинот на нејзиното издавање е донесен и објавен во „Службен весник на Република Северна Македонија“ број 53/2021.

³⁵ Закон за административни службеници, „Службен весник на Република Македонија“ број 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 и 11/18 и „Службен весник на Република Северна Македонија“ број 275/19 и 14/20.

³⁶ Закон за Агенција за национална безбедност („Службен весник на Република Северна Македонија“ број 108/19) член 65; Закон за Оперативно-техничка агенција („Службен весник на Република Македонија“ број 71/18 и „Службен весник на Република Северна Македонија“ број 98/19) член 11, став (1) и член 20 став (1); Закон за Агенцијата за разузнавање („Службен весник на Република Северна Македонија“ број 21/2021), член 25.

³⁷ Закон за административни службеници („Службен весник на Република Македонија“ број 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 и 11/18 и „Службен весник на Република Северна Македонија“ број 275/19 и 14/20), член 30; и Закон за вработени во јавниот сектор („Службен весник на Република Македонија“ број 27/14, 199/14, 27/16, 198/18 и „Службен весник на Република Северна Македонија“ број 14/20), членови 42,43 и 44.

ГЛАВА ПЕТТА

ПЛАНОВИ И ПРОГРАМИ ЗА РАБОТЕЊЕ НА ДИРЕКЦИЈАТА И ФИНАНСИРАЊЕ НА ДИРЕКЦИЈАТА

Член 77

Работата на Дирекцијата се води и реализира според принципите, нормите и процедурите кои важат во системот на планирањето, програмирањето и буџетското работење.

За поефикасна реализација на работата на Дирекцијата, со одредбите на овој член законодавецот определува дека таа треба да се води и да се реализира според принципите, нормите и процедурите кои важат во системот на планирањето, програмирањето и буџетското работење. Како што може да се види во коментарот за следниот член, тоа се изработува во согласност со упатствата и насоките за подготвување на буџетските барања од буџетскиот циркулар што го изработува Министерството за финансии.

Член 78

Финансиските средства за потребите на Дирекцијата се обезбедуваат од Буџетот на Република Северна Македонија.

Финансиските средства за потребите на Дирекцијата можат да се обезбедат и од други извори согласно со закон.

Финансиските средства за државните органи за потребите на заштитата, користењето и меѓународната размена на класифицираните информации се обезбедуваат од Буџетот на Република Северна Македонија во рамките на финансиските средства на тие органи.

Органите на локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од општините, градот Скопје и општините во градот Скопје за потребите на заштитата, користењето и меѓународната размена на класифицираните информации обезбедуваат финансиски средства од сопствени извори и од финансиски и материјални средства на Република Северна Македонија.

Членот 78 од Законот правно го уредува прашањето на финансирањето на Дирекцијата за безбедност на класифицирани информации и финансирањето на самата заштита, користење и меѓународна размена на класифицираните

информации која се презема од страна на други државни органи, органи на локална власт, правни лица итн.

Според став 1 од овој член, Дирекцијата се финансира од Буџетот на Република Северна Македонија. Таа е самостоен орган на државна управа и оттука, нејзиното финансирање и работа не се координираат, на пример, преку некое министерство, туку директно од државниот Буџет.³⁸

Висината на средствата кои се издвојуваат за Дирекцијата е прашање за кое може многу да се дискутира иако излегува од тесните прагматични рамки на еден коментар на закон. Тоа зависи од многу значајни елементи. Како прво, природата и променливата амплитуда на предизвиците со кои се соочува Дирекцијата во нејзиното тековно работење, како и сензитивната сфера на постапување го диктираат на некој начин обемот на потребни средства за ефикасно функционирање на оваа институција. Како второ, речиси сите европски земји, дури и оние најразвиените, се соочуваат со предизвикот на високите издатоци за безбедносните институции. Соодветно на современото сфаќање на заштитната компонента на субјектите кои се задолжени за тоа, како што е и случајот со Дирекцијата, неопходно е да се изгради систем кој ќе обезбеди потребната информација да стигне до крајниот корисник и притоа таа да биде заштитена. Јасно дефинираниот став за потребата од постоење, изградба и развој на соодветен систем за заштита на класифицирани информации, самиот по себе го наметнува прашањето за расходите, односно колку финансиски средства се потребни за обезбедување на овој сегмент.

Оттука, еден од често наведуваните аргументи за обезбедување на потребната функционалност на системот се трошоците, односно, цената, сфатена доследно како обем на финансиски средства кои се потребни да се обезбедат за остварување на посакуваната цел, вклучувајќи ги и средствата кои треба да се обезбедат за подобро организирање и работење.

Дирекцијата, според Законот, може да се финансира и од други извори на финансирање, при што конкретно тие не се наведени во членот, но таквата можност Законот ја предвидува експлицитно.

Што се однесува до финансиските средства за државните органи за потребите на заштитата, користењето и меѓународната размена на класифицираните информации, одредбата од став 3 на овој член определува дека се обезбедуваат од Буџетот на Република Северна Македонија, но во рамките на финансиските средства на тие органи, што значи од државниот Буџет за таа намена ним им се определуваат средства, а не дека тоа оди преку Дирекцијата и средствата наменети за неа.

Органите на локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од општините, градот Скопје и општините во градот Скопје за потребите на заштитата, користењето и меѓународната размена на класифицираните информации обезбедуваат финансиски средства од сопствени извори и од финансиски и материјални средства на Република Северна Македонија во согласност со став 4 на овој член.

³⁸ Предлогот за буџетот на Дирекцијата се изработува во согласност со упатствата и насоките за подготвување на буџетските барања од буџетскиот циркулар што го изработува Министерството за финансии (Подетално в. <https://finance.gov.mk/буџетски-циркулар/>).

ГЛАВА ШЕСТА

НАДЗОР

Член 79

Инспекциски надзор над спроведувањето на овој закон и прописите донесени врз основа на овој закон врши Дирекцијата преку инспекторите за безбедност на класифицирани информации (во натамошниот текст: инспекторите).

Работите на инспекцискиот надзор во рамките на Дирекцијата се вршат во посебна организациона единица.

Според овој член од Законот, предвидено е да се врши инспекциски надзор над спроведувањето на целокупното законодавство за заштита на класифицираните информации. Тоа значи дека инспекторите при вршење на надзорот ќе ги проверат субјектите од аспект на примена на одредбите од Законот, но и одредбите од подзаконските акти донесени врз основа на Законот, односно уредбите и правилниците.

Во вршење на инспекцискиот надзор примарна улога им е доверена на инспекторите за безбедност на класифицирани информации на Дирекцијата. Во спроведување на надзорот нивната задача е да утврдат дали се спроведува Законот и прописите кои се донесени врз основа на овој закон, односно да ги согледаат состојбите и да го оценат вкупното работење на релевантните субјекти. Инспекцискиот надзор во правната наука уште се нарекува и репресивен надзор бидејќи кај него доаѓаат до израз одредени овластувања од принудна природа кои се применуваат со цел да се обезбеди доследно почитување на законитоста во работењето и правниот поредок воопшто.³⁹

Се работи за една систематска активност за согледување на тоа како се почитуваат воспоставените законски стандарди и норми за обезбедување на законито користење на класифицираните информации, како се постапува со класифицираните информации во времетраењето на нивното постоење, какви се условите под кои се ракува и во кои се чуваат класифицираните информации и како е обезбеден заштитниот простор, класифицираниот договор итн. Инспекторите за безбедност на класифицирани информации треба да преземат активности со кои ќе извршат увид во реалната состојба и оценување на вкупното работење. Оваа повратна спрега значи и споредување на вистинските резултати со претходно дефинираните стандарди за работа. Значи, надзорот е во функција на проценето и објективно согледување на состојбите за тоа дали постојат пропусти во спроведувањето и имплементирањето на законските норми кои се базираат на одредени стандарди со кои се спроведува стварното извршување.

Со одредбите од став 2 на овој член се предвидува работите на инспекцискиот

³⁹ Давитковски, Б., Павловска – Данева, А., Административно право – прв дел, Скопје, 2018, стр. 309

надзор да се вршат во посебна организациона единица во рамките на Дирекцијата. Во основа, тоа е и реалното место и елемент од горесинтетизираната анализа која говори дека природно е предодредена самата организациона единица да спроведе инспекциски надзор во оваа сфера, бидејќи тоа е субјектот кој е задолжен и вистински ја познава имплементираната страна на законот и самата суштина на надзорот. Од аспект на систематското поврзување на луѓето кои работат во еден правен субјект со целите, секоја организациона единица е составена од луѓе кои се групирани според одредени критериуми. Во рамките на Дирекцијата тие се дадени во член 81. Организационата единица за инспекциски надзор е составена од професионалци кои ја познаваат материјата на инспекцискиот надзор генерално, но и сензитивната сфера на заштитата на класифицираните информации.

Член 80

Во постапката за вршење на инспекциски надзор се применуваат одредбите од овој закон, а за прашањата што не се уредени со овој закон се применуваат одредбите од Законот за инспекциски надзор и Законот за општата управна постапка.

Начинот на вршењето на инспекциски надзор поблиску се уредува со Правилник што го донесува директорот на Дирекцијата.

Инспекцискиот надзор, како што нагласивме и претходно е од големо значење во процесот на заштита на информациите од најмалку две причини, и тоа: едната е во насока на согледување како се применуваат одредбите од Законот за класифицирани информации(*) и соодветните прописи кои се донесени и кои произлегуваат од Законот *in concreto* и второ, да се откријат слабостите и пропустите во работењето за да се преземат одредени активности во насока на негово подобрување.

Во член 80 став 1 се определени правните основи за вршењето на инспекцискиот надзор во оваа област, односно јасно е наведено дека во постапката за вршење на инспекциски надзор првенствено се применуваат одредбите од овој закон, што е суштински важна одредба, затоа што ваквото решение не беше содржано во претходниот Закон за класифицирани информации и исклучиво се применуваат одредбите од Законот за инспекциски надзор. Тоа значи дека за работите кои се регулирани со овој закон, тој претставува *lex specialis* и тој се применува првенствено, додека Законот за инспекциски надзор (како и Законот за општата управна постапка) е *lex generalis* и неговите одредби се применуваат за прашањата што не се уредени со Законот за класифицирани информации(*) како *lex specialis*.

Евидентно, состојбата е битно различна и оправдана заради специфичноста на оваа сфера, па така одредбите на Законот за инспекциски надзор, во согласност со член 2, став 1, 2 и 3 од Законот⁴⁰ кои се однесуваат на постапката, обврските и условите за вршење на инспекциски надзор, се применуваат на инспекциските служби организирани како органи во состав на министерствата или како организациски единици, во рамки на органите на државната управа, општините, општините во Градот Скопје и Градот Скопје, но не и за Дирекцијата за безбедност на класифицирани информации, и исто така не се применуваат во Министерството за финансии, вклучувајќи ги Управата за јавни приходи и Царинската управа, Министерството за одбрана и Министерството за внатрешни работи.⁴¹ Тоа значи дека

⁴⁰ Закон за инспекциски надзор, „Службен весник на Република Северна Македонија“ број 102/19, член 2.

⁴¹ Исто, член 2, став 4.

Дирекцијата за безбедност на класифицирани информации има оригинално право да спроведува инспекциски надзор преку своите инспектори. Со тоа се постигнува двојна цел и тоа, од една страна, се обезбедува потребната самостојност заради природата на материјата, а од друга страна, секако, се обезбедува законитост во постапувањето во насока на насочување на работата во согласност со законската регулатива.

Законодавецот предвидел дека начинот на вршење на инспекциски надзор поблиску ќе биде уреден со правилник, но оставил и простор за прашањата што не се уредени со овој закон да се применуваат одредбите од Законот за инспекциски надзор и Законот за општата управна постапка. Примената на одредбите од наведените закони е само дополнување во спроведување на потребниот надзор заради комплементарноста на материјата. Така, Законот за општата управна постапка ги уредува прашањата со кои се уредува постапката за остварување на заштита на правата и правните интереси на физичките лица, правните лица и другите странки, како и заштита на јавниот интерес по која се должни да постапуваат министерствата, органите на државната управа, организациите утврдени со закон, другите државни органи, правните и физичките лица на кои со закон им е доверено да вршат јавни овластувања, како и органите на општината, на градот Скопје и општините во градот Скопје, кога во вршењето на своите законски надлежности, постапуваат, решаваат и преземаат други управни дејствија во управни работи⁴² и што е најважно овој закон се применува за сите управни дејствија на јавните органи и на давателите на услуги.⁴³

Погореспоменатиот Правилник има за цел целосно да го разработи начинот на вршење на инспекциски надзор во оваа сфера и секако треба да биде во корелација со Законот за класифицирани информации(*) и другите *inter alia* правни прописи кои се во содејство со Законот за класифицирани информации(*). Со други зборови, одредбите на овој правилник ја рефлектираат цврстата и јасна определба на Законот за класифицирани информации(*) и пропишаните одредби што во практиката треба да создаде лесно конкретизирање на надзорот, односно да нема различни интерпретации за исти и слични прашања во постапувањето или што е особено важно да не се создаде простор за субјективно размислување. Тоа значи дека одредбите треба да се јасни, прецизни и применливи. Нормите во правото кои може да се толкуваат на различни начини се смета дека не го исполнуваат барањето за јасни и прецизни одредби: *lex certa et stricta* кое е консеквенција на начелото на законитост.

Правилникот за начинот на вршење инспекциски надзор е донесен врз основа на член 80, став 2 од овој закон и е објавен во „Службен весник“ број 246/20.

Член 81

Инспекторот, кој го врши инспекцискиот надзор покрај општите услови утврдени со Законот за административни службеници потребно е да ги исполнува следниве посебни услови:

- ▶ да има стекнато 240 кредити според ЕКТС, или завршен VII/1 степен,
- ▶ да има три години работно искуство во областа на безбедноста на класифицирани информации,
- ▶ да има положено стручен испит за инспектор за класифицирани информации.

⁴² Закон за општата управна постапка, „Службен весник“ број 124/15, член 1.

⁴³ Исто, член 2.

Начинот на полагање на стручниот испит за инспекторите за класифицирани информации со Правилник го пропишува директорот на Дирекцијата.

Додатокот на плата на инспекторот се регулира со Законот за инспекциски надзор.

Лице кое ќе врши инспекциски надзор, односно лицето инспектор, мора да исполнува определени услови кои Законот јасно и експлицитно ги наведува. Имено, инспекторот кој го врши инспекцискиот надзор од областа на заштитата на класифицираните информации мора да исполнува најпрвин општи услови кои се пропишани со Законот за административни службеници и посебни услови кои се пропишани во Законот за класифицирани информации(*).

Сите услови се предуслов за компетитивна личност која се очекува дека со своето целесообразно дејствување и индивидуалното поведение ќе направи задачите да се видливи и да придонесе за нивно конкретизирање и остварување.

Нема дилема дека за инспекторот кој го врши инспекцискиот надзор во сферата на заштита на класифицираните информации од аспект на квалификациите, компетенциите, оспособеноста итн., покрај општите услови утврдени со Законот за административни службеници, законодавецот смета дека треба да исполнува и посебни услови заради специфичноста на проблематиката. Во однос на општите услови, во согласност со Законот за административни службеници каде е дадена класификација на работни места на административни службеници, општите компетенции се утврдуваат во Рамката на општите компетенции за административни службеници,⁴⁴ додека законодавецот предвидел посебните услови како потребните стручни квалификации, работното искуство во струката, како и положениот стручен испит за инспектор за класифицирани информации да се утврдат како посебни услови на работното место. Категоријата на работните места на административните службеници според одговорноста, целите, видот и сложеноста на работите и на работните задачи на работното место е во согласност со член 22 од Законот за административни службеници. Работните места на административните службеници се класифицираат во четири категории и тоа: категорија А – секретари, категорија – раководни административни службеници, категорија В – стручни административни службеници и категорија Г – помошно-стручни административни службеници.⁴⁵ Пополнувањето на работните места на административни службеници и вработување на административни службеници се определени во Глава VI и VII од Законот за административни службеници.⁴⁶

Мора да се нагласи дека образованието е клучно за стекнување на потребните компетенции и вештини и дека оставањето на простор во Законот за класифицирани информации(*) како што е определено во став 1 алинеја 1, потенцијално секој профил на образование да е конкурентен, ја релативизира општата заложба за пополнување на организационата единица за инспекциски надзор со стручни и пред сè, компетентни кадри кои располагаат со потребното знаење и вештини стекнати во процесот на образование.

Освен соодветното образование, важен предуслов за успешно вршење на оваа работа е и професионалното и работното искуство. Работното искуство од три години кое е наведено во алинеја 2 остава простор на сериозна дискусија.

⁴⁴ Закон за административни службеници, „Службен весник на Република Македонија“ број 27/14, 199/14, 48/15, 154/15, 5/16, 142/16 и 11/18 и „Службен весник на Република Северна Македонија“ број 275/1019, и 14/20, член 21, став 2.

⁴⁵ Исто, член 22.

⁴⁶ Исто, член 30-47.

Постојат мислења дека инспекторите треба да имаат многу поголемо работно и професионално искуство за да можат да навлезат во сржта на проблемите за да можат да ја разберат променливата амплитуда на работењето во оваа сфера со што би ја исполнила главната цел да бидат катализатор на вкупните состојби во откривање на неправилностите во работењето на правните и физичките лица кои се во допир со класифицирани информации и преземање на дејствија за нивно отстранување и/или санкционирање.

Ставот 2 на овој член ја уредува обврската на Дирекцијата да донесе Правилник за начинот на полагање на стручниот испит за инспекторите за класифицирани информации (третиот посебен услов) кој поблиску ги пропишува условите и начинот на полагање со кој ќе се проверува теоретското знаење на кандидатите кои се пријавиле за инспектори, како и проверување на компетитивноста и оспособеноста на кандидатите.

Правилникот за начинот на полагање на стручниот испит на инспекторите за безбедност на класифицирани информации е донесен и објавен во „Службен весник на Република Северна Македонија“ број 219/20 година и во него се предвидува дека испитот се состои од општ дел (прашања од областите општа управна постапка, инспекциска постапка и прекршочна постапка) и посебен дел (прашања од областа на прописите за безбедност на класифицирани информации).⁴⁷ Кандидатот кој точно одговорил на најмалку 70% од прашањата за секој дел одделно, се смета дека го положил испитот и за тоа добива соодветна потврда.

Ставот 3 кој се однесува на додатокот на плата на инспекторите, стипулира дека тоа се регулира со Законот за инспекциски надзор.

Член 82

Инспекторот врши инспекциски надзор во органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, како и на други правни и физички лица.

Во извршувањето на работата инспекторот е самостоен во својата работа. По потреба, на предлог на раководителот на организационата единица за вршење инспекциски надзор, директорот може да определи тим за инспекциски надзор составен од административни службеници од Дирекцијата.

Инспекторите се должни да постапуваат согласно со законот и прописите. Инспекторите треба да обезбедуваат објективна примена на законот.

Во овој член се прецизира, како што е наведено, кој ќе биде предмет на инспекциски надзор, односно дека тој ќе се спроведува во органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, во правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, како и во други правни и физички лица. Се разбира дека тоа не се сите вакви субјекти, туку оние чијашто работа има допирни точки со сферата на класифицираните информации.

Повеќе од очигледно е дека инспекцискиот надзор е потребен, но сепак за негово целосно ефектуирање е потребно многу знаење и искуство на инспекторите,

⁴⁷ В. член 4 од Правилникот за начинот на полагање на стручниот испит на инспекторите за безбедност на класифицирани информации, „Службен весник на Република Северна Македонија“, број 219/20 година.

а ефективността на надзорот зависи и од антиципативниот пристап на сите субјекти што се вклучени во овој процес, како органите на државната и локалната власт, правните лица основани од Републиката или општините, градот Скопје и општините во градот Скопје, како и други правни и физички лица.

Ставот 2 на членот 82 се однесува на самостојноста на инспекторот во извршување на работата. Самостојноста е важна и клучна компонента за да се осигура дека при вршење на инспекцискиот надзор инспекторот правилно ќе ја заврши својата задача. Тоа значи дека никој не треба да влијае на неговото работење, а самостојноста ќе му овозможи побрзо, поцелосно и пообјективно решавање на проблемот, таа создава објективни услови за непристрасност и подразбира отсуство на притисоци за постапување според нечие барање и желби. Сето тоа е солидна основа инспекторот да може да го објективизира својот поглед и секогаш да настојува ситуацијата да може да се разгледува неутрално.

Но, покрај самостојноста оценета и проценета во вредносно-етичка смисла, како што е погоре елаборирано, треба да се земе предвид и сфаќањето за самостојноста во контекстот на оваа одредба од аспект на самостојно постапување наспроти постапување во тим.

Имено, заради реалните потреби или како резултат на обемот на работата, законодавецот предвидел, на предлог на раководителот на организационата единица за вршење инспекциски надзор, директорот на Дирекцијата за безбедност на класифицирани информации да може да определи тим за инспекциски надзор составен од административни службеници од Дирекцијата. Во одредени специфични ситуации се наметнува потреба за определување на тим што ќе овозможи потемелна и покомплексна анализа на проблемот, а тоа ќе значи порационално да се обезбеди потребната длабочина и широчина на знаење и искуство, што ќе подразбира и побрзо и поцелосно запознавање на карактерот на проблемот кој се решава, но, ова ќе значи понекогаш и потреба за усогласување на мислењата на поголемиот број ангажирани лица за одреден проблем. Оваа можност што ја предвидел законодавецот – директорот да определи тим за инспекциски надзор на предлог на раководителот на организационата единица за вршење инспекциски надзор може да се смета за позитивно решение затоа што тоа подразбира повеќе луѓе да обединат размислување за едно или повеќе прашања што овозможува проблемскиот елемент да се „расветли“ од различни аспекти, мислења, знаења и слично или заради големиот обем. Токму затоа има поголеми шанси да се донесе релевантно мислење и заклучок. Сепак, мора да се нагласи дека во тимското работење може да се случи да се разводнува одговорноста за евентуалната погрешна интерпретација на состојбите. Од горенаведеното, треба да се заклучи дека ваквата можност директорот треба да ја практикува по исклучок, како што, впрочем, и самиот законодавец посредно укажал, предвидувајќи го ваквото решение за факултативна основа.

Во ставот 3 на истиот член се наведува дека инспекторите се должни да постапуваат во согласност со законот и прописите. Инспекторите треба да обезбедуваат објективна примена на законот и воопшто законско постапување. Тоа подразбира дека инспекторите при вршење на инспекцискиот надзор треба да спроведат објективна, сеопфатна, неселективна и недискриминирачка примена на Законот, што значи дека ќе биде добро поставена и адаптирана на карактерот и суштината на проблемите во контролираниот субјект и ќе даде нагласок на повратната спрега изразена преку вкупните односи на сите субјекти вклучени во инспекцискиот надзор (инспекторите и субјектот на контрола). Самиот инспекциски надзор значи надзор за утврдување на тоа дали нечие работење е во согласност со закон, па доколку повеќе (a fortiori) се очекува и нагласува потребата и самите

инспектори законски да ги вршат своите професионални задачи.

Незаконското постапување на инспекторите, имајќи го предвид надзорниот и мошне специфичниот карактер на нивната работа најчесто треба да се третира како сериозна злоупотреба и правно да се квалифицира, зависно од околностите на случајот, како некое од кривичните дела предвидени во глава XX од Кривичниот законик: Кривични дела против службената должност.

Член 83

Во вршењето на инспекцискиот надзор од членот 79 од овој закон, инспекторите се овластени:

- ▶ да вршат надзор над спроведувањето на овој закон и другите прописи од областа на безбедноста на класифицираните информации,
- ▶ да предлагаат мерки за отстранување на утврдените неправилности и недостатоци во определен рок и
- ▶ да преземаат други дејствија согласно со закон.

Во овој член законодавецот на најопшт начин ги навел основните овластувања кои ги имаат инспекторите за безбедност на класифицирани информации, а тие, пред сè, се систематизирани во три области: прво, инспекторите вршат надзор над спроведувањето на законодавството за безбедност на класифицирани информации, второ, тие врз основа на спроведениот надзор *in concreto*, се овластени да предложат мерки за да се отстранат утврдените недостатоци и неправилности во примената на Законот во определен временски период (рок) и трето, да преземат други дејствија во согласност со закон, при што тие се најчесто предвидени во други поконкретни одредби. Наведените овластувања и природно се надоврзуваат едни на други. Имено, за да се предложат, на пример, мерки за отстранување на неправилностите, мора прво да е спроведен инспекциски надзор во рамките на кој таквите неправилности се утврдени итн.

Член 84

Службеното својство на инспекторот се докажува со службена легитимација и значка. При вршењето на инспекцискиот надзор, инспекторите се должни да се легитимираат.

Службената легитимација и значка од ставот 1 на овој член ја издава и одзема директорот на Дирекцијата.

Образецот, формата и содржината на службената легитимација и значка, како и начинот на нивното издавање и одземање, ги пропишува директорот на Дирекцијата.

Законските одредби предвидени во став 1 на овој член го задолжуваат инспекторот при вршење инспекциски надзор задолжително да се легитимира со што ќе го докаже неговото службено својство. Тоа значи дека инспекторот за време на вршење на надзорот мора да носи службена легитимација и значка и кога се повикува на своите работи и работни задачи истовремено е должен да ги покаже и легитимацијата и значката. Ако доследно се толкува оваа одредба, тоа би подразбирало инспекторот кога ќе врши инспекциски надзор, односно при секое спроведување на која било од неговите задачи дадени како овластувања кога е во

контакт со лицето врз кое се спроведува надзорот, без исклучок да се легитимира. Во ситуација кога нема униформирана работна облека, која го идентификува со работното место, потребата од редовно легитимирање е оправдана.

Сепак, би требало оваа одредба да се толкува рестриктивно, што е во корелација со обврската инспекторот на секое барање од странката која се сомнева во неговото службено дејство да се легитимира. Законот ја третира легитимацијата како доказ за оспособеност за вршење инспекциски надзор како своевидна дозвола за професионално занимавање со работите и работните задачи од областа на инспекцискиот надзор. Легитимацијата која ја добива инспекторот со исполнување на општите и посебните услови од Законот за административни службеници и од Законот за класифицирани информации(*) е доказ за положен стручен испит според Правилникот кој го пропишува директорот на Дирекцијата, односно тоа е еден вид „диплома“ која се стекнува за да се добие легитимитет за вршење на работите поврзани со инспекцискиот надзор.

Став 2 на овој член пропишува дека инспекторот е должен да ги врати легитимацијата и значката на барање на директорот на Дирекцијата кога ќе бидат создадени услови за одземање на легитимацијата и значката заради несовесно однесување и други околности кои се основа за одземање.

Таквите околности го прават инспекторот недостоен за натамошно вршење на службата, па претставуваат основа за одземање и на легитимацијата и значката. Секако, органот кој ја издава истовремено е повикан и да ги одземе легитимацијата и значката. Очигледно е и повеќе од логично е дека инспекторот не смее во своето работење да се однесува надвор од пропишаните стандарди на професионално работење и на етичките норми за постапување.

Согласно став 3, образецот, формата и содржината на службената легитимација и значка, како и начинот на нивното издавање и одземање, ги пропишува директорот на Дирекцијата.

Доколку го генерализираме анализираниот став ќе дојдеме до заклучок дека сè поголемата специјализација која е присутна во вршењето инспекциски надзор условува да се издаваат посебни легитимации и значки, а следствено тие мора да бидат пропишани во посебен образец, форма и содржина, со правилник донесен од директорот на Дирекцијата за безбедност на класифицирани информации.

Предвидениот Правилник за образецот, формата и содржината на службената легитимација и значка на инспекторот за безбедност на класифицирани информации, и за начинот на нивното издавање и одземање е донесен и објавен во „Службен весник на Република Северна Македонија“ број 240/20.

Член 85

Заради вршење на инспекциски надзор, органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, како и други правни и физички лица се должни да овозможат непречено вршење на надзорот од областа на безбедноста на класифицираните информации.

Инспекцискиот надзор може да биде редовен, вонреден или контролен.

Редовниот инспекциски надзор опфаќа надзор над спроведувањето на овој закон и се врши според Годишен план и месечен план за работа на секој инспектор

што директорот на Дирекцијата ги донесува согласно со закон.

Вонредниот надзор се врши врз основа на иницијатива поднесена од органите на државната и локалната власт основани согласно со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, физички или правни лица, како и во случај на сомневање на инспекторот (по службена должност).

Контролниот инспекциски надзор се врши по истекот на рокот определен во решението за отстранување на утврдени недостатоци.

При вршењето на инспекцискиот надзор, инспекторите имаат право на пристап и увид во секое време и без најава, во објекти, деловни простории, станбени простории и во простории во кои се ракува и се чуваат класифицирани информации.

За вршење на работите од ставот б на овој член во станбени простории, инспекторите се должни да обезбедат судски налог.

При вршењето на инспекцискиот надзор, инспекторите може да побараат присуство на овластено лице од органот на државната управа надлежен за вршење на работите од областа на полициските работи, заради нивна заштита.

Со член 85 став 1 се определува обврската заради вршење на инспекциски надзор, органите на државната и на локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, како и други правни и физички лица да овозможат непречено вршење на надзорот од областа на безбедноста на класифицираните информации. Односно, ова значи обврска сите субјекти на надзорот да го овозможат неговото непречено вршење. Тоа подразбира сè што е потребно да се стави на располагање за да се согледаат реалните состојби од страна на инспекторите кои го спроведуваат инспекцискиот надзор и ако се евидентираат одредени отстапувања треба да се преземат одредени корективни активности. За да се овозможи непречено вршење на надзорот мора да постои определен вид на соработка. Кога станува збор за отсуство на соработка на правното или физичкото лице кои се предмет на надзор со вршителот на надзорот се наметнуваат неколку дилеми. Првата е во насока на т.н. прикриено отсуство на соработка, односно секогаш е потешко да се измери колкав е квантуумот на документацијата која е потребна за надзорот, а не е доставена за време на неговото вршење (секогаш постои можност да биде дополнително доставена), а уште попроблематична и која вклучува субјективитет бидејќи ставот на вршителот на надзорот и лицата (правни и физички) каде се врши надзорот може објективно да биде различен. Вршителот на надзорот, односно инспекторот треба да биде прецизен и конкретен во своите барања, конзистентен, објективен и непристрасен и да заврши со надзорот во моментот кога ќе ја анализира состојбата и оцени дека тоа е доволно за да донесе соодветен заклучок, наместо да бара одново нови информации итн. кога тоа е непотребно и неоправдано.

Попречувањето или оневозможувањето на вршењето надзор врз правните и врз физичките лица од страна на инспекторите не е опфатено со прекршочните одредби од овој закон. Постоенето на ваква одредба треба директно да биде насочена кон одговорното лице во правното лице, кое го извршува законското битие на прекршокот кое треба да е пропишано алтернативно и тоа како: попречување

на вршењето надзор, односно неовозможување вршење надзор; прикривање на бараната документација, односно нејзино недавање на располагање пред вршителот на надзорот, во случајов инспекторот, или попречување на надзорот преку недавање на потребните документи, податоци и информации, за што на прекршителот треба да му се изрече висока глоба. Сепак, Законот за инспекциски надзор, којшто се применува за сè што не е опфатено со одредбите на Законот за класифицирани информации(*) предвидува прекршок за дејствија кои значат попречување на вршењето инспекциски надзор. Во член 98 став 1 од Законот за инспекциски надзор, се предвидени како прекршочни дејствија, меѓудругото, неовозможувањето пристап до простории, производи, неовозможување увид во документација итн.⁴⁸

Во ставот 2, 3, 4 и 5 на овој член се утврдува начинот на спроведување на инспекцискиот надзор, кој може да биде редовен, вонреден или контролен. Редовниот инспекциски надзор опфаќа надзор над спроведувањето на овој закон и се врши според годишен план и месечен план за работа на секој инспектор коишто директорот на Дирекцијата ги донесува во согласност со закон. Значи, редовен надзор се спроведува постојано и се подразбира како дел од еден континуиран процес во кој надзорот е востановен според редовно утврдена динамика. Ваквите прерогативи се составен дел и на Законот за инспекциски надзор во кој во член 69 став 1 се вели дека редовниот инспекциски надзор е инспекциски надзор врз спроведувањето на соодветните закони и прописите донесени врз основа на тие закони и се врши според однапред предвиден распоред во годишниот план.⁴⁹ Оваа одредба дава поширока рамка и можност ако се утврди дека е потребен и дополнителен надзор дека може да се направи и вонреден и контролен надзор.

Според Правилникот за начинот на вршење инспекциски надзор⁵⁰, редовниот инспекциски надзор кај ист субјект се врши еднаш годишно.

Вонреден надзор најчесто се спроведува дополнително, независно од планираната динамика за спроведување надзор, или како што е наведено во став 4 на овој член, вонредниот надзор се врши врз основа на иницијатива поднесена од органите на државната и на локалната власт основани во согласност со Уставот на Република Северна Македонија и со закон, правни лица основани од Републиката или од општините, градот Скопје и општините во градот Скопје, физички или правни лица, како и во случај на сомневање на инспекторот (по службена должност).

Вонредниот инспекциски надзор, по правило, е ненајавен инспекциски надзор и истиот се спроведува во најбрзо време по добивањето на иницијативата, односно како што предвидува Правилникот во член 2, став 3, најдоцна во рок од 15 работни дена од приемот на иницијативата.

Контролниот инспекциски надзор се врши по истекот на рокот определен во инспекцискиот акт за отстранување на утврдени недостатоци, односно контролниот надзор опфаќа: непосреден увид во пропишаните мерки, увид во активностите за отстранување на неправилностите, односно како што е пропишано во Законот за инспекциски надзор, контролниот инспекциски надзор е инспекциски надзор кој се врши по службена должност со цел инспекторот да утврди дали субјектот на инспекцискиот надзор, по истекот на рокот определен во инспекцискиот акт, при претходно извршен редовен или вонреден инспекциски надзор: постапил по инспекцискиот акт во целост; делумно постапил по инспекцискиот акт или не

⁴⁸ Подетално в. Закон за инспекциски надзор, член 98.

⁴⁹ Исто, член 69.

⁵⁰ Правилник за начинот на вршење инспекциски надзор, „Службен весник“ број 246/20, член 2, став 2.

постапил по инспекцискиот акт.⁵¹

Во согласност со став 6, при вршењето на инспекцискиот надзор, инспекторите имаат право на пристап и увид во секое време и без најава, во објекти, деловни простории, станбени простории и во простории во кои се ракува и се чуваат класифицирани информации и секако, како што е наведено во став 7 за вршење на работите од ставот 6 на овој член, во станбени простории инспекторите се должни да обезбедат судски налог. Ова од причина што станбените простории ја уживаат уставната и казненоправната заштита на неповредливоста на домот.

Воспоставувањето на систем на надзор, кој воедно е и демократски и ефикасен, е еден од посериозните предизвици. Позитивен чекор во спроведувањето на ефикасен надзор е правото на инспекторите да имаат пристап и увид во секое време без најава во објекти, деловни простории, станбени простории (само со налог) и во простории во кои се ракува и се чуваат класифицирани информации, односно својствено за надзорот е сè што се работи да мора да биде контролирано. Сепак, треба да се внимава инспекцискиот надзор и работата на инспекторите да биде транспарентна, демистифицирана и треба да биде во функција на откривање незаконитости во работењето. Со тоа се создава и позитивен однос на контролираните правни и физички лица за нивната работа и задачите што ги преземаат.

Во став 8 на овој член стои дека при вршењето на инспекцискиот надзор, инспекторите може да побараат присуство на овластено лице од органот на државната управа надлежен за вршење на работите од областа на полициските работи, заради нивна заштита. Во рамките на постапувањето може да дојде до одредени ситуации во кои инспекторите при вршење на инспекциски надзор можат да се соочат со непријатни ситуации, отпор и слично, особено кога имаат законска можност без најава да пристапат во објекти, деловни простории, станбени простории и во простории во кои се ракува и се чуваат класифицирани информации, но и во други ситуации при вршење на редовен, вонреден или контролен надзор. За да не дојде до тоа, по претходна процена на ситуацијата, инспекторите можат да побараат асистенција од Министерството за внатрешни работи за да го спроведат потребниот инспекциски надзор таму каде што е планиран.

Член 86

Ако при вршењето на инспекцискиот надзор, инспекторот утврди недостатоци и неправилности во врска со исполнетоста на условите за безбедност на класифицираните информации, донесува решение со кое наредува отстранување на утврдените недостатоци и неправилности во определен рок.

Против решението на инспекторот од ставот 1 на овој член, може да се поднесе жалба во рок од 15 дена од денот на приемот на решението.

По жалбата на решението на инспекторот одлучува Државната комисија за одлучување во втор степен од областа на инспекцискиот надзор и прекршочната постапка.

Значењето на вршењето надзор врз правните и физичките лица е потенцирано со одредбата на член 86 став 1 од овој закон. Оваа одредба е директно насочена кон утврдените недостатоци и неправилности во врска со исполнетоста на условите за

⁵¹ Закон за инспекциски надзор, член 76 и Правилник за начинот на вршење инспекциски надзор, член 2, став 4.

безбедност на класифицираните информации при вршење инспекциски надзор. Во случај кога инспекторот ќе констатира дека постојат неправилности и недостатоци, односно дека контролираните субјекти кои се предмет на инспекциски надзор не се придржуваат на Законот и на другите прописи кои ја регулираат оваа материја, инспекторот ќе донесе решение со кое се наредува отстранување на утврдените недостатоци и неправилности во определен рок. Ова е потврда на теоретските стојалишта дека инспекцискиот надзор, иако во крајна линија е репресивен, тој е првенствено превентивен. Правното лице и физичкото лице кои работат со класифицирани информации треба да преземат конкретни чекори за отстранување на евентуалните недостатоци.

Законодавецот и тука не ја „заборавил“ двостепеноста, па засегнатите субјекти со надзорот имаат право да поднесат жалба, како што е наведено во став 2 на истиот член, ако сметаат дека решението на инспекторот не ја одразува реалната ситуација во работењето со класифицирани информации и се оштетени во постапката со која се утврдило дека дошло до отстапување од пропишаните стандарди утврдени со правната регулатива што би значело дека се направени одредени недоследности во нивната работа.

Рокот за поднесување жалба изнесува 15 дена од денот на приемот на решението, а надлежен орган за одлучување по жалбата е Државната комисија за одлучување во втор степен од областа на инспекцискиот надзор и прекршочната постапка.⁵²

Во согласност со Законот за основање на Државната комисија за одлучување во втор степен од областа на инспекцискиот надзор и прекршочната постапка, Комисијата во постапката за решавање по жалби ги применува одредбите од Законот за општата управна постапка, Законот за инспекциски надзор и Законот за прекршоците, доколку со овој или друг закон поинаку не е уредено. Во согласност со член 11 од истиот закон, против решението на Државната комисија може да се покрене управен спор пред надлежен суд, а тужбата против таквото решение на Државната комисија не го одлага неговото извршување.

Член 87

За извршениот инспекциски надзор, инспекторот составува записник со наод на состојбата кој го доставува на начин и во рок предвиден со закон.

За предложените мерки за отстранување на недостатоците и неправилностите инспекторот донесува решение со рокови за нивно извршување. Одговорното лице во субјектот на надзорот е должно да постапи според решението и да го извести инспекторот за преземените активности.

Членот 87 треба да се чита и во контекст на членот 86 бидејќи уредува ситуација од ставот 1 на тој член. Овие одредби од член 87 се директно насочени кон правното и физичкото лице каде се врши инспекцискиот надзор и се однесуваат на констатирани недостатоци и неправилности што го попречуваат извршувањето на законското битие. За споменатите пропусти и општо за која било констатирана состојба инспекторот е должен да состави записник со наод за состојбата и го доставува на начин и во рок предвиден со закон. Во овој контекст се земаат предвид одредбите на Законот за инспекциски надзор кои предвидуваат за извршениот инспекциски надзор, утврдената фактичка состојба, констатираните и утврдени

⁵² Закон за основање на Државна комисија за одлучување во втор степен во областа на инспекцискиот надзор и прекршочната постапка, „Службен весник на Република Македонија“, број 130/14, 53/16 и 11/18.

неправилности и недостатоци, забелешки, изјави и други релевантни факти и околности, инспекторот да состави писмен записник на местото на вршење на инспекцискиот надзор.⁵³ Записникот го потпишуваат инспекторот и субјектот на инспекцискиот надзор на кој му се предава еден примерок. Ако субјектот на инспекцискиот надзор одбие да го потпише записникот, инспекторот ќе ги наведе причините за одбивањето. По исклучок, кога поради обемот и сложеноста на инспекцискиот надзор, неговата природа и околностите на работа, не е можно да се состави записник на местото на вршење на надзорот, записникот се составува во службените простории на инспекциската служба во рок од три дена од денот на инспекцискиот надзор со образложение на причините за тоа.⁵⁴

Како што е вообичаено, кога ќе се констатираат одредени недоследности и неправилности во работењето се донесува решение за нивно отстранување. Во истиот член 87, во наредните ставови имплицитно се укажува дека одговорното лице во субјектот на надзорот е должно да постапи според решението и да го извести инспекторот за преземените активности. Во решението инспекторот ќе определи рокови за кои треба да се отстранат утврдените недостатоци и неправилности. Како што може да се заклучи, роковите на некој начин ги обврзуваат и двете страни. Во основа, интенцијата на законодавецот е да го ограничи времето во кое треба да се преземат конкретните мерки за отстранување на неправилностите и недоследностите. Субјектот треба да го извести по правило инспекторот за преземените активности. Ваквите решенија на инспекторот се основа и за т.н. контролен инспекциски надзор.

Член 88

Ако инспекторот утврди дека во употреба се наоѓаат уреди, технички средства, инсталации и системи кои не одговараат на пропишаните безбедносни стандарди и критериуми за заштита на класифицирани информации, со решение изрекува забрана на нивна употреба и нивно отстранување.

Со одредбите на овој член, статуирана е обврска на правните и на физичките лица кои работат со класифицирани информации континуирано да се грижат за пропишаните безбедносни стандарди за заштита на класифицирани информации и да не дозволат во употреба да се наоѓаат уреди, технички средства, инсталации и системи кои не се во согласност со пропишаните стандарди. Сосема е логична одредбата дека ако се евидентира ваква ситуација ќе биде донесено решение со кое ќе се забрани нивната употреба и ќе се бара нивно отстранување. Неисполнување на кој било од условите се смета за сериозно прекршување на Законот.

Потребата од поголем надзор над законското работење во сферата на употреба на уреди, технички средства, инсталации и системи е и сè поголемата опасност која доаѓа од развојот на техниката и технологијата, посебно на информатичката технологија.

Член 89

Ако инспекторот при вршењето на надзорот утврди дека постои непосредна опасност од нарушување на безбедноста на објектите или просториите, документите, опремата, системите и лицата во безбедносниот појас, безбедносната зона или административната зона, со решение изрекува забрана за користење на просторот, објектот или дел од објектот.

⁵³ Закон за инспекциски надзор, член 82, став 1.

⁵⁴ Исто, член 82, став 2 и 3.

Ова е јасна рестриктивна норма во поглед на ситуации на директна претстојна опасност за безбедноста. Имено, ако инспекторот при вршењето на надзорот утврди дека постои непосредна опасност од нарушување на безбедноста на објектите или просториите, документите, опремата, системите и лицата во безбедносниот појас, безбедносната зона или административната зона, со решение изрекува забрана за користење на просторот, објектот или дел од објектот.

Суштината на решението со кое се изрекува забрана за користење простор, објект или дел од објект итн. е заштита од штетни последици чиешто настапување е многу веројатно и би значеле повреда и уништување на значајни правни добра, а итноста на ситуацијата е основа за нужноста на ваквото решение.

Член 90

Заради извршувањето на решението од членовите 86 став 1 и 88 од овој закон, инспекторот извршува запечатување на предметниот објект или простории.

Запечатувањето од ставот 1 на овој член се означува со жиг на Дирекцијата.

Содржината и формата на жигот, како и начинот на запечатување, со правилник ги пропишува директорот на Дирекцијата.

Одредбата од став 1 на овој член, предвидува инспекторот да изврши запечатување на предметен објект или простории заради извршување на решението од членовите 86 став 1 и 88 од овој закон. Со тоа се оневозможува нивното натамошно користење до моментот на отстранување на недостатоците. Запечатувањето го врши инспектор и во согласност со став 2 на истиот член тоа се врши со жиг на Дирекцијата, кој од аспект на форма и содржина се уредува со посебен правилник кој го уредува и начинот на запечатување. Правилникот е донесен од страна на директорот на Дирекцијата и е објавен во „Службен весник“ број 187/2020.

Во согласност со неговите одредби, жигот има форма на круг со пречник од 30 мм, изработен од метал за втиснување врз восок за печатење, кој е прицврстен на дрвена рачка, а запечатувањето со жигот се врши на црвен восок и жолтоцрвен конец (лента).

Член 91

По отстранување на утврдените недостатоци, поради кои е изречена мерката забрана, а по писмено барање на субјектот на кој му е изречена мерката, инспекторот извршува отпечатување.

Овој член се надоврзува на претходните, односно уредува дека во случај на отстранување на утврдените недоследности, поради кои е изречена мерка на забрана, а по претходно писмено барање на субјектот на кој му е изречена мерката, инспекторот врши отпечатување. Дирекцијата, поточно нејзините инспектори имаат целосна супрематија во делот на запечатување и отпечатување, односно тоа е етаблирано право кое веќе егзистира и се извршува по реално настаната потреба, па кога потребата од запечатувањето ќе отпадне, инспекторот треба да изврши отпечатување.

Член 92

Во вршењето на надзорот во примената на одредбите од овој закон и другите прописи од областа на безбедноста на класифицираните информации, инспекторите можат да наредат преземање на следниве мерки:

- ▶ демонтирање, преместување или отстранување на опрема, уреди, инсталации и системи со кои се загрозува безбедноста на класифицираните информации,
- ▶ определување на безбедносен појас, безбедносни зони и административни зони околу објектот, просторот или просторијата во објектот во кој се ракува или се чуваат класифицирани информации,
- ▶ поставување на безбедносна информатичко-комуникациска опрема, системи и инсталации за безбедност на класифицираните информации,
- ▶ преместување или отстранување на лица без соодветен безбедносен сертификат или без соодветна дозвола за пристап во безбедносен појас околу објектот и од безбедносни и административни зони во објектот во кој се ракува или се чуваат класифицирани информации,
- ▶ преместување или отстранување на возила без соодветна дозвола за пристап во безбедносен појас околу објектот и во административни зони во објектот во кој се ракува или се чуваат класифицирани информации,
- ▶ изработка на интерни акти за процена на безбедносниот ризик за класифицирани информации и за нивна заштита во случај на вонредни околности,
- ▶ ажурирање и корекција на евиденциите на класифицирани информации и нивно отстранување и уништување,
- ▶ обезбедување на пропишани услови за дисеминација и пренос на класифицирани информации,
- ▶ забрана за прием, ракување, отстапување и чување на класифицирани информации и
- ▶ други мерки за кои инспекторот ќе утврди дека се во функција на заштитата на класифицирани информации во субјектот на надзор.

Надзор над законитоста на работењето на субјектите кои чуваат и во кои се ракува со класифицирани информации остваруваат овластени службени лица за надзор, односно инспектори кои можат да наредат преземање на повеќе мерки. Во став 1 на овој член таксативно се наведени мерките чиешто извршување може да го наредат инспекторите во согласност со одредбите на Законот за класифицирани информации(*). Се работи за мерки кои имаат доминантно превентивен карактер, а тоа се следните: демонтирање, преместување или отстранување на опрема, уреди, инсталации и системи со кои се загрозува безбедноста на класифицираните информации; определување на безбедносен појас, безбедносни зони и административни зони околу објектот, просторот или просторијата во објектот во кој се ракува или се чуваат класифицирани информации; поставување на безбедносна информатичко-комуникациска опрема, системи и инсталации за безбедност на класифицираните информации; преместување или отстранување на лица без соодветен безбедносен сертификат или без соодветна дозвола за пристап во безбедносен појас околу објектот и од безбедносни и административни зони во објектот во кој се ракува или се чуваат класифицирани информации; преместување или отстранување на возила без соодветна дозвола за пристап во безбедносен појас околу објектот и во административни зони во објектот во кој се ракува или

се чуваат класифицирани информации; изработка на интерни акти за процена на безбедносниот ризик за класифицирани информации и за нивна заштита во случај на вонредни околности; ажурирање и корекција на евиденциите на класифицирани информации и нивно отстранување и уништување; обезбедување на пропишани услови за дисеминација и пренос на класифицирани информации; забрана за прием, ракување, отстапување и чување на класифицирани информации и други мерки за кои инспекторот ќе утврди дека се во функција на заштитата на класифицирани информации во субјектот на надзор. Евидентно, овие мерки се во функција на заштита на класифицираните информации во субјектот на надзор.

Член 93

Ако привршењена надзор инспекторот утврди повредана закон и други прописи која претставува прекршок, поднесува барање за поведување на прекршочна постапка согласно со одредбите од овој закон и Законот за прекршоците.

Ако при вршењето на надзорот инспекторот смета дека повредата претставува кривично дело, е должен веднаш да го извести директорот на Дирекцијата заради поведување постапка пред надлежен орган.

Со член 93 став 1 законодавецот предвидува должност за преземање на дејствија во насока на поведување соодветна постапка со која во крајна линија ќе се санкционира повредата на Законот и другите прописи која претставува прекршок или кривично дело.

Патака, инспекторот е должен да поднесе барање за поведување на прекршочна постапка против лице кое ќе го повреди Законот и кое постапува или постапувало спротивно на Законот и на другите прописи во областа на класифицирани информации. Очигледно е дека во овој случај, инспекторот има суверено право да оцени дали се исполнети условите за барање за поведување прекршочна постапка со која се бара против лицето да се поведе прекршочна постапка врз основа на која ќе му се изрече и прекршочна санкција. Постапката се води согласно прекршочните одредби од Законот за класифицирани информации(*) и Законот за прекршоците.

Според одредбата од став 2 на овој член доколку при вршењето на надзорот инспекторот смета дека повредата претставува кривично дело, тој е должен веднаш да го извести директорот на Дирекцијата заради поведување постапка пред надлежен орган. Тоа подразбира дека директорот на Дирекцијата е должен веднаш да преземе мерки и да ги извести надлежните органи заради понатамошно постапување во согласност со закон, односно да поднесе кривична пријава, да го извести Јавното обвинителство, кое понатаму, низ соодветна процедура ќе ги испита наводите, фактите и околностите и ќе донесе одлука дали ќе преземе кривично гонење.

ГЛАВА СЕДМА

ПРЕКРШОЧНИ ОДРЕДБИ

Член 94

Глоба во износ од 3.000 до 5.000 евра во денарска противвредност се изрекува за прекршок на правното лице-корисник на класифицирани информации, ако:

- ▶ не ги спроведе мерките за административна, физичка, безбедност на комуникацискоинформациони системи, безбедност на лицата-корисници на класифицираните информации или индустриска безбедност на класифицираните информации, согласно со одредбите од членовите 26, 28, 29, 31, 32 и 33 од овој закон,
- ▶ не постапува со класифицираните информации, согласно со одредбата од членот 56 став 1 од овој закон (освен ако дејствието не претставува кривично дело),
- ▶ не извести за престанок на исполнетост на некој од условите врз основа на кои е издаден безбедносен сертификат, согласно со одредбите на членот 42 од овој закон,
- ▶ го попречува извршувањето на инспекцискиот надзор согласно со одредбите на членот 79 од овој закон.

Глоба во износ од 1.000 до 2.000 евра во денарска противвредност се изрекува за прекршок на одговорното лице во правното лице-корисник на класифицирани информации за прекршоците од ставот 1 на овој член.

Глоба во износ од 500 до 1.000 евра во денарска противвредност се изрекува за прекршок на физичкото лице-корисник на класифицирани информации за прекршоците од ставот 1 на овој член.

Во член 94, како и во наредните шест члена од овој закон, законодавецот предвидел глоби за сторени прекршоци во однос на несоодветната примена на овој закон за правното лице-корисник на класифицирани информации, одговорното лице во правното лице-корисник на класифицирани информации и за физичкото лице-корисник на класифицирани информации. Водејќи се од одредбите на Законот за прекршоците, и тоа особено во делот на препознавањето на областите во коишто може да се изречат повисоки глоби за прекршоците од оние предвидени со Законот (општиот закон) за физичко лице и за одговорното лице во правно лице,⁵⁵ законодавецот во овој член предвидел повисоки глоби за прекршоците во сферата на класифицираните информации заради природата и

⁵⁵ Исто, член 26, став 4 и 5.

сериозноста на штетите по државата што би можеле да настанат со незаконитото ракување со класифицираните информации и нивното отстапување на користење на неовластени лица. Неовластеното откривање на класифицирани информации би можело штетно да влијае на заштитата на здравјето на луѓето, заштитата на природните богатства, животната средина, заштита на културното наследство, а класифицирани информации може да бидат откриени на неовластени лица од користољубие или да предизвикаат поголема имотна штета.

Како резултат на тоа законодавецот предвидел глоба во износ од 3.000 до 5.000 евра во денарска противвредност за правното лице-корисник на класифицирани информации, ако: не ги спроведе мерките за административна, за физичка, за безбедност на комуникациско-информациските системи, за безбедност на лицата-корисници на класифицираните информации или за индустриска безбедност на класифицираните информации, согласно со одредбите од членовите 26, 28, 29, 31, 32 и 33 од овој закон; не постапува со класифицираните информации, согласно со одредбата од членот 56 став 1 од овој закон (освен ако дејствието не претставува кривично дело); не извести за престанок на исполнетост на некој од условите врз основа на кои е издаден безбедносен сертификат, согласно со одредбите од членот 42 од овој закон, и го попречува извршувањето на инспекцискиот надзор согласно со одредбите од членот 79 од овој закон.

Во вториот став од овој член законодавецот предвидел глоба во износ од 1.000 до 2.000 евра во денарска противвредност за прекршок на одговорното лице во правното лице-корисник на класифицирани информации за прекршоците наведени во ставот 1 на овој член. А во третиот став, предвидел глоба во износ од 500 до 1.000 евра во денарска противвредност за прекршок на физичкото лице-корисник на класифицирани информации за прекршоците од ставот 1 на овој член.

Член 95

Глоба во износ од 1.500 до 2.000 евра во денарска противвредност се изрекува за прекршок на правното лице-корисник на класифицирани информации, ако не ги преземе потребните активности за прием, обработка, утврдување на корисниците и не изврши дисеминација на класифицираните информации до нив, согласно со одредбите на членот 26 од овој закон.

Глоба во износ од 1.000 до 1.500 евра во денарска противвредност се изрекува за прекршок на одговорното лице во правното лице-корисник на класифицирани информации за прекршокот од ставот 1 на овој член.

Глоба во износ од 500 до 1.000 евра во денарска противвредност се изрекува за прекршок на физичкото лице-корисник на класифицирани информации за прекршокот од ставот 1 на овој член.

Во член 95 законодавецот ги пропишал глобите за прекршок на правното лице-корисник на класифицирани информации, на одговорното лице во правното лице-корисник на класифицирани информации и на физичкото лице-корисник на класифицирани информации ако не ги преземат потребните активности за прием, обработка, утврдување на корисниците и не изврши/ат дисеминација на класифицираните информации до нив, во согласност со одредбите на членот 26 од овој закон. Притоа, износот на пропишаната глоба за прекршок на правното лице изнесува од 1.500 до 2.000 евра во денарска противвредност, за прекршок на одговорното лице изнесува од 1.000 до 1.500 евра во денарска противвредност, а

за прекршок на физичкото лице од 500 до 1.000 евра во денарска противвредност.

Член 96

Глоба во износ од 1.500 до 2.000 евра во денарска противвредност, се изрекува на правно лице кое ќе постапи спротивно на обврската за заштита на класифицирани информации означени со степен „ИНТЕРНО“ од членот 47 став 2 и во смисла на членот 2 од овој закон.

Глоба во износ од 1.000 до 1.500 евра во денарска противвредност, се изрекува на одговорното лице во правното лице за прекршокот од ставот 1 на овој член.

Глоба во износ од 500 до 1.000 евра во денарска противвредност, се изрекува на физичкото лице за прекршокот од ставот 1 на овој член.

Во член 96 се пропишани глобите во однос на незаконитото постапување со класифицирани информации означени со степен „ИНТЕРНО“, односно за постапување спротивно на обврската за нивна заштита, уредена во членот 47 став 2 и во смисла на членот 2 од овој закон. Притоа е пропишана глоба во износ од 1.500 до 2.000 евра во денарска противвредност за прекршок на правното лице, глоба во износ од 1.000 до 1.500 евра во денарска противвредност е пропишана за прекршок на одговорното лице во правното лице, а за прекршок на физичкото лице е пропишана глоба од 500 до 1.000 евра во денарска противвредност.

Член 97

Глоба во износ од 500 до 1.000 евра во денарска противвредност, се изрекува на правно лице кое спротивно на членот 12 открие информација со ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“.

Глоба во износ од 450 до 700 евра во денарска противвредност, се изрекува на одговорното лице во правното лице за прекршокот од ставот 1 на овој член.

Глоба во износ од 300 до 500 евра во денарска противвредност, се изрекува на физичкото лице за прекршокот од ставот 1 на овој член.

Во член 97 се пропишани глобите за постапување спротивно на одредбите од членот 12 од овој закон, односно за откривање информација со ознака „ЗА ОГРАНИЧЕНА УПОТРЕБА“. Притоа износот на пропишаната глоба за прекршок на правното лице изнесува од 500 до 1.000 евра во денарска противвредност, за прекршок на одговорното лице изнесува од 450 до 700 евра во денарска противвредност, а за прекршок на физичкото лице од 300 до 500 евра во денарска противвредност.

Член 98

Глоба во износ од 500 до 1.000 евра во денарска противвредност се изрекува за прекршок на офицерот за безбедност на класифицирани информации, ако:

- не исполни некоја од своите должности наведени во членот 68 од овој закон,
- го попречува вршењето на инспекцискиот надзор согласно со одредбите на членот 79 од овој закон.

Во член 98 законодавецот ги пропишал глобите за прекршок на офицерот за безбедност на класифицирани информации во износ од 500 до 100 евра во денарска противвредност ако не исполни некоја од своите должности наведени во членот 68 од овој закон или ако го попречува вршењето на инспекцискиот надзор согласно со одредбите од членот 79 од овој закон.

Треба да се има предвид дека во секој конкретен случај треба да се испитаат сите околности за да се утврди дали одредено дејствие може да се третира и како кривично дело особено ако сторителот постапувал со умисла или со посебна намера и предизвикал штетна последица соодветна на битието на делото.

Член 99

Глоба во износ од 1.000 до 1.500 евра во денарска противвредност, се изрекува на правното лице-создавач на класифицирана информација кое ќе постапи спротивно на членот 10 став 2 и класифицирана информација за која не е направена потребната проценка за можната штета и последици.

Глоба во износ од 500 до 1.000 евра во денарска противвредност, се изрекува на одговорното лице во правното лице за прекршокот од ставот 1 на овој член.

Глоба во износ од 300 до 500 евра во денарска противвредност, се изрекува на физичкото лице за прекршокот од ставот 1 на овој член.

Законодавецот предвидел глоби за прекршок на правното лице-создавач на класифицирана информација, на одговорното лице во правното лице и на физичкото лице ако постапат спротивно на членот 10 став 2 од овој закон, односно не определат соодветен степен на класификација на информацијата врз основа на проценка за можната штета и последиците кои би произлегле од неовластениот пристап до неа. Притоа, за прекршок на правното лице-создавач на класифицирана информација законодавецот предвидел глоба во износ од 1.000 до 1.500 евра во денарска противвредност, за прекршок на одговорното лице во правното лице предвидел глоба во износ од 500 до 1.000 евра во денарска противвредност, а за прекршокот на физичкото лице предвидел глоба во износ од 300 до 500 евра во денарска противвредност.

Неопределувањето на соодветен степен на класификација на определена информација може да има сериозни последици бидејќи со тоа, наместо да е соодветно заштитена, информацијата останува целосно или делумно достапна на лица кои објективно не би требало да бидат запознаени со нејзината содржина, па тоа може да претставува конкретно загрозување на интереси на државата и да резултира со штетна последица и во таков случај треба да се испитаат можностите за извршена злоупотреба, односно кривично дело.

Член 100

Глоба во износ од 1.500 до 2.000 евра во денарска противвредност, се изрекува на правното лице-создавач на класифицирана информација кое ќе постапи спротивно на членот 16 став 3 и членот 18 став 2 и не го извести корисникот на класифицираната информација за промената на степенот на класификација или за нејзината декласификација.

Глоба во износ од 1.000 до 1.500 евра во денарска противвредност, се изрекува

на одговорното лице во правното лице за прекршокот од ставот 1 на овој член.

Глоба во износ од 500 до 1.000 евра во денарска противвредност, се изрекува на физичкото лице за прекршокот од ставот 1 на овој член.

Во член 100 се пропишани глобите за прекршок на правното лице-создавач на класифицирана информација, на одговорното лице во правното лице и на физичкото лице ако постапат спротивно на членот 16 став 3 и членот 18 став 2 од овој закон и не го известат корисникот на класифицираната информација за промената на степенот на класификација или за нејзината декласификација.

Притоа, за прекршок на правното лице-создавач на класифицирана информација законодавецот предвидел глоба во износ од 1.500 до 2.000 евра во денарска противвредност, за прекршок на одговорното лице во правното лице предвидел глоба во износ од 1.000 до 1.500 евра во денарска противвредност, а за прекршокот на физичкото лице предвидел глоба во износ од 500 до 1.000 евра во денарска противвредност.

ПОСТАПКА ЗА ПОРАМНУВАЊЕ СО ИЗДАВАЊЕ НА ПРЕКРШОЧЕН ПЛАТЕН НАЛОГ

Член 101

За прекршоците утврдени во овој закон, согласно со Законот за прекршоците, инспекторот е должен на сторителот на прекршокот да му издаде прекршочен платен налог, пред да поднесе барање за поведување на прекршочна постапка.

Инспекторот е должен да води евиденција за издадените прекршочни платни налози и за нивниот исход.

Во евиденцијата од ставот 2 на овој член се собираат, обработуваат и чуваат следниве податоци: име и презиме, односно назив на сторителот на прекршокот, живеалиште, односно престојувалиште, седиште, вид на прекршокот, број на прекршочниот платен налог кој му се издава и исходот на постапката.

Личните податоци од ставот 3 на овој член се чуваат пет години од денот на внесување во евиденцијата.

Директорот ја пропишува формата и содржината на прекршочниот платен налог.

За се што не е определено со овој закон, во поглед на прекршочниот платен налог се применуваат одредбите од Законот за прекршоците.

Во член 101 законодавецот го уредува институтот „порамнување“ во прекршочната постапка. Во согласност со Законот за прекршоците⁵⁶, законодавецот

⁵⁶ Закон за прекршоците, „Службен весник на Република Северна Македонија“ број 96/19, член 51.

уредил дека инспекторот за класифицирани информации е должен на сторителот на прекршокот да му издаде прекршочен платен налог, пред да поднесе барање за поведување на прекршочна постапка. Во вториот став е уредено дека инспекторот води евиденција за издадените платни налози во којашто се собираат, обработуваат и чуваат следните податоци: име и презиме, односно назив на сторителот на прекршокот, живеалиште, односно престојувалиште, седиште, вид на прекршокот, број на прекршочниот платен налог кој му се издава и исходот на постапката. Притоа е уредено дека личните податоци се чуваат пет години од денот на внесување во евиденцијата.

Законодавецот предвидел формата и содржината на прекршочниот платен налог со подзаконски акт да ги пропише директорот на Дирекцијата, а за сè што не е определено со овој закон, во поглед на прекршочниот платен налог да се применуваат одредбите од Законот за прекршоците.

Всушност, Законот за прекршоците како *lex generalis* се применува секогаш кога во посебниот закон определен институт или постапка од прекршочното право не се поинаку уредени.

Правилникот за формата и содржината на прекршочниот платен налог е донесен и објавен во „Службен весник на Република Северна Македонија“ број 181/20 и 285/20.

Член 102

За прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

Во член 102 законодавецот предвидел дека за прекршоците утврдени со овој закон, прекршочна постапка води и прекршочна санкција изрекува надлежен суд.

Оваа одредба е во согласност со член 54 став 1 од Законот за прекршоците.

ГЛАВА ОСМА

КАЗНЕНИ ОДРЕДБИ

ОДДАВАЊЕ НА КЛАСИФИЦИРАНИ ИНФОРМАЦИИ СО СТЕПЕН „СТРОГО ДОВЕРЛИВО“ И „ДОВЕРЛИВО“

Член 103

Тој што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што е класифицирана со степен „СТРОГО ДОВЕРЛИВО“ до којашто има пристап согласно со закон и со тоа ги загрози или повреди виталните интереси на Република Северна Македонија, се казнува со затвор од една до пет години.

Тој што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „СТРОГО ДОВЕРЛИВО“, а до која дошол на противправен начин, се казнува со затвор од една до три години.

Тој што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што е класифицирана со степен „ДОВЕРЛИВО“ до којашто има пристап согласно со закон и со тоа ги загрози или повреди важните интереси на Република Северна Македонија, се казнува со затвор од една до три години.

Тој што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „ДОВЕРЛИВО“, а до која дошол на противправен начин, се казнува со парична казна или затвор од шест месеци до три години.

Ако делото од ставовите 1 и 3 на овој член, е извршено за време на воена состојба, сторителот се казнува со затвор од една до десет години.

Обидот за делото од ставовите 2, 3 и 4 на овој член, е казнив.

Ако делото од ставовите 1 и 3 на овој член, е сторено од небрежност, сторителот се казнува со парична казна или затвор до една година.

Во член 103 е инкриминирано оддавањето на класифицирани информации со степен „СТРОГО ДОВЕРЛИВО“ и „ДОВЕРЛИВО“.

Со воведувањето на овие одредби во Законот се пополнува моменталниот

вакуум, односно празнината во казнената регулатива во однос на незаконското постапување со информации со степените на класификација „СТРОГО ДОВЕРЛИВО“ и „ДОВЕРЛИВО“.

Имено, Кривичниот законик содржи одредби само во однос на информациите што се сметаат за „ДРЖАВНА ТАЈНА“ и пропишува казни санкции за нивното оддавање во рамките на глава дваесет и осма: Кривични дела против државата, во член 317.⁵⁷

Од таа причина, во првиот став на овој член законодавецот предвидел дека лицето што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што е класифицирана со степен „СТРОГО ДОВЕРЛИВО“ до којашто има пристап во согласност со закон и со тоа ги загрози или повреди виталните интереси на Република Северна Македонија, ќе се казни со затвор од една до пет години.

Во вториот став предвидел одговорност за лицето што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „СТРОГО ДОВЕРЛИВО“, а до која дошол на противправен начин, при што ваквото дејствие се казнува со затвор од една до три години.

Обликот од став 1 според законодавецот е потешок од обликот на делото од став 2, бидејќи во првиот случај противправното дејствие го врши лице кому класифицираната информација е му е доверена, што значи дека тој ја злоупотребува својата должност, во услови кога се очекува толкму тој да ја пружи потребната заштита од неовластен пристап. Делото од ставот 2 значи дека сторителот дошол на противправен, односно недозволен, незаконски начин со класифицираната информација, при што истата ќе ја направи достапна на неповикано лице или на јавноста.

Во третиот став законодавецот предвидел дека лицето што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што е класифицирана со степен „ДОВЕРЛИВО“ до којашто има пристап во согласност со закон и со тоа ги загрози или повреди важните интереси на Република Северна Македонија, ќе се казни со затвор од една до три години. А, во четвртиот став утврдил дека тој што на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што знае дека е класифицирана со степен „ДОВЕРЛИВО“, а до која дошол на противправен начин, се казнува со парична казна или затвор од шест месеци до три години.

Во петтиот став законодавецот предвидел т.н. квалифициран облик на делото, поточно доколку делото од ставовите 1 и 3 е извршено за време на воена состојба, сторителот ќе се казни со затвор од една до десет години.

Воедно, експлицитно предвидел и дека обидот за делото од ставовите 2, 3 и 4 на овој член е казнив, бидејќи согласно пропишаната казна за делата од наведените ставови не може да се примени одредбата од член 19 од Кривичниот законик за казнивост на обидот. Всушност, обидот за сите дела од ставовите 1-4 е казнив, само што за ставот 1 тоа е врз основа на член 19 од Кривичниот законик, а за другите ставови тоа е експлицитно предвидено.

Законодавецот го санкционира и стореното дејствие од небрежност, па во последниот став на овој член предвидел дека ако лицето од небрежност на јавноста или на неповикано лице соопшти, предаде или стори достапна информација што е класифицирана со степен „СТРОГО ДОВЕРЛИВО“ или „ДОВЕРЛИВО“ до којашто има пристап во согласност со закон и со тоа ги загрози или повреди виталните, односно

⁵⁷ Кривичен законик, член 316 став 6 и член 317.

важните интереси на Република Северна Македонија, дека истиот ќе се казни со парична казна или затвор до една година.

НЕОВЛАСТЕНО ОТКРИВАЊЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЈА УПОТРЕБЕНА ВО СУДСКА ИЛИ ДРУГА ПОСТАПКА

Член 104

Тој што спротивно на закон, неовластено открие класифицирана информација со степен на класификација „ДРЖАВНА ТАЈНА“ за која дознал во судска или друга постапка, се казнува со затвор до пет години.

Доколку класифицираната информација е со степен на класификација „СТРОГО ДОВЕРЛИВО“ или „ДОВЕРЛИВО“, сторителот се казнува со затвор од една до три години.

- ▶ Обидот за делото од ставот 2 на овој член, е казнив.
- ▶ Ако делото од ставовите 1 и 2 на овој член, е сторено од небрежност, сторителот се казнува со парична казна или затвор до една година.

Членот 104 содржи инкриминација на неовластеното откривање на класифицирана информација за која лицето дознало во судска или друга постапка, што претставува новина во однос на досегашната регулатива за класифицирани информации во оваа смисла.

Имено, наместо една класифицирана информација да се декласифицира со цел да биде употребена во судска постапка (како доказ или сл.), со што би се изгубила смислата на класифицирањето бидејќи тоа би претставувало „мала врата“ за доаѓање до сознанија кои е важно да бидат тајни и заштитени, законодавецот предвидува обврска за кое било лице за чување во тајност на информации кои се класифицирани, а за кои тоа дознало во некаква постапка. Притоа, тој не го ограничува тоа само на судските постапки, туку и на други, на пример, управна постапка, со цел да бидат покриени сите можни случаи, дури и оние кои во практиката се многу ретки.

Всушност, судијата кој постапува во вакви предмети (како и јавниот обвинител, ако се работи за предмет во кој тој има надлежност) би требало да има безбедносен сертификат, а оваа одредба би требало да ги покрива другите учесници во постапката, зависно од тоа за каква постапка се работи итн.

Повредата на ваквата прохибитивна казненоправна норма се санкционира соодветно на степенот на класификација на информацијата за која станува збор во конкретниот случај, па врз основа на тоа, се детектираат неколку облици на делото.

Имено, законодавецот предвидел дека лицето што спротивно на закон, неовластено открие класифицирана информација со степен на класификација „ДРЖАВНА ТАЈНА“ за која дознал во судска или во друга постапка, ќе се казни со затвор до пет години, што од казненоправен аспект значи рамка од 30 дена до 5 години затвор.⁵⁸ Доколку класифицираната информација е со степен на класификација „СТРОГО ДОВЕРЛИВО“ или „ДОВЕРЛИВО“, законодавецот предвидел

⁵⁸ В. Кривичен законик, член 35. Имено, во член 35, став 1 се определени општиот законски минимум и максимум на казната затвор кои изнесуваат 30 дена, односно 20 години, а со оглед на фактот што во инкриминацијата од член 104 од Законот за класифицирани информации(*) законодавецот го определил само законскиот максимум, за минимум се применува оној што е предвиден како општ минимум, односно 30 дена.

сторителот да се казни со затвор од една до три години.

Обидот за делата од став 1 и 2 е казнив, при што обидот за делото од став 1 се казнува согласно општата одредба за обид од член 19 од Кривичниот законик,⁵⁹ а обидот делото од став 2 не влегува во опсегот на споменатата одредба од член 19 од Кривичниот законик, па затоа законодавецот во овој член тоа изрично го предвидува.

Доколку делото биде сторено од небрежност, во последниот став на овој член е уредено дека сторителот се казнува со парична казна или затвор до една година, што е сосема оправдано, бидејќи се работи за извршување на делата со полесниот облик на вина – небрежност, додека ставовите 1 и 2 ги опфаќаат умислените облици на делото.

⁵⁹ В. Кривичен законик, член 19. Согласно член 19 став 1 обидот е казнив за кривично дело за кое може да се изрече затвор од 5 години, па оттука член 104 став 1 во поглед на обидот е опфатен со член 19 од Кривичниот законик.

ГЛАВА ДЕВЕТТА

ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 105

Подзаконските акти предвидени со овој закон ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон.

Подзаконските акти донесени врз основа на Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/2004, 113/2007, 145/10, 80/12, 41/14, 21/18 и 83/18), ќе се применуваат до денот на влегувањето во сила на подзаконските акти утврдени со овој закон.

За успешно спроведување на одредбите на Законот за класифицирани информации(*) потребно е донесување на подзаконски акти со кои подетално се регулираат определени дејствија. Во преодните одредби од член 105 законодавецот предвидува дека таквите подзаконски акти ќе се донесат во рок од шест месеци од денот на влегувањето во сила на овој закон, а дека дотогаш ќе се применуваат подзаконските акти донесени врз основа на Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 и 83/18).

Во врска со оваа одредба досега донесени се следните подзаконски акти:

- ▶ Правилник за формата и содржината на обрасците на безбедносниот прашалник и на безбедносните сертификати;⁶⁰
- ▶ Правилник за содржината, формата и начинот на водење на евиденцијата за издадените безбедносни сертификати и за пополнетите безбедносни прашалници и на посебната евиденција за издадените дозволи за пристап до класифицирани информации;⁶¹
- ▶ Правилник за начинот на вршење инспекциски надзор;⁶²
- ▶ Правилник за начинот на полагање на стручниот испит за инспекторите за безбедност на класифицирани информации;⁶³
- ▶ Правилник за формата и содржината на прекршочниот платен налог;⁶⁴
- ▶ Правилник за службената легитимација и значка на инспекторот за безбедност на класифицирани информации, како и за начинот за нивно

⁶⁰ „Службен весник на Република Северна Македонија“ број 123/20.

⁶¹ „Службен весник на Република Северна Македонија“ број 150/20.

⁶² „Службен весник на Република Северна Македонија“ број 246/20.

⁶³ „Службен весник на Република Северна Македонија“ број 219/20.

⁶⁴ „Службен весник на Република Северна Македонија“ број 181/20 и 285/20.

издавање и одземање;⁶⁵

- ▶ Правилник за форма и содржина на жигот на Дирекцијата за безбедност на класифицирани информации и начинот на запечатување;⁶⁶
- ▶ Правилник за образецот на службената легитимација на вработените лица во Дирекцијата за безбедност на класифицирани информации и за начинот на нејзиното издавање.⁶⁷

Во фаза на усогласување со Секретаријатот за законодавство се нацрт-текстовите на следните подзаконски акти:

- ▶ Уредба за начинот на чување и ракување со информациите за ограничена употреба, начинот на промена на степенот на класификација на информацијата, начинот на декласификација на информацијата, начинот на определување на корисниците и вршењето на дисеминација на добиените странски класифицирани информации и мерките и активностите за административна безбедност на класифицирани информации;
- ▶ Уредба за физичка безбедност на класифицирани информации;
- ▶ Уредба за безбедност на лица-корисници на класифицирани информации;
- ▶ Уредба за индустриска безбедност на класифицирани информации;
- ▶ Уредба за безбедност на комуникациско-информациски системи.

Изработен е и нацрт-текстот на Упатството за процесот на менаџирање на ризикот за физичка безбедност на класифицираните информации којшто по усвојувањена новата Уредба за физичка безбедност ќе биде предмет на усогласување со Секретаријатот за законодавство во форма на правилник.

Член 106

Прописите коишто регулираат прашања од областа на класифицираните информации ќе се усогласат со одредбите од овој закон во рок од една година од денот на влегувањето во сила на овој закон.

Во член 106 е предвидено прописите коишто регулираат прашања од областа на класифицираните информации да се усогласат со одредбите од овој закон во рок од една година од денот на влегувањето во сила на овој закон.

Тоа подразбира, пред сè, измени на други прописи, измени и дополнувања со соодветни одредби во други закони чијашто материја има допирни точки со заштитата на класифицираните информации, но посредно значи и потреба од евентуални измени и ставање вон сила на одредби во Кривичниот законик со кои ќе се пропишат казнени санкции и за другите степени на класифицирани информации (иако тоа сега е покриено со овој закон), а не само за информациите што се препознаваат како „ДРЖАВНА ТАЈНА“⁶⁸, како и ставање вон сила на одредбите за оддавање воена тајна и слични опсолетни одредби.

⁶⁵ „Службен весник на Република Северна Македонија“ број 240/20.

⁶⁶ „Службен весник на Република Северна Македонија“ број 187/20.

⁶⁷ „Службен весник на Република Северна Македонија“ број 53/21.

⁶⁸ Кривичен законик, член 317.

Член 107

Безбедносните сертификати издадени до денот на влегувањето во сила на овој закон продолжуваат да важат до истекот на рокот на нивната важност.

Во член 107 законодавецот предвидел дека безбедносните сертификати издадени до денот на влегувањето во сила на овој закон продолжуваат да важат до истекот на рокот на нивната важност. Со тоа, всушност, се спречува важечките сертификати да престанат да важат само заради донесувањето на нов закон, особено што нема причини да се прекине континуитетот на нивната важност до нејзиниот истек, по што продолжувањето на важноста на истите и издавањето нови безбедносни сертификати ќе се врши во согласност со новиот закон.

Непостоењето на оваа одредба би предизвикало криза во работењето на ракувачите со класифицирани информации бидејќи одеднаш сите важечки сертификати на релевантните субјекти во државата би станале неважечки, Дирекцијата би се пренатрупала со барања за нови сертификати, а работата во многу институции би била блокирана со месеци, имајќи го предвид фактот дека процедурата вообичаено трае подолго.

Член 108

Дирекцијата за безбедност на класифицирани информации основана со Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/2004, 113/2007, 145/10, 80/12, 41/14, 21/18 и 83/18), од денот на влегувањето во сила на овој закон продолжува да работи како Дирекцијата за безбедност на класифицирани информации согласно со надлежностите утврдени со овој закон.

Законодавецот обезбедува континуитет во работењето на Дирекцијата за безбедност на класифицирани информации основана со Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 и 83/18) со тоа што во член 108 предвидува дека од денот на влегувањето во сила на овој закон истата продолжува да работи како Дирекција за безбедност на класифицирани информации во согласност со надлежностите утврдени со овој (новиот) закон.

Член 109

Директорот на Дирекцијата за безбедност на класифицирани информации именуван до денот на влегувањето во сила на овој закон продолжува да ја извршува функцијата до истекот на мандатот за кој е именуван.

Во член 109 законодавецот предвидел континуитет и во работата на директорот на Дирекцијата за безбедност на класифицирани информации именуван до денот на влегувањето во сила на овој закон со тоа што уредил дека истиот продолжува да ја извршува функцијата до истекот на мандатот за кој е именуван.

Член 110

Со денот на влегувањето во сила на овој закон, престанува да важи Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/2004, 113/2007, 145/10, 80/12, 41/14, 21/18 и 83/18).

Во член 110 законодавецот предвидел дека со денот на влегувањето во сила на овој закон, ќе престане да важи Законот за класифицирани информации („Службен весник на Република Македонија“ број 9/04, 113/07, 145/10, 80/12, 41/14, 21/18 и 83/18), односно претходниот закон со сите негови измени и дополнувања станува неважечки закон.

Член 111

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

Во последниот член 111 од овој закон е пропишан т.н. *vacatio legis*, односно периодот од објавувањето до влегувањето во сила на законот, односно во овој случај е наведено дека влегувањето во сила ќе биде осмиот ден од денот на неговото објавување во Службен весник на Република Северна Македонија.

CIP - Каталогизација во публикација

Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

351.083.8(497.7)(094.5.072)

342.738(497.7)(094.5.072)

БАКРЕСКИ, Оливер

Коментар на Законот за класифицирани информации [Електронски извор] / Оливер Бакрески, Александра Деаноска-Трендафилова. - Скопје : Центар за управување со безбедносниот сектор - Женева, подружница Скопје ДЦАФ, 2021

Начин на пристапување (URL):

<https://dcaf.ch/resources?type=publications>. - Начин на пристапување

(URL): <https://www.dbki.gov.mk>. - Текст во PDF формат, содржи 114 стр. - Наслов преземен од екранот. - Опис на изворот на ден 01.07.2021. - Фусноти кон текстот

ISBN 978-608-66657-5-3

1. Деаноска-Трендафилова, Александра [автор]

а) Класифицирани информации -- Заштита -- Македонија -- Коментирани закони

COBISS.MK-ID 54250757

