ДЪРЖАВНА КОМИСИЯ
ПО СИГУРНОСТТА
НА ИНФОРМАЦИЯТА

ПЪРВОНАЧАЛНО ОБУЧЕНИЕ

СБОРНИК ЛЕКЦИИ

София, 2020

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

ПЪРВОНАЧАЛНО ОБУЧЕНИЕ

СБОРНИК ЛЕКЦИИ

(ЧЕТВЪРТО ДОПЪЛНЕНО ИЗДАНИЕ)

СОФИЯ, 2020

СЪДЪРЖАНИЕ

РИСКОВИ ФАКТОРИ ЗА ИНТЕРЕСИТЕ НА РЕПУБЛИКА БЪЛГАРИЯ В ОБЛАСТТА НА ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Членството на Република България в Европейския съюз и НАТО постави по-високи изисквания за защита на националната и предоставяната ни от страните-съюзници класифицирана информация (КИ). Нейното опазване е въпрос на национална отговорност и коректност към партньорите. Утвърждаването на гражданското общество в условията на динамично развиващите се информационни технологии поставя нови предизвикателства пред защитата на националната и чуждестранната класифицирана информация.

Понятие за национална сигурност

Понятието **национална сигурност** се появява най-напред в американската политология. За първи път то е употребено от президента Теодор Рузвелт в обръщение към Конгреса на САЩ през 1904 г. за обосноваване на присъединяването на зоната на Панамския канал в интерес на националната сигурност. Това понятие отново се употребява от тридесет и втория президент на САЩ Франклин Делано Рузвелт след извършеното от Япония нападение срещу американската военноморска база Пърл Харбър през декември 1941 год.

Първото определение на националната сигурност в категориите на националните интереси е дадено от известния журналист и политически наблюдател Уолтър Липман. Според него държавата се намира в състояние на сигурност, когато не й се налага да принася в жертва своите законни интереси, за да избегне войната и когато тя е в състояние да защити при необходимост своите интереси чрез водене на война.

В литературата могат да се намерят над 200 определения за понятието национална сигурност. През последните години в България са в „обръщение" десетки определения за национална сигурност. Официалната Концепция за национална сигурност, приета през 1998 г. от Народното събрание на Република България гласи: „Национална сигурност има, когато са защитени основните права и свободи на българските граждани, държавните граници, териториалната цялост и независимостта на държавата, когато не съществува опасност от въоръжено нападение, насилствена промяна на конституционния ред, политически диктат или икономическа принуда за държавата и е гарантирано демократичното функциониране на държавните и гражданските институции, в резултат на което обществото и нацията запазват и увеличават

своето благосъстояние и се развиват. Сигурността е гарантирана, когато страната успешно реализира националните си интереси, цели и приоритети и при необходимост е в състояние ефективно да ги защити от външна и вътрешна заплаха".

Важно значение в разбирането за националната сигурност е поставянето й във фокуса на сигурността на отделния човек. Понятието **лична сигурност** (human security), разглеждано като част от националната сигурност, обхваща условията на живот на отделния човек и изразява потребността му от сигурност в области, в които той изпитва своите непосредствени потребности. Понятието „лична сигурност" е пряко свързано със защитата на правата и свободите на човека. Този фокус към личната сигурност на отделния човек и защитата на неговите права и свободи е ясно дефиниран в параграф 1, т. 13 от Допълнителните разпоредби на Закона за защита на класифицираната информация. Там най-ясно и синтезирано е разтълкувано понятието национална сигурност: „Национална сигурност" е състояние на обществото и държавата, при което са защитени основните права и свободи на човека и гражданина, териториалната цялост, независимостта и суверенитетът на страната и е гарантирано демократичното функциониране на държавата и гражданските институции, в резултат на което нацията запазва и увеличава своето благосъстояние и се развива.

Макар и дефинирани различно, общото в посочените по-горе определения е, че националните измерения на сигурността обхващат всички предизвикателства, рискове, заплахи и опасности за сигурността на ниво държава. Националната сигурност в нейната многоаспектна същност предполага тя да бъде разглеждана като комплексно явление, което се декомпозира на сфери на сигурност в зависимост от различните аспекти на обществения живот. Съдържанието на националната сигурност може да се представи като съвкупност от сфери за сигурност: политическа, икономическа, военна, социална, информационна, екологична и т.н.

Говорейки за опазване на националната сигурност, ние включваме тук и защитата на класифицираната информация като съществен сегмент от националната сигурност. За да защитим класифицираната информация от различни рискове, опасности и заплахи, е необходимо да умеем да ги разпознаваме, да ги идентифицираме, дори да ги предвиждаме и прогнозираме, така че да сведем до минимум вредните последици от тях, а при възможност – да ги премахнем.

Дефиниране и разграничаване на понятията заплаха, опасност и риск

Заплахата е опасност, възможност за поява на нещо неприятно, лошо, закана да се причини някому нещо неприятно, зло. В синонимен и семантичен смисъл за понятието „заплаха” се използват: „страх”, „сплашване”, „заплашване”, „закана”, „риск”, „угроза”, „застрашаване”, „опасност”, „тормоз”.

Заплахата е изказано намерение или демонстрирана готовност за нанасяне на вреди или унищожаване на набелязания обект, било срещу отделна личност или срещу елемент от системата за национална сигурност. По отношение на системата за национална сигурност могат да произтекат действия, изразени или дефинирани по различен начин. Може да съществуват намерение, подготовка и планиране или да се извършат конкретни действия, които имат за цел отслабване на държавата или държавността, вредителство или унищожаване на определени ценности.

Заплахата нанася вреди върху цялостната система на обществения живот, като се започне от отделната личност, групата, колектива, държавата, както и на регионалната и глобалната сигурност. Проблеми с функционирането на държавната администрация, икономическата система и системата за национална сигурност водят до безконтролност на ситуацията и възможност за възникване на гражданско неподчинение, граждански конфликти, гражданска война.

Ще разгледаме заплахата в няколко аспекта. На първо място, по отношение на отделната личност, заплахата е намерение или желание за увреждане на достойнството и интегритета на друг човек. Заплаха може да е публично или персонално отправяне на нападки, изразяване на открито намерение за нанасяне на вреди върху личността на заплашвания човек. Заплахата към високопоставено лице е потенциална възможност определен източник успешно да му въздейства да извърши или да го възпре от извършването на определено действие. Терористи могат да използват заплаха за намаляване на ефективността на силите за сигурност, като се опитват да ги накарат да се страхуват и в резултат – да бездействат. Заплахата може да предизвика намаляване на обществената подкрепа към правителството или да накара гражданите да го бойкотират, като например не гласуват на избори или не участват в референдум. В този смисъл може да се каже, че заплахата е един от ефективните начини за въздействие с така нареченото насочено влияние върху психиката и поведението на даден индивид (например, високопоставеното лице), за да се постигне преследваната от заплашващия цел.

На второ място, заплахата е състояние на средата на сигурност, когато тя е в нормално състояние. Заплаха за сигурността е вероятността от вредно въздействие върху човека, на което обикновено не сме в състояние да се противопоставим или да го неутрализираме. На тази база бихме могли да определим заплахата като състояние на средата за сигурност, което предхожда кризата. Следователно, заплахата като състояние на средата за сигурност сигнализира и предизвестява за загуба на контрол върху факторите на въздействието.

В сферата на информационната сигурност, заплаха е всяка възможност за случаен или целенасочен нерегламентиран достъп до създаваната, обработваната, съхраняваната и пренасяната национална и чуждестранна класифицирана информация. Заплахата представлява реална опасност за системата. Тя може да бъде причинена от човек, предмет или събитие.

Заплаха може да бъде публично или персонално отправяне на нападки, изразяване на открито намерение за нанасяне на вреди върху личността на заплашвания човек. Високият потенциал на заплахата, особено на тази, която е резултат от умишлена човешка дейност, се съдържа в наличието на мотивация, ресурси, метод и начин на действие, чрез които тя може да бъде осъществена.

Заплахата може да се определи и като **опасност, която се намира в етап на възможност да се превърне в действително събитие**. Някои автори споделят виждането, че заплахата е родствено понятие на **опасността** – възможност или вероятност да се случи нещо лошо, някаква беда, нещастие. В социалното битие опасността е свързана с възникването на потенциални или реални явления, събития, процеси. Последните са в състояние да нанесат вреди, нежелани последствия на човек, държава, регион или на планетата.

Опасността е свързана с две неизвестности:

– неизвестност, която се съдържа в познатите условия на съществуване;

– неизвестност при реализирането на някакво опасно събитие (в реалния живот това може да бъде пожар, земетресение, война и др.).

Тъй като опасността е свързана с възможно бъдещо развитие на процесите и явленията, е необходимо, особено в сферата на националната сигурност, да се търси генезиса на нещата в цялост, а не като отделни компоненти. Факт е, че в основата на криминогенните фактори стоят икономически и социални предпоставки.

Разликата между опасност и заплаха е, че заплахата съществува сега, а опасността е свързана с възможно бъдещо развитие.

Заплахата е реален факт, проявено обстоятелство, докато опасността се крие в сферата на възможното. На заплахата трябва да се противодейства. Опасността трябва да се предвиди и да се направи необходимото, за да се

избегне. Заплахата в повечето случаи има ясно очертан израз и при далновидно наблюдаване на протичащите процеси могат да се планират мероприятия и изграждат модели за противодействие.

Опасността характеризира действия или бездействия, състояния и ситуации (включително недостиг на ресурси или неадекватно поведение) в страната или извън нея, които развивайки се или задълбочавайки се, могат да нанесат сериозни щети на националната сигурност. Опасностите се откриват по-трудно, те могат да бъдат регистрирани или идентифицирани, едва когато са настъпили вредни последици за държавата, обществото и отделния индивид. Опасност възниква тогава, когато заплахата и рискът преминат определена граница на интензивност.

Съществуващите днес определения дефинират **риска** като действие при неопределеност, вероятност от последици, опасно условие, вреда и загуба, полза и печалба, начин на поведение. Риск е възможен там, където може да се прояви повече от един резултат. Рискът се свързва с вероятността да възникнат нежелани или неблагоприятни промени, а също и с несигурност за конкретен бъдещ момент или период от време. Рискът е заплаха с неустановен срок – няма предварително определено време за настъпването му. Дори да бъде установен достатъчно рано, той си остава принципно невъзможен за неутрализиране.

Рискът може да възникне като вътрешен (национален) проблем, но предизвикан от външни фактори. Един етнически проблем, например, лесно може да бъде подбуден от външни фактори. България е в такава геополитическа зона, в която вътрешни процеси и проблеми могат лесно да се използват от външни враждебни фактори.

Рискът прилича на заплаха, но се отличава по това, че между заплахата и кризата няма друго състояние, докато между появата на риска и кризата, времето е неустановено.

Характерна особеност на риска в сферата на сигурността е фактът, че наличието на източник на заплаха само по себе си не означава наличие на риск. За да дефинира наличието на риск, за организацията е необходимо източникът на заплаха да може да въздейства (независимо дали целенасочено или неумишлено) върху съществуващи или потенциални уязвими места на системата за сигурност. Понятието риск се използва, за да се дефинира вероятността за целенасочено или инцидентно въздействие на определен източник на заплаха. Този източник трябва да притежава съответни способности, мотивация и насоченост на влияние. Той се забелязва при целенасочена активност спрямо реално съществуващи или потенциални слабости и недостатъци на системата за сигурност, правейки я уязвима на въздействие. Във връзка с това, заплахата може да се изрази в действия или предварителен замисъл на дадена

държава, група или отделни лица, насочени срещу елементи на националната сигурност и срещу отделни лица, които имат отношение към националната сигурност. Заплахата е конкретизиран риск с възможност или вероятност за реализация непосредствено или в обозрима перспектива.

Бихме могли да обобщим, че винаги има опасност, почти винаги риск, но не винаги заплаха.

Източникът на заплаха не представлява риск, ако не е уязвима системата, върху която се въздейства. Източник на заплаха са субекти, събития или явления, които притежават потенциал да предизвикат негативни последици при въздействие върху системата за национална сигурност, социалните организации или отделни личности. Източникът на заплаха възниква и се развива при определени условия и в резултат на конкретни причини. Той се характеризира със способности, намерения, мотивация, насоченост и се проявява в разнообразни форми, при използване на различни методи и способи. За да бъдат обективно идентифицирани заплахите, е необходимо да бъдат разгледани всички реални и потенциални източници на заплахи, които има вероятност да причинят вреди на системата за национална сигурност, а също така и причините, които биха мотивирали извършване на посегателство върху тази система и биха повлияли на нейното нормално функциониране. Чрез обективна картина на заплахата може детайлно да се определи нейният източник като структура, организация, причини и условия за възникване, елементи, класификации и други признаци. Това може да бъде основа за прилагане на активни стратегии за влияние и въздействие върху причините за възникване на заплахата и оттам изграждане на модел за управление на риска и процесите, свързани с атаката на източниците на заплаха към уязвимите места на системата за национална сигурност.

На базата на анализ и оценка на минали и настоящи прояви на източника (или източниците) на заплаха за системата за национална сигурност, може да се състави картина на мотивацията и методите на действие и да се изготви прогноза за евентуалната насока на проявление на заплахата. Изграждането на точна прогноза за бъдещите действия на източниците на заплаха може да стане чрез придобиване на информация за техни минали проявления и настоящи действия. Необходимо е да се направи задълбочен исторически преглед на поведението на източниците на заплаха (разкрити, предотвратени, неутрализирани действия на източника на заплаха) и на тази база да се изгради модел за противодействие. Дейността по прогнозирането на бъдещите действия на източниците на заплаха е една от най-важните. Тя може да даде отговор за бъдещото развитие и динамиката на процесите, мотивите, капацитета, методите на действие, очакваните признаци на проявление и характера на източника на заплаха.

Източникът на заплаха може да се оцени при отчитане на следните фактори:

– наличие на достоверна информация за насоченост на източника на заплаха към даден елемент от системата за сигурност;

– наличие на информация за подготовка на източника на заплаха да осъществи негативно въздействие върху системата за сигурност;

– наличие на информация за мотивация и намерение за реализация на заплахата;

– способност на източника на заплаха да осъществи негативно или конфликтно взаимодействие;

– съществуваща връзка между минала и настояща активност на източника на заплаха.

Ключов момент при осигуряване на правилното функциониране на националната система за защита на класифицирана информация е идентифицирането на нейните уязвими откъм заплахи места.

Основна предпоставка за успешното идентифициране на риска е познаването на същността на организацията, на нейните цели и задачи. Анализът започва с избор на обект. За неголеми организации може да се разглежда цялата информационна инфраструктура, но за големи организации това може да се окаже бавен и необосновано скъп процес. В тези случаи ще трябва да се анализират най-важните възли от информационната инфраструктура.

Дейността на организация, която работи с класифицирана информация, е изложена на много рискове. Анализът на тези рискове включва дейности по характеризиране на организацията, идентифициране на източниците на заплаха, определяне на уязвимите места с оглед подсигуряване на дейността на организацията.

Съвременната глобална среда за сигурност и новите технологични реалности изведоха на преден план нов тип заплахи, дефинирани като **асиметрични заплахи**. Асиметрична е заплаха, в която се съдържат нетрадиционни, непознати и неочаквани за противника тактики, действия или средства, срещу които противникът не може да противодейства успешно. При този вид заплахи липсва обща база за сравнение между противоборстващите страни по отношение на количеството и качеството на използваните способи, за да може да се постигне необходимото превъзходство. Чрез създаване на неочаквани, непредвидими заплахи, асиметрични по отношение на противника, се постигат набелязани цели, като страх, паника и пр. Успехът на по-слабия се състои в това да принуди по-силния да издигне на стратегическо равнище онова, което нормално не би трябвало да бъде там.

За понятието асиметрична заплаха има много определения. Едно от тях гласи, че асиметричната заплаха представлява мислене, организация и действие, различни от тези на противника, с цел да се увеличат съответните предимства, да се използват слабостите на противника, да се запази инициативата или да се спечели по-голяма свобода на действие. Асиметрията означава използване на различията с цел постигане на предимство над противника. Асиметрично състояние възниква тогава, когато някоя разлика в ценностите, силите, боеспособността, възможностите, обучението или организацията може да създаде условия, които да бъдат успешно използвани.

При състояние на симетрия между противоборстващи страни, те имат относително равностойни потенциали, като целта им е да успеят да получат превъзходство чрез тактически прийоми, за да наклонят везните на успеха на своя страна. Симетрията не винаги означава, че двете противопоставящи се страни действат с еднакви методи или средства. На атакуващата страна са необходими такива конвенционални или неконвенционални средства, които тя е натрупала и подготвила за постигане на преследваните цели и осигуряване на победа или превъзходство. Страната, която се защитава, трябва да разполага със средства за противодействие на противниковите атаки и печелене на определено предимство. При наличие на еквивалентност на потенциалите, изкуството във воденето на борбата между противопоставящите се страни се състои във въвеждането на тактическа асиметрия за обръщане на успеха на своя страна. При противопоставяне на противници, които разполагат с равностойни потенциали, нещата изглеждат сравнително прости: една от страните трябва да намери форма, чрез която да сломи волята на противника си и да постигне превъзходство. Изкуството в борбата се състои в използването и въвеждането на тактическа асиметрия. Това е условието за успех в борбата между равностойните противници.

По друг начин стоят нещата, когато противниците имат различен потенциал и по-слабият се опитва да използва методи, с които противникът в момента не разполага. Тогава в действие влиза така наречената **стратегическа асиметрия**. За да постигне крайния ефект на компенсация, по-слабият се опитва да използва изключителни методи, с каквито противникът му не разполага, като концентрира усилията си върху всякаква възможна тактическа материална и морална уязвимост на противника. Използват се изненадата, дързостта, моралът и се употребяват възможно най-екстремалните средства, за да се ударят слабите места на противника. Към инструментариума на асиметричните средства по-слабият прибягва, когато е доведен до тотална слабост и е изчерпал всички възможни средства за противодействие. Тогава се търси оправдание за предприемане на асиметрични действия, като се търсят

аргументи в историческите и националните корени на засегнатата страна.

Хибридни заплахи

През последните години все по-актуален и значим става въпросът за същността на хибридната заплаха, нейните принципи, пътища и средства за реализиране и концептуалната рамка.

Теорията за хибридната заплаха е разработена основно в САЩ и силно е повлияна от участието на страната в конфликтите в Ирак и Афганистан.

Хибридните заплахи включват киберзаплахи, сценарии на асиметрични конфликти с ниска интензивност, глобален тероризъм, пиратство, незаконна миграция (Европейска мигрантска криза),корупция, етнически и религиозни конфликти, демографски предизвикателства, транснационална организирана престъпност, проблеми на глобализацията и разпространение на оръжия за масово унищожаване

Хибридна война (на англ.: *hybrid warfare*) е термин, който се появява в края на 20 век в САЩ за означение на нестандартна военна стратегия, инкорпорираща в себе си бойни действия, диверсия и кибервойна. Традиционно хибридната война се свежда до информационна война, но не само.

Тази война не се обявява официално. Тя не се води (поне не се признава) от регламентирани играчи (държави); използва неконвенционални средства (инфилтрация на информационната среда на други държави, подклаждане на паника, финансиране на нарочно създадени политически субекти с цел промяна на външнополитическата линия на набелязаните противници и войната не се „печели“, поне не в официалния смисъл на думата.

Американското виждане определя хибридната заплаха като съчетания от действия на конвенционални въоръжени сили с нередовни сили, които едновременно ангажират и използват наличните им военни способности и средства, подкрепени от комбинация от модерни технологии, конвенционални оръжия, кибер атаки и информационни операции за постигане на взаимноизгодни политически цели.

Европейският съюз и НАТО използват понятието хибридна заплаха като обобщително за определяне на неясни открити и прикрити действия на определена държава, която използва всички инструменти на властта за постигане на специфични политически цели. В техните позиции съществуваща тенденция за разполагане на заплахата в пространството между законни и незаконни действия и методи, национални и международни правни норми, ред и безредие, информация и пропаганда, традиционни и нетрадиционни методи и средства.

На национално ниво различните публикации и автори по различен начин дефинират хибридната заплаха. За някои от тях хибридната заплаха удобно се заменя с понятието хибридна война, а за други хибридната война е продукт на хибридната заплаха. Все пак липсва доктринално формулирано и законно възприето определение на понятието хибридна заплаха, което възпрепятства изготвянето на национална, общо възприета стратегия за противодействие.

Видове заплахи

При класифицирането на заплахите, които застрашават националната сигурност, в т.ч. информационната сигурност, се разграничават две големи групи заплахи: **природни заплахи** и **заплахи в резултат на човешка дейност**. От своя страна породените от човешка дейност заплахи могат да се разделят на два подвида – заплахи, породени от умишлена човешка дейност и заплахи, породени от неумишлена (непредпазлива) човешка дейност.

Не бива да забравяме и вредните последици, породени от природни въздействия, които биха създали предпоставки за застрашаване на информационната сигурност на всяка организационна единица.

В зависимост от намесата или въздействието на човека върху природните явления бихме могли да отделим чисто природните въздействия от онези природни въздействия, които са резултат от човешка дейност.

Чисто природните въздействия са характерни с това, че човек не винаги може да предвиди и да предприеме превантивни, профилактични или други организационни мерки за тяхното предотвратяване. Тук можем да отнесем въздействията, които се получават в резултат на природни катаклизми без участието на човека. Те трудно се предсказват и човек е безсилен пред тях (такива са земетресенията, ураганите, изригването на вулкани). По отношение на природните бедствия, резултатът от настъпващите вредни последици може да се минимизира с предварително планирани и изпълнени мероприятия.

Природните въздействия, породени от дейността на хората, са резултат от умишлена или неумишлена (непредпазлива, неволна) човешка дейност. Разликата между двата вида въздействия не се долавя лесно. Има природни въздействия, които са резултат от комбинацията на умишлена и неумишлена човешка дейност. Поради тази причина този вид заплахи ще бъдат разглеждани общо.

На сегашния етап от развитие на човечеството се очертават някои много сериозни и важни природни катаклизми, които биха имали отрицателни последици върху живота на човечеството. Това са глобалното затопляне, парниковият ефект, изтъняването на озоновия слой, увеличаването на

въглеродния диоксид, екологичните кризи в отделни райони на света в резултат на изсичане и масово обезлесяване. Всички тези природни катаклизми са свързани помежду си и взаимно си влияят. Тези природни въздействия като последствие от човешката дейност, умишлена или непредпазлива, имат влияние върху редица фактори, свързани с човешкото оцеляване. Ще поставим акцент върху заплахите, които са резултат от умишлена човешка дейност. Това е категорията заплахи, която оказва решаващо влияние върху информационната сигурност.

Заплахите, породени от умишлена човешка дейност са преди всичко в резултат на преднамерена човешка дейност. Деструктивната дейност на човека е в състояние да нанесе вреди във всички области на обществото. Заплахите, породени от умишлена човешка дейност, можем да разделим на два подвида: **традиционни (общи) и специфични**.

Традиционните заплахи са постоянно действащи и играят значителна роля с влиянието си върху средата за сигурност в глобален, регионален, териториален и индивидуално-обектен мащаб. Според обхвата на действие традиционните заплахи могат да бъдат **глобални, регионални, вътрешно-държавни, както и срещу физически лица и материални обекти.** Традиционните заплахи бихме могли за разделим на още няколко подгрупи в зависимост от различни фактори:

– според източника на заплахата или в зависимост от посоката на въздействие;

– според насочеността;

– според проявеността;

– в зависимост от областта на въздействие;

– по времево действие;

– по характер.

Нека разгледаме всяка една от тези подгрупи традиционни заплахи.

Ползвайки направената по-горе класификация, ще се спрем на два вида заплахи за информационната сигурност **в зависимост от посоката на въздействие - външни и вътрешни**.

Външни заплахи за информационната сигурност са:

– враждебни действия на чуждестранни организации, групи от хора или отделни лица в световното информационно пространство, водещи до застрашаващи националната сигурност последствия;

– дейност на чуждестранни политически, икономически, военни и разузнавателни информационни структури, насочена срещу националната информационна сигурност;

– дейност на международни терористични организации в международното и националното информационно пространство;

– дейност на космически, въздушни, морски и наземни технически и разузнавателни средства на чужди държави, събиращи класифицирана информация;

– изостряне на международната конкуренция в областта на информационните технологии;

– опити за доминиране и ощетяване на интересите на България в световното информационно пространство, изтласкването й от външния и вътрешния информационен пазар на стоки и услуги;

– увеличаване на технологичното откъсване на България от водещите държави в света и намаляване на възможностите за създаване или усвояване в страната на конкурентноспособни информационни технологии.

Вътрешни заплахи за информационната сигурност са:

– враждебни действия в националното информационно пространство от страна на отделни лица, групи от хора и организации в страната, водещи до последици, които заплашват националната сигурност;

– неблагоприятна криминогенна обстановка, съпроводена от тенденции за сращване на държавни и криминални структури в информационното пространство, достъп на криминални структури до класифицирана информация, засилване на влиянието на организираната престъпност върху живота на обществото, снижаване на степента на защитеност на законните интереси на гражданите, обществото и държавата;

– недостатъчна (неразвита) законова и подзаконова нормативна база, регламентираща отношенията в националното информационно пространство, както и нейното неефективно прилагане;

– некоординираност в дейността на държавните органи по отношение на създаване и осъществяване на единна държавна информационна политика;

– изоставане на България от водещите страни в света по равнище на информатизация на органите на държавната власт и органите на местното самоуправление, на кредитно-финансовата сфера, на промишлеността, селското стопанство, в сферата на здравеопазването, услугите и т.н.;

– недостатъчно финансиране на мероприятията, гарантиращи информационната сигурност на страната;

– намаляване на ефективността на националната образователна система и появата на дефицит на квалифицирани кадри в областта на информационната сигурност;

– предизвикани от човешка дейност катастрофи и аварии, както и разрушаване на строителни конструкции, отказ на жизнено важни енергийни

системи или системи за контрол, автоматично регулиране и управление, радиоактивно и химическо замърсяване и пр.;

– природни бедствия и стихии, в това число внезапни силни въздушни течения, електрически токови удари от светкавици, наводнения и пр.

Вътрешни и външни заплахи за информационната сигурност на България могат да произтекат и от враждебни действия на противникова страна. Тези действия могат да бъдат настъпателни (активни) и отбранителни (пасивни).

Настъпателните действия, които носят външни или вътрешни заплахи за информационната сигурност, са преди всичко внезапни мащабни атаки в националното информационно пространство с цел разрушаване, унищожаване, манипулиране или нарушаване на структури и ресурси.

Отбранителните действия са поредица от превантивни или ответни мероприятия, провеждани с цел наблюдение, събиране и анализ на информация, контрол и защита на националните информационни структури и ресурси.

Всички враждебни действия в информационното пространство са вид информационен конфликт (информационна война) – нова, нетрадиционна форма на борба. Информационната война се води за постигане на определени политически или икономически цели.

Следващата подгрупа традиционни заплахи ги определя според тяхната насоченост. В зависимост от начина, по който са насочени към средата за сигурност, разграничаваме **преки и косвени** заплахи. Преките заплахи въздействат непосредствено върху системата за национална сигурност на държавата. Косвените заплахи оказват индиректно въздействие върху националната сигурност на държавата. Това са процеси и явления, които може да не се виждат реално, но с косвени индикатори нанасят вреди на сигурността.

Подгрупата **заплахи според проявеността им, се разделят на актуални и потенциални.** Заплахите с актуално проявление действат в момента върху системата за национална сигурност и могат да доведат до диспропорции в различни области от обществено-политическия живот на страната. Актуална заплаха за нашата страна може да се окаже непрекъснатото нарастване на цените на петрола и другите енергоносители, което води до повишаване на цените на хранителни стоки, услуги и др. Това от своя страна дестабилизира икономиката на държавата и води до пораждане на социални конфликти, които могат да прераснат в открити форми на граждански протести.

Въздействието на потенциалните заплахи ще се прояви на един по-късен етап. Например, отрицателните последици от радиационно замърсяване от наш или чуждестранен източник ще се почувстват след години с всички последици за хората и екологичната среда. В аспекта на съвременния глобализиращ се

свят, изоставането днес на България в научно-техническо и информационно отношение, утре може да ни постави в неравностойно положение, което ще рефлектира в бъдещото развитие на нацията. Същото се отнася и за икономическото изоставане спрямо страните от региона и света. Като потенциална заплаха с потенциално проявление за България може да се посочи ислямският фундаментализъм.

В зависимост от областта на въздействие заплахите биха могли да бъдат насочени към политическата, икономическата, социалната, демографската, екологичната, информационната и други видове сигурност.

Подгрупата заплахи по време се разделя на две категории - постоянни и временни. Постоянните заплахи могат да създават дисбаланс и трайно да засегнат системата за национална сигурност. Като пример за постоянни заплахи могат да се посочат тези, които са чисто природни или са предизвикани в резултат на човешка дейност. Временните заплахи действат само за определен период от време. В резултат на управленска или друга човешка дейност определени временни заплахи биха могли да се преодолеят и да отпаднат като такива. Временни заплахи може да се проявят, например, в резултат на възникване на енергийна криза, породена от дефицит на петрол, природен газ, въглища и други енергоносители. Друга временна заплаха в чисто икономически план се съдържа в периодичните рецесии, в които изпадат икономиките на развитите държави – това се отразява както на самите тях, така и на икономиките на малките и слаборазвитите държави.

Заплахите по характер могат да бъдат военни и невоенни. Военните заплахи се свързват преди всичко с военните конфликти. България към момента е извън сферата на тази категория заплахи. През последните години в международните отношения се утвърдиха някои положителни аспекти, като комплексен подход към сигурността и търсене на общи решения на проблемите в различните области. Това намали до известна степен вероятността от избухване на глобален или съпоставим по мащаб военен конфликт.

Най-общо, към заплахите от невоенен характер бихме могли да отнесем всички заплахи извън сферата на военните конфликти. По-конкретно, с невоенен характер са информационните заплахи, демографското състояние, социалното неравенство, екологичните и промишлените аварии, катастрофите и природните бедствия. Глобалните заплахи от невоенен характер са особено актуални в сферата на природните бедствия, които в последните години са доста често срещано явление.

Както отбелязахме, освен традиционни, заплахите, породени от умишлена човешка дейност биват и специфични. **Специфични заплахи** са тези, които се обуславят от конкретни фактори, оказващи влияние върху средата за сигурност

за даден регион, конкретна страна, отделен индивид. Специфичните заплахи са конкретни за различните райони и държави. Това, което ги определя като специфични, е тяхната повишена интензивност и превръщането им в най-сериозната заплаха за националната и международната сигурност.

Специфичните заплахи, също както и традиционните заплахи, можем да разделим според обхвата на действие на глобални, регионални, вътрешно-държавни.

В съвременната епоха на развиващи се информационни технологии е от изключително значение да се познават заплахите, опасностите и рисковете, които могат да се отразят върху сигурността на създаването, обработването, съхраняването и пренасянето на класифицираната информация. Това би помогнало да се предприемат организационни, управленчески и технически мерки за ограничаване и премахване на отрицателните последици от нерегламентиран достъп до класифицираната информация.

НАЦИОНАЛНА СИСТЕМА ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

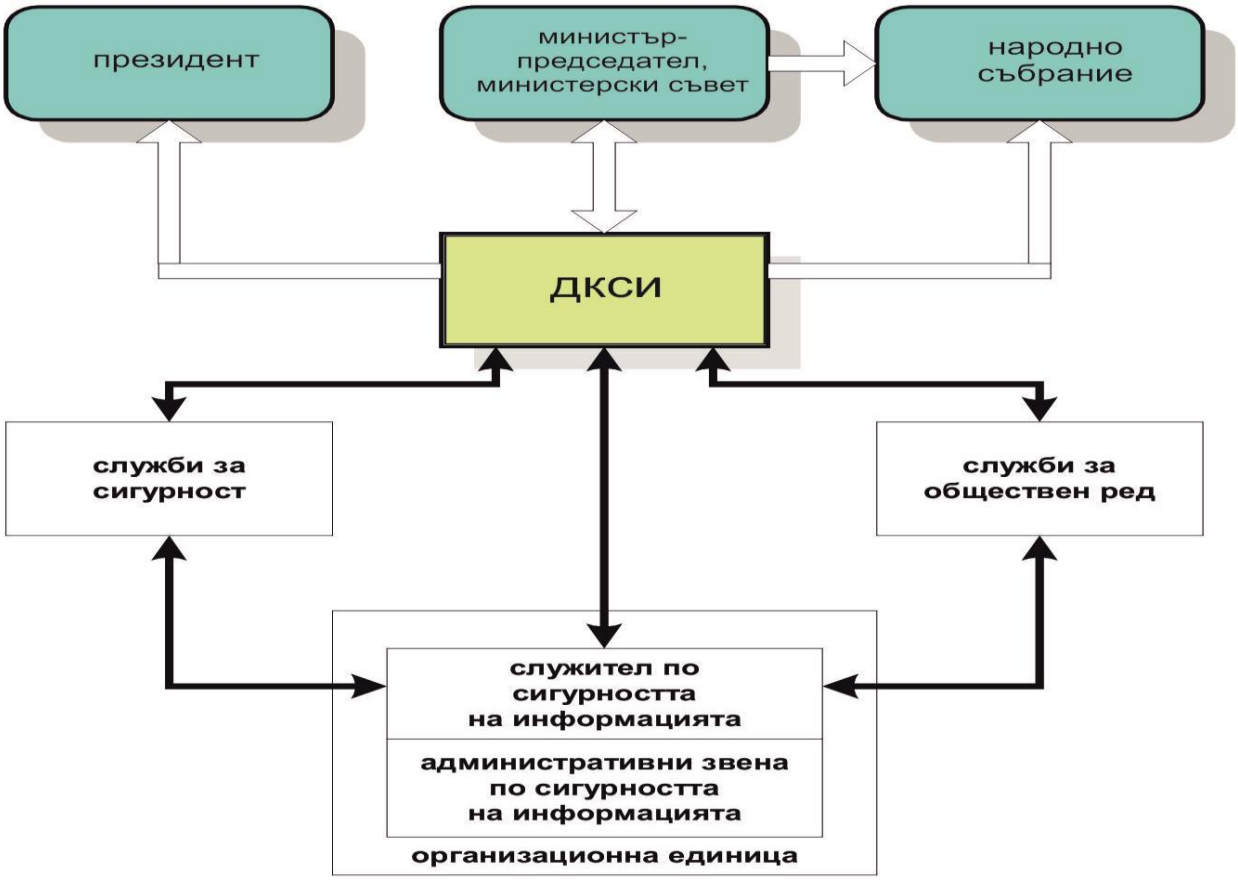
ОРГАНИ ЗА ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

1. Система от органи за защита на класифицираната информация

Системата за сигурност, в частност и системата за защита на класифицираната информация е комплекс от законови и подзаконови нормативни актове, административни, организационни, технически, оперативни и информационни процедури, механизми и действия, гарантиращи защитата на сигурността на дадена организация и създаващи условия за надеждно изпълнение на функциите й.

Изграждането на държавна система за защита на класифицираната информация, сертифицирането на нейните средства и формирането на ефективни механизми за защитата й са неотделима част от информационната сигурност на страната. Това е свързано с разработването на правила и политики за защита на класифицираната информация.

Системата за защита на класифицираната информация в Република България включва основните държавни институции, службите за сигурност, службите за обществен ред и организационните единици, показани на схемата по- долу.



- **Народното събрание (НС) –** България е парламентарна република и Народното събрание е институцията, която осъществява законодателната власт (чл.62, ал.1и чл.84, т.1 от Конституцията на РБ). Приема законите в областта на защитата на класифицираната информация, техните изменения и допълнения.

- **Президентът на Република България – има ограничени правомощия в законодателния процес; съгласно Конституцията на Република България президентът обнародва всички законодателни актове на Народното събрание (чл. 98, т.4).**

- **Министерският съвет (МС) –** определя насоките на националната политика за защита на класифицираната информация. Въз основа и в изпълнение на законите Министерският съвет приема постановления, разпореждания и решения. С постановления Министерският съвет приема и правилници и наредби (чл. 114 от Конституцията на РБ).

- **Държавната комисия по сигурността на информацията (ДКСИ),** която има водеща роля в системата за сигурност, тъй като дейността й допринася за гарантирането на националната сигурност на Република България в един от най-важните й аспекти – защитата на класифицираната информация.

Държавната комисия по сигурността на информацията, като отчита всички тези фактори, изпълнява своите функции в системата за защита на националната и чуждестранната класифицирана информация.

Тази система има следните основни задачи:

– да определя и оценява рисковете и заплахите за националната сигурност, в това число и информационната;

– да взема решения за пътищата и средствата за предотвратяването им;

– да поддържа постоянни материални и човешки ресурси за осигуряване на целостта на държавата, да разработва и провежда необходимите практически действия за защита на основните интереси на обществото чрез средства и способи, адекватни на вътрешната и международна обстановка.

- **Служби за сигурност (СС) и служби за обществен ред (СОР).**

- **Служителите по сигурността на информацията (ССИ).**

Системата от органи, ангажирани в противодействието на рисковете и заплахите за защита на класифицираната информация работят като изграждат общодържавен и специализиран механизъм.

Общодържавен механизъм за противодействие на рисковете и заплахите за класифицираната информация

Общодържавният механизъм за противодействие на рисковете и заплахите за класифицираната информация спада към категорията на превантивно профилактичните дейности, прилагани от държавата и държавните органи.

Тази подсистема за противодействие на рисковете и заплахите за компрометиране на класифицираната информация обхваща два механизма: **общодържавен механизъм за противодействие от дейности от организационно-управленски характер и дейности от нормативен характер**.

Общодържавен механизъм за противодействие на заплахите с дейности от организационно – управленски характер

Тази система от дейности има отношение към рисковете и заплахите за информационната сигурност в контекста на цялостния механизъм за противодействие на рисковете и заплахите за националната сигурност.

В рамките на този механизъм за противодействие можем да очертаем няколко аспекта:

- **Разработване на концепции и програми**, съдържащи задачи и постановки на държавните органи на различни нива за противодействие на опитите за нанасяне на вреди в информационното пространство. Органите на държавната администрация на областно и общинско ниво трябва да имат разработени механизми за действие и противодействие при всякакви случаи на усложнена обстановка – терористичен акт, природни бедствия, земетресения, наводнения и пр., които могат да предизвикат непоправими щети в информационните системи;
- **Координация и взаимодействие между държавните органи** и организации на различните нива на управление. Изисква се разработване на правила и варианти на действие при различни варианти на противоправна дейност, свързана с опити за нерегламентирано проникване и използване на класифицирана информация;

Обмен на информация между нисшите и висши държавни органи на управление за процесите и явления в областта на противодействие на всякакви опити за кибератаки. Наличието на точна и навременна информация към висшите държавни органи за управление дава възможност за адекватно реагиране на създадена кризисна или конфликтна ситуация.

Общодържавен механизъм за защита на класифицираната информация с дейности от нормативен характер

Приети са редица нормативни актове, които регламентират определени обществени отношения, дейности и правила, които имат за цел да осигурят защитата на класифицираната информация. Приети са Закон за защита на класифицираната информация, правилник за прилагането му. Разработени са наредбите по видовете сигурност на класифицираната информация – персонална, индустриална, физическа, документална, сигурност на комуникационните и информационните системи (КИС) и криптографска. Важен елемент от механизма за защита на класифицираната информация са задължителните указания на ДКСИ, които внасят конкретика и яснота в различните елементи на защитата на информацията.

За осигуряване на взаимната защита на класифицираната информация по инициатива на ДКСИ са подписани двустранни споразумения за обмен и защита на класифицирана информация.

Специализиран механизъм от дейности за противодействие на заплахите над високопоставените лица

Специализираният механизъм за защита на класифицираната информация включва комплекс от дейности на службите за сигурност и службите за обществен ред. В този механизъм от дейности за защита на класифицираната информация ще разгледаме **оперативни мерки на службите за сигурност и службите за обществен ред.**

- **Оперативен механизъм за защита на класифицираната информация**

Оперативните мерки за защита на класифицираната информация от страна на службите за сигурност и службите за обществен ред заемат важно място в рамките на общата система на националната сигурност. Оперативните мерки за защита на класифицираната информацията представляват всички онези действия в рамките на законово определените функции и задачи на службите за сигурност и службите за обществен ред, при които се прилагат специализирани способи. В оперативния механизъм за защита на класифицираната информация от страна на службите за сигурност и службите за обществен ред има няколко важни функции като:

– превантивна, изразяваща се в долавяне и разкриване на признаци за замисляне и подготовка на заплахи над системата за защита на

класифицираната информация и предприемане на мерки за предотвратяването им;

– **издирвателна**, състояща се в установяването на неизвестни автори извършители на заплахи над системата за защита на класифицираната информация;

– **профилактична**, имаща за цел да приложи мерки за отстраняване на причини или условия, благоприятстващи извършване на заплахи над системата за защита на класифицираната информация;

– **сигнална**, която се осъществява чрез информиране на съответните държавни органи за възникнали причини, които биха могли да доведат до извършване на заплахи над системата за защита на класифицираната информация;

– **методическа**, състояща се от оказване на помощ от страна на ДКСИ, службите за сигурност и службите за обществен ред към другите държавни органи за изработване и прилагане на мерки по противодействие на заплахите над системата за защита на класифицираната информация;

– **координираща**, предполагаща извършване на дейност, свързана със съгласуване на задачите и формите на участие на звената от държавния апарат, ангажирани в противодействие на заплахите над системата за защита на класифицираната информация;

– **контролна**, изразяваща се в реализиране на тематични или общи проверки за разкриване на нарушения в прилагането на законови и нормативни актове по отношение на административно-правния механизъм, третиращ борбата срещу престъпността, свързана с посегателства над системата за защита на класифицираната информация.

Специализираните способи за противодействие на заплахите над системата за защита на класифицираната информация могат да включат **подбор, изучаване и вербовка на сътруднически апарат и използването на специални разузнавателни средства** в установения от Закона за СРС ред. Към специализираните способи причисляваме и различни оперативни похвати, залегнали в правилниците и инструкциите на специализираните служби (**оперативно разкриване, оперативно предотвратяване, оперативна комбинация, оперативно проникване, подстава и пр**.). Оперативните мерки и способи никога не са самоцел. Те се основават на дълбок анализ на оперативната обстановка, прогнозиране на тенденциите за зараждащи се или протичащи заплахи към системата за защита на класифицираната информация.

Държавна комисия по сигурността на информацията

Като национален орган, който осъществява политиката на Република България за защита на класифицираната информация, се създава Държавната комисия по сигурността на информацията. Комисията е колегиален орган, състоящ се от петима членове, включително председател и заместник-председател. Съставът на ДКСИ се определя по предложение на министър-председателя с решение на Министерския съвет за срок от 5 години.

Създаването на този нов за българската институционална система административен орган е отражение на общата идея за необходимостта от граждански контрол върху определени сфери на дейност в областта на националната сигурност. Конкретното измерение на контрола се изразява в задължението на председателя на ДКСИ да представя пред Министерския съвет годишен доклад относно цялостната дейност по защитата на класифицираната информация, който Министерският съвет представя в Народното събрание за приемане с решение. Председателят на ДКСИ предоставя еднаква по обем и съдържание информация на председателя на Народното събрание, президента и министър-председателя на Република България.

Годишният доклад се подготвя в изпълнение на чл. 7, ал. 1 от ЗЗКИ и обхваща цялостната дейност на ДКСИ по защита на класифицираната информация. Основната цел на всеки доклад е анализът на извършената през предходната година дейност, представяне на актуалното състояние на системата за защита на класифицираната информация и очертаване на насоки за нейното развитие през следващата година. В него се разглежда дейността на ДКСИ като Национален орган по сигурността на информацията, на службите за сигурност и службите за обществен ред и на другите организационни единици по прилагане на ЗЗКИ, международното сътрудничество на Република България по защитата на класифицираната информация, основните аспекти по видовете защита на класифицираната информация.

Правомощия на ДКСИ

ДКСИ е държавен орган, осъществяващ политиката на Република България за защита на класифицираната информация (чл.4, ал.1 от ЗЗКИ). ДКСИ **организира, осъществява, координира и контролира дейността по защита на класифицираната информация** и осигурява еднаква защита на класифицираната информация.

ДКСИ извършва съвместно със службите за сигурност **проучвания за надеждност** на лицата, предложени за служители по сигурността на информацията и по тяхно предложение издава разрешения на тези лица. Извършва проучвания на български граждани, работещи в международни организации и структури на НАТО и ЕС.

Организира и осигурява функционирането на регистратурите в областта на международните отношения. ДКСИ е органът, който извършва проверките за изпълнението на изискванията за разкриване на регистратури за класифицирана информация на НАТО и на ЕС.

Уведомява незабавно министър-председателя, **в случай на нерегламентиран достъп** до класифицирана информация до най-високото ниво на достъп „Строго секретно".

Осъществява методическо ръководство спрямо служителите по сигурността на информацията.

Води регистри на издадените, отнетите или прекратени разрешения, удостоверения, сертификати, откази, което дава възможност за строга отчетност на тези документи и отразява актуалното състояние на системата в цялата страна.

Комисията води и регистър на материалите и документите, съдържащи класифицирана информация – държавна или служебна тайна. Това от своя страна позволява на ДКСИ да извършва непрекъснат анализ на обема и нивата на класифицирана информация в цялата страна, да отправя препоръки за преразглеждане с цел декласификация, унищожаване при наличие на съответните основания за това, да препоръчва реорганизация на мерките в случаи на нарастващ обем на класифицирана информация в конкретната организационна единица.

ДКСИ е органът, който съгласно ЗЗКИ дава **разрешения за унищожаване на оригинали на документи и материали**, съдържащи класифицирана информация на организационните единици и тези разрешения се отразяват в поддържаните от Комисията регистри.

Осъществява общ контрол по защитата на класифицираната информация, съхранявана, обработвана и предавана в комуникационните и информационните системи.

Осъществява общо ръководство на дейността по проучване на физически или юридически лица, кандидатстващи за сключването на договор или изпълняващи договор, свързан с достъп до класифицирана информация и утвърждава образец на удостоверение за сигурност. Практически това се реализира чрез извършване на проверки за оказване на методическа помощ, организиране на тематични семинари.

Важна част от контролната дейност на ДКСИ в областта на персоналната и индустриалната сигурност е разглеждането на жалби срещу постановени откази или отнемания на издадени разрешения за достъп/удостоверения за сигурност. Жалбата се подава в писмена форма чрез органа, чийто акт се обжалва, пред ДКСИ и в двуседмичен срок ДКСИ излиза с решение (чл. 63 – 67

от ЗЗКИ). Органът, който е компетентен да се произнесе е ДКСИ. В процеса на разглеждане на всяка жалба, ДКСИ проверява всички факти и обстоятелства, послужили за постановяване на обжалвания акт, проверява цялото проучване за надеждност от гледна точка на законосъобразност при извършването му. Това от една страна осигурява на лицата възможност за право на защита, от друга позволява да се извърши контрол от страна на ДКСИ върху цялата процедура по проучване. Това има и своя превантивен ефект върху проучващите органи, който се изразява в значително подобряване на процедурата по проучване и окомплектоваността на делата. С цел осъществяване на общ контрол върху процедурата по проучване на лицата, ДКСИ провежда ежегодни проверки на делата по проучване за надеждност за установяване на тяхната пълна окомплектованост и законосъобразност.

Решението на ДКСИ, с промените в ЗЗКИ от 2016 г. може да се обжалва пред тричленен състав на Върховния административен съд (чл. 68 и 69 от ЗЗКИ).

Организира и координира обучението за работа с класифицирана информация. В цялостната система от мерки за защита на класифицираната информация, обучението заема ключово място. Провеждат се и периодични семинари със служителите на ДКСИ, служителите по сигурността на информацията, завеждащите регистратури и други служители с разрешения за достъп до класифицирана информация на министерства, други държавни органи, областни администрации, общини и фирми. Обученията са първоначални, текущи, общи, тематични, специфични за конкретната длъжност. Целта на целия обучителен процес е лицата, които имат достъп до класифицирана информация да познават нормативните правила за нейната защита, рисковете и заплахите, да придобият практически умения за работа.

Извършва анализ и оценка и дава указания за готовността по защита на класифицираната информация срещу случаи на нерегламентиран достъп.

Превантивната дейност на ДКСИ е свързана с недопускане на нерегламентиран достъп.

Разработва и внася за приемане от Министерския съвет **проекти на нормативни актове** в областта на защитата на класифицираната информация.

Приоритетно място в дейността на ДКСИ заема осъществяването на тясно взаимодействие с органите, които имат компетенции в областта на защитата на класифицираната информация. Сътрудничеството със службите за сигурност и службите за обществен ред спомага до голяма степен за решаването на редица ключови въпроси, свързани с изпълнението на изискванията на Закона за защита на класифицираната информация (ЗЗКИ) и Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ).

При изпълнение на своите задачи и дейности ДКСИ може **да изисква информация** от информационните масиви на службите за сигурност и службите за обществен ред, от държавните органи и органите на местното самоуправление и необходимата информация от физическите и юридическите лица.

От особена важност е правомощието на ДКСИ да издава задължителни указания до задължените по закона субекти. Чрез тях се унифицира практиката по прилагане на законовата база в областта на защитата на класифицираната информация. Те се явяват изключително полезни за хората, които работят с класифицирана информация, тъй като дават отговор на конкретни хипотези в ежедневната работа и спомагат за еднаквото тълкуване и прилагане на законовите правила.

При осъществяването на своите правомощия ДКСИ се подпомага от обща и специализирана администрация, структурирана в дирекции.

Общата администрация на ДКСИ е организирана в дирекция „Финансово-стопански дейности и управление на собствеността“, дирекция „Човешки ресурси и учебно-методическа дейност“ и дирекция „Канцелария”.

Специализираната администрация подпомага ДКСИ при осъществяване на правомощията й по ЗЗКИ и се състои от пет дирекции: дирекция „Защита на класифицираната информация”, дирекция „Правна и международноправна дейност”, дирекция „Информационни фондове и системи”, дирекция „Сигурност” и дирекция „Специална куриерска служба“.

Международна дейност на ДКСИ

В международен аспект ДКСИ е Национален орган по сигурността (НОС) на Република България. Аналогични структури на ДКСИ съществуват във всички държави членки на НАТО и ЕС. В политиката за сигурност и директивите на НАТО се регламентира изрично съществуването на Национален орган по сигурността във всяка държава, чийто функции съответстват на правомощията на ДКСИ. Има различия в начина на формиране и в структурата на съответните органи, но правомощията им са аналогични. Общият принцип е, че Националният орган по сигурността представлява самостоятелна структура, подпомагана от администрация. Възможно е НОС да е обособен в рамките на Министерството на отбраната, Министерството на вътрешните работи или Министерството на външните работи, а така също и в рамките на разузнавателните/ контраразузнавателните служби.

ДКСИ полага усилия за изграждането на стабилна международноправна рамка в областта на защитата на класифицираната информация. В този смисъл

сключването на двустранни споразумения за взаимна защита и обмен на класифицирана информация представлява една от основните насоки в нейната дейност.

Когато Република България е страна по международни договори, ДКСИ организира, контролира и отговаря за изпълнението на задълженията за защита на класифицираната информация, съдържащи се в тези международни договори. ЗЗКИ въвежда като задължително условие за предоставянето и обмена на класифицирана информация с други държави и/или международни организации наличието на сключено и влязло в сила споразумение за взаимна защита и обмен на класифицирана информация. Тези споразумения създават правната възможност за предоставяне и обмен на национална класифицирана информация и регулират мерките за нейната защита.

ДКСИ инициира създаването на Междуведомствен координационен механизъм по водене на преговори и сключване на международни договори в областта на защитата на класифицираната информация, в който участват представители на ДКСИ и на заинтересованите ведомства. Неговата основна задача е да обсъжда проекти на международни договори и да изработва българската позиция при водене на преговори. Към септември 2020 г. са подписани и са влезли в сила общо 51 споразумения за взаимна защита и обмен на класифицирана информация.

ДКСИ установява тясно сътрудничество с националните органи по сигурността на други държави като домакин на множество срещи. Нейни представители участват в международни конференции и форуми по проблеми в различни области на сигурността на информацията. Предмет на срещите са представяне на националните практики по видовете защита на класифицираната информация, обмяната на опит и добри практики в тази област, споделянето на идеи за усъвършенстване на нормативната уредба и функционирането на системата за защита на класифицираната информация.

В рамките на двустранното сътрудничество, председателят на ДКСИ провежда работни срещи с ръководители на дипломатически представителства, акредитирани в Република България. Целта на тези срещи е представяне дейността на Комисията, активизиране на сътрудничеството и създаване на условия за установяване на преки контакти с органите с правомощия в областта на защитата на класифицирана информация и в сферата на сигурността на съответните държави.

Отчитайки политическите и икономическите приоритети на Република България, в контекста на членството й в НАТО и ЕС, освен сключването на двустранни споразумения със страните членки на НАТО и ЕС, ДКСИ активизира действията си по подготовка и сключване на двустранни

споразумения и с държави, с които Република България работи активно в различни области на икономическия и обществен живот. Особено внимание се обръща на контактите с държави, чиито физически и юридически лица развиват икономическа дейност на територията на страната ни или участват в управлението на търговски дружества, регистрирани по българското законодателство.

Чрез своята интензивна международна дейност, ДКСИ в продължение на повече от 18 години, спомага за утвърждаване на положителния външнополитически образ на Република България, като достоен член на европейското демократично семейство.

Служби за сигурност

Службите за сигурност и обществен ред са неразделна част от системата от органи за защита на класифицираната информация. Правомощията на службите за сигурност са посочени в чл. 11 – чл. 14 от ЗЗКИ, а правомощията на службите за обществен ред – в чл. 15 – чл. 16 от ЗЗКИ.

Службите за сигурност са :

- Държавна агенция „Национална сигурност“ (ДАНС);
- Държавна агенция „Разузнаване“ (ДАР);
- Национална служба за охрана (НСО);
- Служба „Военно разузнаване“ (СВР);
- Държавна агенция „Технически операции” (ДАТО);
- Главна дирекция „Борба с организираната престъпност“ (ГДБОП);
- Дирекция „Вътрешна сигурност“;
- Органите по чл. 16, ал. 2 от ЗПКОНПИ.

Правомощия на службите за сигурност

Проучвания по:

– персонална сигурност;

– индустриална сигурност.

Защита на сигурността на:

– КИС;

– криптираната комуникация (криптосигурност).

Превантивна и контролна дейност

Службите за сигурност извършват проучванията за надеждност единствено на своите служители, след което издават, отказват, прекратяват или

отнемат разрешения за достъп до класифицирана информация. Службите за сигурност извършват и проучванията на физически и юридически лица, които кандидатстват за сключване и изпълнение на договор, свързан с достъп до класифицирана информация (индустриална сигурност). Издават удостоверения за сигурност.

Съдейства за изпълнението на задачите на ДКСИ във връзка с чл. 9 от ЗЗКИ.

Службите за сигурност имат право :

- да прилагат разузнавателни способи и средства;
- да прилагат специални разузнавателни средства спрямо лица,

кандидатстващи за получаване на разрешение за достъп до класифицирана информация с ниво „Строго секретно";

- да използват данни от своите информационни масиви за физически и юридически лица, обекти на проучване;
- да съхраняват данните, получени в процеса на проучване;
- да съхраняват данни за случаите на нерегламентиран достъп;
- да получават необходимата информация от държавните и местните органи, от физическите и юридическите лица;
- да взаимодействат помежду си.

Правомощия на ДАНС

На национално равнище Държавна агенция „Национална сигурност" има по-широки правомощия по отношение на проучванията за надеждност по персонална сигурност и индустриална сигурност. Другите служби за сигурност и служби за обществен ред имат правомощия за своите служители, кандидати за работа, физически или юридически лица по договор със съответните служби.

Държавната агенция „Национална сигурност" е компетентният орган, извършващ проучвания за надеждност на българските граждани:

- военнослужещи и цивилни служители по трудови или служебни правоотношения;
- физически и юридически лица, на които е необходим достъп до класифицирана информация.

След приключване на процедурата по проучване ДАНС издава или отказва достъп. В правомощията на ДАНС е да отнеме вече действащо разрешение за достъп при нови негативни факти и обстоятелства за дадено лице и да прекрати действието на издадено разрешение.

Председателят на ДАНС определя служители за осъществяване на пряк контрол, които получават достъп до:

- помещенията в организационната единица – обект на контрол, включително за извършване на оглед; до документите, свързани с организацията по защита на класифицираната информация в организационната единица;
- комуникационните и информационните системи, където се създава, обработва или съхранява класифицирана информация.

Определените служители могат да дават препоръки, да изискват информация, да привличат експерти и да дават предписания във връзка със защитата на класифицираната информация. Редът за извършване на проверките по прекия контрол се определя с наредба, приета от МС. Събраната по време на проверките информация може да бъде използвана и предоставяна само за целите на защитата на класифицираната информация. Целта на проверките е отстраняването на всички рискове и заплахи за сигурността на информацията.

Видове проверки

Проверките в организационните единици обекти на контрол според обхвата са:

- **обща проверка** – за всички видове защита на класифицираната информация;
- **тематична проверка** – за отделни видове защита на класифицираната информация.
- Проверките в организационните единици обекти на контрол според планирането са:

– планови с предварително уведомяване на организационната единица;

– планови без предварително уведомяване на организационната единица;

– инцидентни (непланови) – при необходимост, по решение на контролиращите органи или при сигнал за опасност от възникване или за възникнал нерегламентиран достъп.

Като орган по прекия контрол, ДАНС прилага разпоредбите, касаещи прекия контрол, като планира и осъществява конкретни действия по разкриване, предотвратяване и пресичане на опитите за нерегламентиран достъп до класифицирана информация.

Сигурност на КИС и криптираната информация

Държавната комисия по сигурността на информацията осъществява общо ръководство и контрол на дейностите по криптографска сигурност на класифицираната информация.

Държавна агенция „Национална сигурност” е орган по криптографска сигурност (ОКС) на Република България, който:

- осъществява дейностите по криптографската защита на класифицираната информация;
- издава сертификат за сигурност на комуникационните и информационните системи;
- координира и контролира дейността по защита от паразитни електромагнитни излъчвания на техническите средства;
- осъществява и контролира обучението за работа с криптографски методи и средства.

Служби за обществен ред

Службите за обществен ред са:

- Главна дирекция „Национална полиция" – МВР;
- Главна дирекция „Жандармерия, специални операции и борба с тероризма" – МВР;
- Главна дирекция „Гранична полиция" – МВР;
- Главна дирекция „Пожарна безопасност и защита на населението" – МВР;
- Областните дирекции на МВР;
- Служба „Военна полиция" – МО.

Правомощия на службите за обществен ред

Извършват проучвания по персонална сигурност на своите служители и на кандидатите за работа, като издават, прекратяват, отказват и отнемат разрешенията на тези лица.

Службите за обществен ред оказват съдействие на службите за сигурност.

Службите за обществен ред имат право :

- да прилагат оперативно-издирвателни способи и средства;
- да използват данни от своите информационни масиви за физически и юридически лица;
- да съхраняват данните, получени в процеса на проучване на своите служители;
- да съхраняват данни за случаи на нерегламентиран достъп;
- да получават всякаква необходима информация от други организационни единици във връзка с проучваните лица.

2. Служител по сигурността на информацията

Служителят по сигурността на информацията заема важно място в системата за сигурност и защита на класифицираната информация в организационната единица.

Със Закона за защита на класифицираната информация за пръв път в Република България се създава тази длъжност – служител по сигурността на информацията. Всяко ведомство, създаващо, обработващо и съхраняващо класифицирана информация има задължението да определи лице, изпълняващо такива функции. Законът изчерпателно урежда изискванията (да има българско гражданство, да има разрешение за достъп до класифицирана информация до съответното ниво, което му е необходимо и задължително да е преминал обучение в областта на защитата на класифицираната информация), на които следва това лице да отговаря и конкретните му задължения.

Законът урежда и отделни организационни звена за съхранение и обработка на класифицирана информация – регистратури за класифицирана информация. Служителят по сигурността на информацията е лицето, което отговаря за спазването и прилагането на всички мерки за защита на класифицираната информация в организационната единица и в регистратурата за класифицирана информация. Всички служители в регистратурата са на пряко подчинение на служителя по сигурността на информацията.

Служителят по сигурността на информацията се явява и проучващ орган, тъй като извършва проучването на лицата в организационната единица, на които е необходим достъп до класифицирана информация до ниво „Поверително” (извършва обикновено проучване съгласно чл. 47, ал. 1 от ЗЗКИ).

ПОНЯТИЕ ЗА ОРГАНИЗАЦИОННА ЕДИНИЦА. ЗАДЪЛЖЕНИЯ НА РЪКОВОДИТЕЛЯ НА ОРГАНИЗАЦИОННАТА ЕДИНИЦА И СЛУЖИТЕЛИТЕ В ОРГАНИЗАЦИОННАТА ЕДИНИЦА

1. Организационна единица

Легалната дефиниция на понятието „Организационна единица” е дадена в §1, т. 3 от Допълнителните разпоредби на Закона за защита на класифицираната информация (ЗЗКИ). Съгласно нея „Организационна единица” са: органите на държавната власт и техните администрации; Министерството на отбраната и определени от министъра на отбраната структури на пряко подчинение на министъра на отбраната и формирования на Българската армия; органите на местното самоуправление и местната администрация; публичноправни субекти, създадени със закон или акт на орган на изпълнителната власт; физическите и юридическите лица, в които се създава, обработва, съхранява или предоставя класифицирана информация.

Органът, пред който се обявява организационната единица е Държавната комисия по сигурност на информацията (ДКСИ). Задължението за определяне като организационна единица пред ДКСИ произтича от закона и изпълнението му способства за идентифицирането на задължените по закона субекти. Неизпълнението на това задължение не освобождава съответните субекти, които създават, съхраняват, обработват или предоставят класифицирана информация от прилагане на законоустановените мерки.

Изпраща се официално писмо до ДКСИ, което съдържа следната информация:

– пълно наименование на организационната единица, седалище и адрес, телефони, факс, e-mail;

– предмет на дейност или задачите, които налагат създаване, обработване, съхраняване или предоставяне на класифицирана информация;

– данни за ръководителя на организационната единица – име, телефон, (ако има валидно разрешение за достъп до класифицирана информация се посочва неговият номер, дата на издаване, ниво на достъп, орган издал документа);

– данни за лицето, предложено от ръководителя на организационната единица за служител по сигурността на информацията (ССИ) – име, телефон;

– данни за завеждащ регистратура – име, телефон, (ако има издадено разрешение за достъп до класифицирана информация се посочва неговият номер, дата на издаване, ниво на достъп, орган, издал документа);

– данни за заместник-завеждащ регистратура – име, (ако има издадено разрешение за достъп до класифицирана информация се посочва неговият номер, дата на издаване, ниво на достъп, орган, издал документа);

– данни за регистратурата:

- при съществуваща регистратура се посочва адресът и местонахождението на помещението, в което е изградена регистратурата, както и нивото на класификация;
- при предстоящо разкриване на регистратура се посочва адресът и предвиденото местонахождение на помещението, в което ще се изгради регистратурата с ниво, съответстващо на най-високото ниво на класификация на документите, с което ще се работи в нея.

Нивото на регистратурата впоследствие може да бъде променено, т.е. да се повиши или понижи.

При необходимост в една организационна единица могат да бъдат разкрити повече от една регистратури, към тях могат да се разкрият контролни пунктове и специализирани звена. Регистратурите могат да бъдат както за национална, така и за чуждестранна класифицирана информация на НАТО и на Европейския съюз (ЕС).

Регистратурите се откриват след проверка за изпълнение на изискванията за защита на класифицираната информация и получаване на уникален идентификационен номер (УИН) от ДКСИ.

За да се разкрие една регистратура се извършва проверка от назначена от РОЕ комисия, в която вземат участие – ССИ, служител на ОЕ и представител на съответната служба за сигурност. Комисията изготвя протокол в три екземпляра – по един за ДКСИ, за съответната служба за сигурност и за регистратурата на организационната единица. След получаване на протокола ДКСИ изпраща на ОЕ уникален идентификационен номер на регистратурата.

При наличие на промени в обстоятелствата, послужили за издаване на УИН, както и при необходимост от повишаване на нивото на класификация на информацията, обработвана в регистратурата, се извършва нова проверка. След получаване на протокола от проверката ДКСИ взема решение за потвърждаване на издадения УИН.

Регистратура се закрива, когато в нея не се създава, обработва, съхранява или предоставя класифицирана информация, поради връщане на информацията на организационните единици, от които е била получена, поради унищожаването ѝ или предаването ѝ в архив по правилата на глава пета, раздел IX от ППЗЗКИ или по други причини. В този случай до ДКСИ и до органа по прекия контрол се изпраща предложение за закриване на регистратурата, изготвено от ССИ. В предложението задължително се посочва броят на

съхраняваните в регистратурата документи и материали през времето на нейното функциониране и причината за закриването й.

Органът по прекия контрол задължително извършва проверка по правилата на Наредбата за реда за извършване на проверките за осъществяване на прекия контрол по защита на класифицираната информация. След приключване на проверката изпраща доклад до ДКСИ от нея.

Въз основа на данните от предложението за закриване и от доклада ДКСИ взема решение за анулиране на УИН.

2. Задължения на организационните единици (чл. 17 от ЗЗКИ)

Организационните единици трябва:

– да прилагат изискванията за защита на класифицираната информация и да контролират тяхното спазване;

– да отговарят за защитата на класифицираната информация;

– в случай на нерегламентиран достъп до класифицирана информация да уведомяват незабавно ДКСИ и да предприемат мерки за ограничаване на неблагоприятните последици;

– да предоставят информация по искане на ДКСИ, службите за сигурност и службите за обществен ред.

3. Задължения на ръководителя на организационната единица (чл. 20, чл. 26 и чл. 37 от ЗЗКИ, чл. 23, чл. 49 и чл. 50 от ППЗЗКИ)

Ръководителят на организационната единица (РОЕ) се задължава: да ръководи, организира и контролира дейността по защита на класифицираната информация. Той назначава служител по сигурността на информацията след получаване на разрешение за достъп до класифицирана информация, издадено от ДКСИ. По изключение, в зависимост от обема на класифицираната информация ръководителят на ОЕ може да изпълнява и функциите на служител по сигурността на информацията. Трябва да притежава разрешение за достъп до най-високото ниво, с което се работи в ОЕ.

Ръководителят на ОЕ обявява списъците и вътрешните правила във връзка с класифицирането на информацията, както следва:

– Определя списък на длъжностите или задачите, за които се изисква достъп до съответното ниво на класифицирана информация, представляваща държавна тайна. (чл. 37 от ЗЗКИ). Настъпили структурни промени в организационната единица (например нов устройствен правилник) налагат актуализация на списъка.

– Определя със заповед списък на категориите информация, подлежащи на класификация като служебна тайна (чл. 21 от ППЗЗКИ).

– Обявява списък на категориите информация за сферата на дейност на конкретната организационна единица (списъкът е публичен – чл.26 от ЗЗКИ).

– Определя със заповед списък на длъжностите или задачите, за които се изисква достъп до класифицирана информация, представляваща служебна тайна (чл. 23 от ППЗЗКИ).

– Определя вътрешни правила при спазване на законовите изисквания за правилно определяне на нивото на класификация, както и за неговата промяна или премахване. С оглед предотвратяване настъпването на вреди по смисъла на §1, т. 15 от Допълнителните разпоредби на ЗЗКИ в тези правила за сферата на дейност на конкретната организационна единица се степенуват възможните вреди, които могат да настъпят в резултат на нерегламентиран достъп до класифицирана информация, създавана или съхранявана в организационната единица (чл. 49 от ППЗЗКИ).

– Създава организация и определя ред за периодично преразглеждане на създадената в организационната единица класифицирана информация с цел промяна или премахване на нивата на класификация (чл. 50 от ППЗЗКИ).

Служителят по сигурността на информацията е пряко подчинен на ръководителя на организационната единица.

4. Задължения на служителите в организационните единици, които имат достъп до класифицирана информация (чл. 18 от ЗЗКИ)

Служителите в организационните единици с достъп до класифицирана информация са задължени да спазват принципа “необходимост да се знае”, залегнал още в чл. 3 от ЗЗКИ.

Съгласно чл. 18 от ЗЗКИ при работа с класифицирани документи и материали те трябва да спазват изискванията на всички видове сигурност и да защитават класифицираната информация от нерегламентиран достъп. Уведомяват незабавно служителя по сигурността на информацията за случаи на нерегламентиран достъп, както и при всички промени на класифицираните материали и документи, при които не е налице такъв.

Лицата, получили разрешение за достъп до класифицирана информация, с ниво на класификация “Строго секретно”, са длъжни да информират писмено служителя по сигурността на информацията за всяко частно задгранично пътуване преди датата на заминаването, освен ако пътуването е в държави, с които Република България има сключени споразумения за взаимна защита на класифицираната информация.

5. Предоставяна информация на ДКСИ от организационната единица

В изпълнение на разпоредбите на чл. 9, т. 12 от ЗЗКИ и чл. 28 от Устройствения правилник на ДКСИ и нейната администрация в Комисията са създадени и се водят съответните регистри:

– Регистър на организационните единици, в който се съдържа информация за наименованието и адреса на организационната единица, ръководителя на организационната единица, служителя по сигурността на информацията, списъка по чл. 37 от ЗЗКИ, списъка по чл. 23 от ППЗЗКИ, броя на регистратурите, адрес на регистратурите, данни за лицата, завеждащи регистратурите;

– Единните регистри на издадените, отнетите или прекратените разрешения, удостоверения, сертификати и потвърждения на отказите за издаването или за прекратяването им;

– Регистър на документите и материалите, съдържащи класифицирана информация (държавна или служебна тайна), съгласно чл. 35 от ЗЗКИ. В базата данни се съдържа информация за създадени в организационната единица класифицирани документи и материали, за промяна или премахване на нивото на класификация, за направените предложения за унищожаване, както и за физическото унищожаване.

Организационните единици своевременно трябва да предоставят информация на ДКСИ за поддържане и актуализиране на регистрите.

6. Форма и начин на предоставяне на информацията

В ППЗЗКИ са определени образци за формата и съдържанието на някои от основните документи, които организационните единици изготвят и предоставят на ДКСИ.

Разрешенията, отнеманията, прекратяванията и отказите за достъп до класифицирана информация, издавани от ССИ след обикновено проучване, трябва да се изготвят съгласно Приложения № 10,11, 12 и 13 към чл. 145, ал. 2 от ППЗЗКИ.

Информацията за поддържане на Регистър на документите и материалите, съдържащи класифицирана информация (държавна или служебна тайна), се предоставя от ОЕ в таблична форма.

ДКСИ е изготвила образци за информацията по чл. 35, чл. 50, ал. 5, чл. 120 от ППЗЗКИ. Таблиците могат да се изготвят в програмите EXCEL или WORD.

СЛУЖИТЕЛ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

1. Понятие за служител по сигурността на информацията

По смисъла на Закона за защита на класифицираната информация (ЗЗКИ) служител по сигурността на информацията (ССИ) е физическо лице, назначено от ръководителя на организационната единица за осъществяване на дейността по защита на класифицираната информация в организационната единица (§1, т.4 от Допълнителните разпоредби на ЗЗКИ).

Изисквания за назначаване на длъжността служител по сигурността на информацията:

- лицето да притежава само българско гражданство;
- да е получило издадено от ДКСИ при условията и по реда на ЗЗКИ

разрешение за достъп до най-високото ниво на класифицирана информация, с което се работи в организационната единица.

След назначаването му **ССИ задължително преминава обучение в областта на защитата на класифицираната информация** (ЗКИ) в курс за задължително първоначално обучение, организиран и проведен от Държавната комисия по сигурността на информацията (ДКСИ) в нейния Учебен център в град Банкя. При проверките по прекия контрол контролиращите органи изискват удостоверение за преминат такъв курс.

2. Статут на служителя по сигурността на информацията

Законът за защита на класифицираната информация (ЗЗКИ) определя мястото и ролята на служителя по сигурността на информацията в организационната единица (ОЕ). Назначаването на ССИ в организационната единица е задължително. Той се назначава със заповед на ръководителя на организационната единица (РОЕ), след като е получил издадено от ДКСИ разрешение за достъп до класифицирана информация. Подчинен е пряко на ръководителя на организационната единица (чл. 20, ал. 2 и ал. 4 от ЗЗКИ).

Законът за защита на класифицираната информация и подзаконовите актове по неговото прилагане не предвиждат възможност служителят по сигурността на информацията да изпълнява и функциите на завеждащ регистратурата (ЗР) за класифицирана информация в организационната единица. Поради различните по обем и характер функции, които изпълняват ССИ и ЗР, както и прякото йерархично подчинение на ЗР на ССИ в системата за защита на класифицираната информация в организационната единица, съвместяването на двете длъжности е недопустимо. Като се вземе предвид и липсата на изрична разпоредба на ЗЗКИ или на Правилника за прилагане на ЗЗКИ (ППЗЗКИ), която да допуска съвместяването на функциите, **длъжностите ССИ и ЗР трябва да се заемат от различни лица.**

Законът допуска по изключение (в зависимост от нивото и обема на класифицираната информация) **функциите на служител по сигурността на информацията да се изпълняват от ръководителя на организационната единица,** ако отговаря на изискванията по чл. 21 от ЗЗКИ. Тази практика се

среща по-често в организационни единици, които имат недостатъчен брой лица с разрешения за достъп до класифицирана информация или работят с ограничен обем документи и материали, носители на класифицирана информация.

Служителят по сигурността на информацията трябва да бъде **щатен служител в организационната единица** по служебно или трудово правоотношение. Длъжността може да бъде основна за лицето или да се заема по съвместителство, което не се отразява на статута и функциите, възложени на ССИ от закона.

Изпълнението на функции на служител по сигурността на информацията по т. нар. граждански договор е несъвместимо с разпоредбите на ЗЗКИ. Както вече беше посочено, ССИ е пряко подчинен на ръководителя на организационната единица. В рамките на посочените две правоотношения служителят или работникът е подчинен на органа по назначаване или работодателя и дължи спазване на определеното работно място, работно време и трудова дисциплина, докато изпълнителят по „граждански договор“ може самостоятелно да определя мястото си на работа и времето, през което ще я извършва. В този смисъл той не е подчинен на РОЕ като възложител по договора, а дължи само определения в договора резултат.

В рамките на **една организационна единица може да има един служител по сигурността на информацията.** Назначаването му има за цел осъществяване на дейността по защита на класифицираната информация в организационната единица. Не се допуска възможността той да делегира на други лица своите задължения, установени от ЗЗКИ и актовете по неговото прилагане.

В случаите на отсъствие **служителят по сигурността на информацията може да бъде заместван при определени условия.** Със заповед ръководителят на организационната единица определя лице, което да го замества за времето на отсъствие. То трябва да отговаря на следните изисквания:

- да е служител в организационната единица;
- да не е ССИ в друга организационна единица;
- да отговаря на изискванията на закона за заемане на длъжността ССИ

В случаите на заместване не е необходимо заместващото лице да притежава издадено от ДКСИ разрешение за достъп до класифицирана информация. Достатъчно е разрешението за достъп до класифицирана информация на заместващото лице да е издадено от съответния компетентен проучващ орган. Ръководителят на организационната единица преценява дали да се възползва от възможността сам да замества отсъстващия ССИ или да определи за заместващ друго лице, отговарящо на посочените условия. Във всички случаи ръководителят на организационната единица трябва да уведоми ДКСИ за заместването.

При изпълнение на възложените му от закона задачи, **служителят по сигурността на информацията може да се подпомага от административни звена по сигурността** в зависимост от обема класифицирана информация или

при усложнена административна структура на организационната единица. При това следва да се спазва забраната за делегиране на правомощия от ССИ.

Законът за защита на класифицираната информация и подзаконовите актове по неговото прилагане не допускат едно лице да бъде ССИ в повече от една организационна единица.

3. Задължения на служителя по сигурността на информацията

Основното задължение на служителя по сигурността на информацията е да осъществява дейността по защита на класифицираната информация в организационната единица, като:

– прилага нормативните изисквания за защита на класифицираната информация и указанията на контролиращите органи;

– в рамките на своите функции контролира спазването в организационната единица на изискванията и указанията за защита на класифицираната информация.

В чл. 22, ал. 1 от ЗЗКИ са определени следните задължения:

- да следи за спазването на изискванията на ЗЗКИ и на международните договори във връзка със защитата на класифицираната информация;
- да прилага правилата относно видовете защита на класифицираната информация;
- да разработва план за охрана на организационната единица чрез физически и технически средства и следи за неговото изпълнение;
- да извършва периодични проверки на отчетността и движението на материалите и документите;
- след писмено разпореждане на ръководителя на организационната единица да извършва обикновено проучване в рамките на организационната единица, при условията и по реда на ЗЗКИ, като води регистър на проучените лица;
- да уведомява ДКСИ при изтичане на срока на разрешенията, при напускане или преназначаване на служителя, както и при необходимост от промяна на разрешението, свързано с достъп до определено ниво на класификация;
- незабавно писмено да информира както ДКСИ, така и компетентната служба за всяка промяна в обстоятелствата, свързани с издаваните разрешения, удостоверения, сертификати или потвърждения;
- да води на отчет случаите на нерегламентиран достъп до класифицирана информация и на взетите марки, като незабавно информира ДКСИ за това;
- да следи за правилното определяне на нивото на класификация на информацията при спазване на утвърдените от ръководителя на организационната единица вътрешни правила по чл. 49 от ППЗЗКИ;

- да разработва план за защита на класифицираната информация при положение на война, военно или друго извънредно положение**;**
- да организира и провежда обучението на служителите в организационната единица в областта на защитата на класифицираната информация.

В областта на документалната сигурност:

- съвместно с ръководителя на организационната единица да издава писмено разрешение за достъп до помещение на регистратурата на лица, извън лицата, осъществяващи пряк контрол;
- да разрешава работа с класифицирана информация извън работното време;
- да предлага поставянето на допълнителни ограничения върху материалите и документите;
- да извършва периодични проверки на отчетността и движението на материалите и документите с класифицирана информация;
- да осъществява контрол върху цялостната дейност и състоянието на регистратурата, включително да получава протоколите на извършваните от ЗР ежемесечни вътрешни проверки на регистратурата;
- да организира заедно с ръководителя на организационната единица текущ контрол на регистратурата (регистратурите, ако ОЕ има повече такива) чрез планови и извънпланови, годишни, частични и цялостни проверки;
- да получава протокола за резултатите от годишната проверка на регистратурата, извършена от назначена от ръководителя на организационната единица комисия, както и да следи за предоставянето на този протокол на Държавна агенция „Национална сигурност“ (ДАНС) и на ДКСИ.

В областта на персоналната сигурност:

- да изисква и да получава данни от службите за обществен ред и от компетентните държавни органи, а при необходимост – да иска съдействие от службите за сигурност с цел изясняване на обстоятелствата във връзка с попълването на въпросника при извършване на обикновено проучване;
- да издава или отказва разрешение за достъп до класифицирана информация – държавна тайна с ниво на класификация „Поверително“, като своевременно уведомява за това ДКСИ;
- да проверява факти, поставящи под съмнение лицата;
- да предлага прекратяване или отнемане на разрешението;
- да разрешава на лица от други организационни единици да се запознават с документи;

- да получава срещу разписка попълнения от кандидата въпросник – приложение № 2 към чл. 47 и 48 от ЗЗКИ и незабавно да завежда получения въпросник;
- да изпълнява и другите възложени му от ЗЗКИ и ППЗЗКИ функции при извършването на обикновено проучване.

В областта на физическата сигурност:

- да подпомага ръководителя на организационната единица при осъществяването на мерките за физическата сигурност в ОЕ;
- да разработва план за физическа сигурност;
- да определя зоните за сигурност и административните зони около тях, в които се извършва контрол на хора и моторни превозни средства;
- да въвежда контролиран режим за влизане, движение и излизане от зоните за сигурност;
- да подпомага ръководителя на организационната единица при осигуряването на съответен контрол над зоните за сигурност и административните зони чрез служители от звената за сигурност и охрана;
- да въвежда специален режим за съхранение на ключове от помещения, каси и други съоръжения;
- да изпълнява и другите възложени му от ЗЗКИ и актовете по неговото прилагане функции по отношение на физическата сигурност.

В областта на индустриалната сигурност:

- може да бъде определен от ръководителя на организационната единица – възложител да осъществява контрол по спазване на разпоредбите на закона и актовете по неговото прилагане и за консултиране на изпълнителя при изпълнението на договора (чл.105 от ЗЗКИ);
- може да бъде и лицето по чл.12 от Наредбата за общите изисквания за гарантиране на индустриалната сигурност, което отговаря за прилагането на мерките за ЗКИ при изпълнение на договора;
- да изготвя мотивирано писмено становище при възлагане на обществени поръчки, които имат за предмет държавна тайна.

4. Информация, която служителят по сигурността на информацията периодично предоставя на ДКСИ

Служителят по сигурността на информацията е длъжен периодично да предоставя на ДКСИ информация:

- по § 9 от Преходните и заключителните разпоредби на ЗЗКИ (относно изготвените до влизането в сила на закона материали и документи, обозначени

със степен на секретност);

- по чл. 37 от ЗЗКИ (относно определения от РОЕ списък на длъжностите или задачите, за които се изисква достъп до съответното ниво на класифицирана информация, представляваща държавна тайна);
- по чл. 23 от ППЗЗКИ (относно определения със заповед на РОЕ списък на длъжностите или задачите, за които се изисква достъп до класифицирана информация, представляваща служебна тайна).

Служителят по сигурността на информацията следва да подпомага ръководителя на организационната единица и в случаите, когато организационната единица е задължена да информира ДКСИ:

- по чл. 33 от ЗЗКИ (относно получаването на разрешение от ДКСИ за унищожаване на класифицираната информация в ОЕ);
- по чл. 35 от ЗЗКИ (за завеждане във водения от ДКСИ регистър на материалите и документите, съдържащи класифицирана информация, представляваща държавна или служебна тайна);
- по чл. 50 от ППЗЗКИ (относно създадената от РОЕ организация и определения от него ред за периодичното преразглеждане на създадената в ОЕ класифицирана информация с цел промяна или премахване на нивата на класификация).

Служителят по сигурността на информацията следва да извършва всекидневен контрол върху работата с класифицирана информация и нейната защита в организационната единица, като информира контролиращите органи (ДАНС) за всяка нередност.

ОРГАНИЗИРАНЕ И ПРОВЕЖДАНЕ НА ОБУЧЕНИЕ ПО ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ ОТ СЛУЖИТЕЛЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Значим елемент от цялостния процес за работа с класифицирана информация е обучението по защита на класифицираната информация. Чрез неговата превантивна роля за сигурността и защитата на информацията се решават множество фундаментални и практически въпроси, свързани с укрепването на националната система за защита на класифицираната информация.

1. Нормативна уредба

Принципната уредба на обучението е регламентирана в чл.22, ал.1, т.12 от **Закона за защита на класифицираната информация** (ЗЗКИ), чл.158 и чл.159 от **Правилника за прилагане на ЗЗКИ** (ППЗЗКИ) и **Задължителните указания на ДКСИ относно обучението на лицата в областта на защитата на класифицираната информация,** които доразвиват нормативната уредба в тази сфера.

2. Органи, отговорни за провеждането на обучението

Органите, на които законът възлага отговорности при провеждането на обучение по защита на класифицираната информация, са Държавната комисия по сигурността на информацията (ДКСИ) и служителите по сигурността на информацията в организационните единици.

Държавната комисия по сигурността на информацията организира, координира и провежда първоначалното и текущото обучение на лицата, определени за заемане на длъжността служител по сигурността на информацията и осъществява общото ръководство и контрола на цялостната дейност по обучение за работа с класифицирана информация.

Служителят по сигурността на информацията организира, координира и провежда обучението на служителите с достъп до класифицирана информация в организационната единица (чл. 22, ал.1, т.12 от ЗЗКИ). Той отговаря за провеждане на обучението на следните категории лица:

- ръководител на организационната единица;
- служителите в организационната единица с достъп до класифицирана информация;
- куриерите, които пренасят документи и/или материали, съдържащи класифицирана информация;
- служителите, на които е възложено изпълнението на други задачи или дейности, свързани с достъп до класифицирана информация.

Единствено ДКСИ провежда задължителното първоначално обучение на служителите по сигурността на информацията по чл. 21, ал. 2 от ЗЗКИ, за което издава валидно удостоверение.

3. Цели на обучението

Целта на обучението по защита на класифицираната информация е да се придобият знания, умения и опит за работа с класифицирана информация. В резултат на обучението лицата с достъп до класифицирана информация трябва:

- да познават ЗЗКИ и подзаконовите актове в областта на защитата на класифицираната информация;
- да придобият практически умения за прилагане на правилата относно видовете защита на класифицираната информация;
- да усвоят специфични професионални умения, необходими за изпълнение на функционалните задължения на съответната длъжност, респективно за изпълнение на съответна задача.

4. Видове обучения

В зависимост от целите на обучението по защита на класифицираната информация, то бива: първоначално, текущо, функционално и тематично обучение.

Първоначално обучение

Първоначалното обучение по защита на класифицираната информация има задължителен характер и се провежда на всички лица с оглед заемане на определена длъжност, или за изпълнение на конкретна задача, свързана с достъп до класифицирана информация. То обхваща общата задължителна подготовка и задължително функционално обучение.

Програмата за общата задължителна подготовка трябва да включва следните тематични области:

- Рискови фактори за интересите на Република България в областта на защитата на класифицираната информация.
- Национална система в областта на защитата на класифицираната информация – компетенции.
- Понятие за организационна единица – права и задължения на организационните единици и техните служители.
- Мерки за защита на класифицираната информация по видовете сигурност.
- Защита на класифицираната информация на Европейския съюз и класифицираната информация на НАТО (само за лицата, притежаващи съответните разрешения за достъп).

- Контрол върху дейността по защита на класифицираната информация.
- Предотвратяване на нерегламентиран достъп до класифицирана информация и на последиците от него.
- Административнонаказателна отговорност в областта на защитата на класифицираната информация.

Система за оценяване на първоначалното обучение

Всяко първоначално обучение по ЗКИ завършва с тест за оценка на знанията. При изготвянето на изпитния тест въпросите трябва да се формулират точно и ясно. Всеки въпрос следва да предполага структуриран отговор или да е с ограничена свобода на отговора. Възможно е включването на въпроси – уловки, но е недопустимо отговорите да са поставени в зависимост един от друг.

За успешно преминато обучение се счита това, при което обучаемият е отговорил вярно на не по-малко от 70% от въпросите в теста. Броят на въпросите в теста се определя от служителя по сигурността на информацията в организационната единица. Препоръчително е в теста да бъдат включени между 25 и 35 въпроса.

Удостоверяване на преминато първоначално обучение

Органът, провел първоначалното обучение по ЗКИ задължително издава Удостоверение за преминато първоначално обучение по образеца, установен в приложение № 19 към чл. 159, ал. 3 от ППЗЗКИ.

Оригиналът на удостоверението се съхранява от служителя (обучаемия), а копие може да се съхранява от служителя по сигурността на информацията. В случай, че служителят по сигурността на информацията съхранява оригинал на удостоверение за преминато обучение, при напускане на служителя следва да му го върне.

Всеки служител (обучаем) след преминато първоначално обучение по ЗКИ попълва декларация – приложение № 18 към чл. 159, ал. 3 от ППЗЗКИ, която се съхранява от служителя по сигурността на информацията.

Организиране на първоначално обучение по ЗКИ

При организиране на първоначално обучение по ЗКИ, служителят по сигурността на информацията следва да подготви: **програма** на обучението съобразена със задължителните тематични области, **списък** на служителите включени в обучението, **тест** за проверка на знанията, **заповед** на ръководителя за провеждане на обучението, **удостоверение** – приложение № 19 към чл. 159,

ал. 3 от ППЗЗКИ и **декларация** – приложение № 18 към чл. 159, ал. 3 от ППЗЗКИ.

Задължително функционално обучение

Задължителното функционално обучение е специфично за съответната длъжност или задача, за която се провежда. Насочено е към трайно усвояване на знания и умения за изпълнение на съответните функционални задължения или за изпълнение на конкретна задача. На функционално обучение по ЗКИ подлежат служителите по сигурността на информацията, завеждащите регистратури и други служители в регистратурите за класифицирана информация, куриерите, които пренасят документи и/или материали съдържащи класифицирана информация и други длъжностни лица със задължения по контрола на мерките за защита на класифицираната информация.

Тематичната насоченост на задължителното функционално обучение е обвързана с общите за всички обучаеми права и задължения и със специфичните изисквания за съответната длъжност или задача, за която се провежда. Това обучение може да се провежда в лекционна форма или чрез използване на някои от следните методи – решаване на практически задачи или казус, брейнсторминг, симулация и др.

За успешно преминато обучение се счита това, при което обучаемият е отговорил вярно на не по-малко от 70% от въпросите в теста. Броят на въпросите в теста се определят от служителя по сигурността на информацията в организационната единица. За преминато функционално обучение задължително се издава удостоверение.

Текущо обучение

Текущото обучение има за цел придобиването на допълнителни познания в областта на защитата на класифицираната информация чрез повишаване на квалификацията и опита на обучаемите лица.

Този вид обучение е надграждащо по отношение на първоначалното обучение. Конкретното съдържание, методите на провеждане, системата за оценяване и продължителността на текущото обучение се определят от служителя по сигурността на информацията.

Текущо обучение се провежда в следните случаи:

- при изменение или допълнение в нормативната уредба в областта на защитата на класифицираната информация;

- при констатиране на нарушения при работа с класифицирана информация;
- след указание или предписание от ДКСИ и/или от органа по прекия контрол;
- спрямо лица, чиито служебни задължения или задачи не са изисквали работа с класифицирана информация повече от една година.

След преминато текущо обучение, органът провел обучението издава Удостоверение за преминато текущо обучение.

Всеки служител (обучаем) след преминато текущо обучение по ЗКИ попълва декларация – приложение № 18 към чл. 159, ал. 3 от ППЗЗКИ, която се съхранява от служителя по сигурността на информацията.

Тематично обучение

Тематичното обучение обхваща теоретични и практически казуси по видовете защита на класифицираната информация.

Конкретното съдържание, методите на провеждане, системата за оценяване и продължителността на тематичното обучение се определят от служителя по сигурността на информацията.

5. Регистър на обученията

Служителят по сигурността на информацията съгласно чл. 159, ал. 6 от ППЗЗКИ води **Регистър на проведените обучения** (Приложение № 20 към чл. 159, ал. 6 от ППЗЗКИ).

Приложение № 18
към чл. 159, ал. 3 от ППЗЗКИ

ДЕКЛАРАЦИЯ

Подписаният..... декларирам, че съм преминал курс по първоначално/текущо обучение в областта на сигурността на класифицираната информация, познавам правилата за нейната защита и ще опазвам класифицираната информация до изтичането на сроковете за защитата й по чл. 34 от ЗЗКИ.

Дата:

Подпис: .....

Подпис: .....
(служител по сигурността на информацията)

Приложение № 19
към чл. 159, ал. 3 от ППЗЗКИ

УДОСТОВЕРЕНИЕ ЗА ЗАВЪРШЕНО ОБУЧЕНИЕ ПО ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

..... издава настоящото
(компетентен орган по сигурността)

на

.....,
(трите имена на лицето) ,

ЕГН..... в уверение на това, че е завършил(а) курс за обучение по защита на класифицираната информация. Същият(та) може да има достъп до ниво на класифицирана информация .....
(ниво на класификация)

Подпис: _____
Печат: (фамилия)

(дата на издаване)
(място на издаване)

Приложение № 20
към чл. 159, ал. 6 от ППЗЗКИ

РЕГИСТЪР

(електронен) за отчет на проведено обучение в областта на сигурността на лицата, допуснати за работа с класифицирана информация в (организационна единица/звено)

№	Име, презиме, фамилия, ЕГН	Длъжност, дирекция/ звено	Притежава ниво на разрешение	Вид на обучението	Дата на преминато обучение	Подпис на лицето
1	2	3	4	6	7	8
1.	Иван Иванов Иванов 7708089999	гл. експерт в дирекция „Сигурност”	„поверително”	първоначално	22.08.2020 г.	
2.	Петър Петров Петров 8808088888	мл. експерт в дирекция ЗКИ	„секретно”	текущо	15.12.2020 г.	

УСЛОВИЯ И РЕД ЗА ПОЛУЧАВАНЕ НА ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Сигурността на класифицираната информация е комплекс от всички нормативно установени принципи, способи и мерки, гарантиращи, че класифицираната информация няма да бъде обект на нерегламентиран достъп. Следователно защитата на класифицираната информация е система, която следва да бъде изградена и поддържана в състояние, при което са неутрализирани или поне сведени до минимум възможните заплахи.

Спектърът от възможните заплахи за сигурността на класифицираната информация е изключително широк, поради което нейната защита трябва да бъде организирана системно и последователно. Върху тази основа се установяват правилата на Закона за защита на класифицираната информация (ЗЗКИ) и подзаконовите актове по неговото прилагане, които предвиждат система от органи, ангажирани със защитата на класифицираната информация и изграждането на система от мерки, необходими за постигането на тази защита.

По своята същност проучването за **надеждност има за цел** да се прецени предварително дали на едно лице може да му бъде предоставен достъп до класифицирана информация. С предварителната проверка на надеждността на лицето по критериите, установени в закона, се счита, че се неутрализира, респективно ограничава в допустими граници рискът за сигурността на информацията, чиято заплаха произтича от самото лице.

1. Правна рамка

Редът и условията за достъп до класифицирана информация се уреждат със ЗЗКИ, ППЗЗКИ, Наредбата за реда за извършване на проверките за осъществяване на пряк контрол по защита на класифицираната информация.

Със **Закона за защита на класифицираната информация и правилника за прилагането му** в областта на персоналната сигурност се регламентира предоставянето на достъп до класифицирана информация, процедурата по проучване за надеждност на лицата, прекратяването й, воденето на делата по проучванията и мерките за осигуряване персонална сигурност на класифицираната информация. Целта на закона е класифицираната информация да бъде защитена от нерегламентиран достъп.

2. Персонална сигурност – принципи и мерки

Персоналната сигурност представлява **система от принципи и мерки**, прилагани от компетентните органи спрямо лица **с цел гарантиране на тяхната надеждност** с оглед защитата на класифицираната информация.

Мерките за защита на класифицираната информация в областта на персоналната сигурност гарантират достъп до класифицирана информация само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „необходимост да се знае" и след извършено проучване за надеждност, в резултат на което на лицето е издадено разрешение за достъп до класифицирана информация до съответно ниво.

Принципът „**необходимост да се знае**" е сред основните положения, на които се изгражда цялостната защита на класифицираната информация. Означава ограничаване на достъпа само до определена класифицирана информация и само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

Принципът „необходимост да се знае" способства ограничаването на необоснованото разширяване на кръга от лица, които се запознават с конкретна класифицирана информация. Необоснованото разширяване на кръга от лица, имащи право на достъп до определена класифицирана информация е риск за сигурността ѝ.

Именно спазването на този принцип не позволява концентриране на информация в едно лице, а установява ограничения в обема на информацията, с която едно лице може да се запознава.

3. Процедура по проучване

Лица, получаващи достъп по право (чл. 39 от ЗЗКИ)

Чл. 39 от ЗЗКИ определя лицата, които получават достъп до класифицирана информация по силата на служебното си положение, а именно:

- председателя на Народното събрание;
- президента на Република България;
- министър-председателя;
- заместник-министър председателите и министрите;
- главния секретар на Министерския съвет;
- народните представители;
- съдиите от Конституционния съд, прокурорите, адвокатите и следователите;
- членовете на Висшия съдебен съвет, главния инспектор и инспекторите в Инспектората към Висшия съдебен съвет.

Председателят на Народното събрание, президентът на Република България и министър-председателят получават достъп до всички нива на класифицирана информация, считано от момента на встъпването им в длъжност, за срока на заемане на длъжността им. **Заместник-министър председателите, министрите и главният секретар на Министерския съвет** получават достъп до всички нива на класифицирана информация, считано от момента на встъпването им в длъжност, спазвайки принципа „необходимост да се знае" в кръга на тяхната компетентност. **За народните представители** – при взето по установения ред решение на парламентарна комисия или на Народното събрание или когато комисия или Народното събрание заседават в закрито заседание. **За съдиите, прокурорите, адвокатите и следователите** – само за конкретното дело. **За членовете на Висшия съдебен съвет –** при взето по установения ред решение на съответната колегия или пленума на Висшия съдебен съвет, когато колегията или пленума заседават в закрито заседание. **За главния инспектор и инспекторите в Инспектората към Висшия съдебен съвет** – при осъществяване на техните правомощия.

Изисквания за получаване на разрешение

Изискванията, на които трябва да отговаря лицето, кандидатстващо за достъп до национална класифицирана информация са:

- да притежава българско гражданство, с изключение на случаите по глава шеста, раздел VI;
- да е пълнолетно;
- да има завършено средно образование;
- да не е осъждано за умишлено престъпление от общ характер, независимо от реабилитацията;
- срещу лицето да няма образувано досъдебно или съдебно производство за умишлено престъпление от общ характер;
- да е надеждно от гледна точка на сигурността;
- да не страда от психически заболявания, удостоверено по съответния ред;
- да е определено като надеждно за опазване на тайна.

Н**адеждност на лицето от гледна точка на сигурността** означава, че лицето не е осъществявало дейност срещу интересите на Република България или срещу интереси, които Република България се е задължила да защитава по силата на международни договори. Също така лицето не трябва да има участие или съучастие в шпионска, терористична, саботажна или диверсионна дейност.

За проучваното лице трябва да се установи, че не е осъществявало друга дейност против националната сигурност, териториалната цялост или суверенитета на страната или целяща насилствена промяна на конституционно установения ред, както и дейност, насочена срещу обществения ред.

Надеждност на лицето от гледна точка на опазване на тайната е налице, когато в хода на проучването за надеждност се установи, че липсват данни относно укриване или даване на невярна информация от проучваното лице за целите на проучването. Няма факти и обстоятелства, които биха дали възможност за изнудване на проучваното лице, както и несъответствие между стандарта на живот на проучваното лице и неговите доходи. Установява се, че лицето не страда от психично заболяване или други нарушения на психичната дейност, които биха повлияли отрицателно върху способността му да работи с класифицирана информация и не е зависимо от алкохол и наркотични вещества.

Целта на процедурата по проучване е да се установи дали проучваното лице отговаря на гореизброените изисквания. Службите за сигурност в хода на проучването проверяват със свои способи и методи информацията, която е получена, в резултат на което издават или не издават разрешение за достъп до класифицирана информация.

За да стартира процедурата по проучване за надеждност трябва да има писмено съгласие на лицето, обект на проучването, което може да бъде оттеглено в хода на процедурата по проучване. Ако лицето оттегли своето писмено съгласие, процедурата се прекратява незабавно. Явните документите се връщат на лицето срещу писмена разписка, а въпросникът и всички документи и материали, събрани в процеса на проучване се унищожават съгласно ППЗЗКИ.

Лицето няма право да кандидатства за достъп до класифицирана информация за срок от една година.

Необходими документи

Необходими са следните документи, които лицето трябва да подготви, за да стартира процедурата по проучване:

- искане от ръководителя на организационната единица до компетентния проучващ орган за започване на процедура по проучване;
- молба от кандидата до ръководителя на организационната единица за заемане на длъжността или изпълнение на конкретно възложена задача, която съдържа писмено съгласие на лицето;
- копие на диплом за завършено образование;
- медицинско свидетелство за психично здраве;
- декларация по чл. 74, ал. 2, т. 1 от Данъчно-осигурителния

процесуален кодекс;

- съгласие във връзка с чл. 62, ал. 9 от Закона за кредитните институции;
- попълнен въпросник – приложение № 2 от ЗЗКИ.

В случай, че едно лице кандидатства за длъжността служител по сигурността на информацията, комплектът от документи се подава в **ДКСИ**. В искането изрично се посочва, че лицето ще изпълнява функциите на служител по сигурността на информацията. ДКСИ съвместно със службите за сигурност извършва проучването на служителите по сигурността на информацията и по тяхно предложение издава разрешение за достъп до класифицирана информация на тези лица.

Във всички останали случаи комплектът от документи се подава до Държавна агенция „Национална сигурност“ (**ДАНС**), която на национално равнище има по-широки компетенции в областта на персоналната сигурност.

Видове проучване и срокове

Проучванията биват три вида, в зависимост от нивото на достъп, за което лицето кандидатства.

Обикновено проучване – за ниво „Поверително”

Извършва се от служителя по сигурността на информацията (ССИ) след писмено разпореждане на ръководителя на организационната единица. Установява се дали лицето е български гражданин, дали срещу него има образувано досъдебно или съдебно производство, дали е надеждно от гледна точка на опазване на тайната и дали не страда от психични заболявания. Не се проверява надеждността от гледна точка на сигурността. Служителят по сигурността на информацията може да изисква информация от службите за обществен ред, а при необходимост и от службите за сигурност. Към комплекта от документи за извършване на проучването не се изисква Съгласие за проверка на авоарите в банките, във връзка с чл. 62, ал. 9 от Закона за кредитните институции.

Разширено проучване – за ниво „Секретно”

Освен горепосочените проверки се изискват справки и се извършва оперативно проучване на лицето, което включва проверки по местоживеене, по месторабота, проверяват се банковите сметки на проучваното лице и се извършват справки в данъчните регистри.

Специално проучване – за ниво „Строго секретно”

Освен горепосочените действия се провежда и интервю с проучваното лице, както и с тримата гаранти, посочени от него във въпросника.

При извършването на процедурата по проучване има определени срокове, в които тя трябва да приключи. Тези срокове са различни за съответното ниво на достъп. А именно:

- обикновено проучване – до 30 дни от получаването на писмено искане;
- разширено проучване – до 45 дни;
- специално проучване – до 60 дни.

Всеки един от тези срокове може да бъде удължен максимум с 20 дни. В 10-дневен срок от приключване на проучването за надеждност, Държавната комисия по сигурността на информацията, службите за сигурност или служителят по сигурността на информацията издават или отказват издаването на разрешение за достъп до класифицирана информация до съответното ниво.

Проучващи органи

Държавна комисия по сигурността на информацията

Проучва български граждани, които кандидатстват за заемане на длъжности или изпълнение на конкретно възложени задачи, налагащи работа с класифицирана информация на друга държава или международна организация, след постъпване на писмено искане от компетентния орган по сигурността на съответната държава или международна организация.

Съвместно със службите за сигурност ДКСИ извършва проучване и издава разрешение за служители по сигурността на информацията.

Държавна агенция „Национална сигурност”

Проучва всички цивилни и военни лица.

Други служби за сигурност и служби за обществен ред

Извършват проучване за своите служители.

Служител по сигурността на информацията

Извършва обикновено проучване на служителите в организационната единица.

Резултати от процедурата по проучване

Разрешение, отказ

Разрешението се издава на лица, които отговарят на изискванията на чл. 40. То е писмен документ, който се издава в 3 екземпляра, които се съхраняват в ДКСИ, проучващия орган и организационната единица. Сроковете, за които е валидно издаденото разрешение за достъп до национална класифицирана

информация съответстват на нивото на достъп:

- „Поверително” – пет години
- „Секретно” – четири години
- „Строго секретно” – три години

При необходимост от преиздаване на разрешението, когато срокът на валидност изтича, стартира процедура по повторно проучване, най-късно три месеца преди изтичането на валидността на разрешението.

Разрешението се издава персонално за лицето, което означава, че с издаденото разрешение може да се променя месторабoтата и при необходимост с него може да се премине от една организационна единица в друга.

В хода на проучването може да се установи, че лицето не отговаря на изискванията на чл. 40, ал. 1 или проучваното лице съзнателно е представило неверни или непълни данни за целите на проучването. В такъв случай проучващият орган издава **отказ** за достъп до национална класифицирана информация. Отказът не се мотивира, а само се посочва правното основание. Проучвано лице, на което е отказано разрешение за достъп до класифицирана информация, няма право да кандидатства за заемане на длъжност или за изпълнение на конкретна задача, свързана с работа с класифицирана информация от същото или по-високо ниво на класификация, за срок от една година от издаването на отказа.

Отнемане и прекратяване

По време на текущия контрол, който проучващият орган осъществява, може да се установи, че има нови факти и обстоятелства относно лоялността на лицето. Може да констатира, че лицето е извършило нарушение на закона или на подзаконовите актове по прилагането му, което е създало опасност от възникване или е довело до значителни вреди за интересите на държавата, организациите или лицата в областта на защитата на класифицираната информация, или че лицето е извършило системни нарушения на закона или на подзаконовите актове, свързани със защитата на класифицираната информация. В такъв случай проучващият орган **отнема** разрешението. Отнемането на издаденото разрешение за достъп до класифицирана информация не се мотивира, а се посочва само правното основание и не подлежи на обжалване по съдебен ред. Лице, на което е отнето разрешението за достъп до класифицирана информация, няма право да кандидатства за заемане на длъжност или за изпълнение на конкретна задача, свързана с работа с класифицирана информация, за срок от три години от отнемането.

Разрешението може да бъде **прекратено** при смърт на лицето, изтичане сроковете на валидност, промяна в необходимостта от достъп до по-високо

ниво на класификация за сигурност на информацията или отпадане на необходимостта от достъп до класифицирана информация. Както и другите два акта, прекратяването също не може да бъде обжалвано по съдебен ред.

Процедура по обжалване

Лицето, на което е издаден отказ, отнемане или прекратяване, може да подаде жалба единствено пред ДКСИ. Срокът за обжалване е 7-дневен считано от уведомяването на лицето. Жалбата трябва да бъде подадена в писмен вид чрез органа, издал акта, който се обжалва. В 7-дневен срок проучващият орган трябва да преразгледа решението си и ако прецени, че постановеният акт е неоснователен – да издаде разрешение за достъп. При преценка, че жалбата е неоснователна, проучващият орган я изпраща в ДКСИ. В случай, че в 7-дневния срок жалбата не е подадена от проучващия орган в Комисията, жалбоподателят има право да изпрати препис от нея. Тогава ДКСИ изисква по служебен път преписката. След получаването ѝ при необходимост се събират нови доказателства. Срокът, в който ДКСИ трябва да се произнесе е две седмици. Решението, с което се произнася е: отмяна на административния акт за отказ, отнемане или прекратяване или отхвърля жалбата. В 3-дневен срок от постановяване на решението ДКСИ го съобщава на жалбоподателя, на органа, чийто акт се обжалва и на организационната единица. Решението на ДКСИ подлежи на обжалване пред Върховен административен съд. Жалбата се подава в 14-дневен срок до Върховния административен съд, който се произнася в срок до един месец и решението му е окончателно.

Отказът, прекратяването и отнемането на издадено разрешение за достъп до класифицирана информация, издадени от ДКСИ, подлежат на обжалване пред Върховен административен съд. Решението на съда е окончателно.

4. Дела по проучване за надеждност

Делата по проучване за надеждност (ДПН) се откриват от компетентния проучващ орган;

Делата по проучване за надеждност се съхраняват, поддържат, актуализират, картотекират и закриват от органа, извършил проучването;

Срок на съхранение – не-повече от пет години след изтичането на срока на разрешението.

Съдържание на делото по проучване за надеждност

Раздел I

- опис на документите, съдържащи се в ДПН на лицето;
- списък на служителите, запознали се с ДПН;
- регистрационна бланка на делото;
- материалите по чл. 71 от ЗЗКИ;
- справки по оперативния отчет на службите за сигурност и службите за обществен ред и справки за извършени проверки в информационните фондове;
- други справки и данни за лицето, събирани в хода на проучването.

Раздел II

- разрешения;
- отнети или прекратени разрешения;
- откази;
- сертификати.

5. Обучение и контрол

Обучение

След като лицето получи разрешение за достъп до национална класифицирана информация, то трябва да премине първоначално обучение за работа с класифицирана информация. **Обучението** в областта на защитата на класифицираната информация се осъществява с цел придобиване на знания, умения и опит за работа с класифицирана информация. Обучението включва: първоначално изучаване на правилата за защита на класифицираната информация и текущо обучение за повишаване на квалификацията и опита на лицата с разрешение за достъп. Целта на първоначалното обучение е лицата да бъдат запознати със ЗЗКИ и подзаконовите актове в областта на защитата на класифицираната информация. Също така придобиване на практически умения за прилагане на закона и усвояване на специфични професионални умения, необходими за изпълнение на съответната длъжност, изискваща работа с класифицираната информация. Общата задължителна подготовка е еднаква за всяко обучение за работа с класифицираната информация, което се провежда за заемане на конкретна длъжност или изпълнение на определена задача, свързана с достъпа до класифицирана информация. Задължителното функционално обучение се провежда за съответната длъжност и е насочено към усвояване на знания и умения за изпълнение на функционалните задължения.

Контрол

Една от функциите на проучващия орган е да осъществява **контрол** за надеждност на лицата, получили достъп до национална класифицирана информация. Целта е да бъде осъществен пряк контрол по защитата на класифицираната информация. Да бъдат спазени нормативните актове в тази област, както и отстраняване на всички рискове и заплахи, чиито проявление би довело до нерегламентиран достъп до класифицирана информация.

Контролът за надеждност на лицата, получили достъп до класифицирана информация, е установен с цел да се гарантира, че те ще отговарят на изискванията за надеждност и след приключване на процедурата по проучване.

Контролът може да бъде осъществяван докато това е необходимо, съгласно сроковете за защита на класифицираната информация, а не само в рамките на действието на разрешението за достъп на лицето. За разлика от проучването за надеждност и обучението за работа с класифицирана информация, които имат превантивен характер, контролът е перманентна дейност.

6. Обобщение

Персоналната сигурност на класифицираната информация има за цел и е насочена към неутрализиране на заплахите, които едно физическо лице, имащо достъп до класифицирана информация, може да създаде. Поради това като предварително изискване се установява преценката на надеждността на лицето, обучението му за работа с класифицирана информация и спазване на принципа „необходимост да се знае”.

Определянето на едно лице като надеждно, от гледна точка на персоналната сигурност, става в резултат на прилагането на принципите и мерките, предвидени в тази област. По същество това е процес, който изисква известен период от време и се извършва в контекста на обичайни за лицето условия и среда.

ФИЗИЧЕСКА СИГУРНОСТ

1. Същност и особености на физическата сигурност

Физическата сигурност на класифицираната информация включва система от мерки, способи и средства за предотвратяване на нерегламентиран достъп до материали, документи, техника и съоръжения, класифицирани като държавна или служебна тайна. Системата от мерки има за цел:

- да защити сградите, помещенията и съоръженията, в които се създава, обработва и съхранява класифицирана информация;
- да създаде организация за осъществяване на ефективен контрол върху достъпа до тях.

Съгласно Закона за защита на класифицираната информация (ЗЗКИ) физическата сигурност се прилага за защита на класифицираната информация от всяка заплаха или вреда в резултат на терористична дейност, саботаж, нерегламентиран достъп до класифицирана информация или опит за такъв.

Нормативна уредба за защита на класифицираната информация

Нормативната уредба, въз основа на която се прилагат мерките за физическата сигурност, са подробно описани в Наредбата за системата от мерки, способи и средства за физическа сигурност и за условията и реда за тяхното използване, приета с ПМС № 52 от 04.03.2003 г. обн. в ДВ, бр.22 от 11.03.2003 г., която накратко ще наричаме Наредбата.

Цифровата оценка за степента на защита, която сме постигнали, прилагайки системата от мерки, способи и средства за защита на класифицираната информация се получава след прилагане на Методиката за оценка на средствата и системите за физическа сигурност на класифицираната информация, приета с решение на ДКСИ № 26-I/10.04.2012 г. и попълване на Таблицата за оценка.

Самата методика е нова като философия. Тя ни позволява, ако нямаме възможност да завишим повече дадено средство за защита, да усилим друго, така че крайният математически резултат да бъде удовлетворителен.

Самата система от мерки може да бъде разгледана съгласно ЗЗКИ и съгласно Наредбата. ЗЗКИ обособява мерките като:

- Организационни – наредби, инструкции и вътрешни правила за организиране защитата на класифицираната информация.
- Физически – физическа охрана, пропускателен режим и др.
- Технически – изграждане на алармени системи против проникване, видеонаблюдение, пожарогасителни, пожароизвестителни системи и други.

Наредбата обособява мерките за физическата сигурност като:

Общи мерки

Те са организационни и се изразяват в определяне и изграждане на зоните за сигурност.

В изпълнение на чл. 74 от ЗЗКИ ръководителят на организационната единица с помощта на служителя по сигурността на информацията следва да определи със заповед зоните за сигурност, а около тях и административни зони, в които се извършва контрол на хора и моторни превозни средства. Въвеждат контролиран режим на влизане, движение и излизане от зоните за сигурност, както и задължително придружаване на лица в тези зони или на лица с право на достъп до по-ниски нива или на лица без достъп до класифицирана информация. Чрез служители от звеното за сигурност осигуряват съответния контрол над зоните за сигурност и административните зони. Задължително въвеждат специален режим на съхраняване на ключове от помещения, каси и други помещения и съоръжения, служещи за съхраняване на класифицирана информация.

Изискванията към зоните за сигурност са подробно указани в гл. III на Наредбата – „Изграждане на зони за сигурност“. Въпреки това в немалко организационни единици се допускат грешки при определяне на зоните за сигурност клас I и клас II.

Зона за сигурност клас I е зона, в която се създава, обработва, съхранява или предоставя информация с ниво на класификация „Поверително” или по-високо, по начин, осигуряващ пряк достъп до тази информация при влизане в зоната.

Зона за сигурност клас II е зона, в която се създава, обработва, съхранява или предоставя информация с ниво на класификация „Поверително” или по-високо по начин, непозволяващ пряк достъп до тази информация при влизане в зоната.

Около зоните за сигурност клас I и клас II се изгражда административна зона, която да отговаря на следните изисквания:

- Видимо определен периметър, позволяващ контрол на лица и транспортни средства.
- Осигурен пропускателен режим на входа и на изхода на периметъра.

В административната зона може да се създава, обработва, съхранява или предоставя единствено класифицирана информация с ниво на класификация „За служебно ползване”.

Системата за контрол на физическия достъп се изгражда така, че да позволява влизането само на лица, притежаващи разрешение за достъп до съответното ниво на класификация на информацията и при спазване на принципа „необходимост да се знае”. За всички останали лица се осигурява придружител .

Конкретни мерки

Те са описани в чл. 8 ал. 3 от Наредбата и включват:

- **Определяне и изграждане на периметъра**

Трябва да е налице ясно обозначена външна граница на зоните за сигурност, които изискват защита.

Поставят се физически бариери и технически средства, възпрепятстващи нерегламентирания достъп. Степента на прилагане на тези средства зависи от нивото и обема на класифицираната информация, която се съхранява в зоната за сигурност.

– Защитно осветление – трябва да осигурява възможност за ефективно наблюдение от страна на звеното за сигурност и охрана и техническите средства за защита.

– Алармени системи против проникване (АСПП)

За повишаване нивото на защита на периметъра в зоните за сигурност се използват АСПП. Тези системи са задължителни. Те сигнализират при опит за нерегламентиран достъп или осъществен такъв и се използват съгласно плана за физическа сигурност на обекта.

- **Контрол на физическия достъп**

Осъществява се от служителите от звеното за сигурност и охрана. Дейността им се регламентира с инструкция, утвърдена от ръководителя на организационната единица. Контролът на физическия достъп се осъществява чрез:

– технически и физически средства за защита;

– регистриране на всички лица,пребивавали в зоната;

– списък на внасяни или изнасяни в зоната технически средства или оборудване и др.

- **Защита срещу подслушване и наблюдение**. Подслушването и наблюдението бива пасивно и активно.

Пасивно – чрез незащитени комуникации, директно без специални средства или прихващане на електромагнитните излъчвания от комуникационните и информационните системи.

Активно – чрез жични микрофони, радиомикрофони или други вградени устройства.

Защитата при пасивно подслушване и наблюдение се извършва чрез намаляване и изолиране на електромагнитните излъчвания, криптиране на информацията, звукоизолиране на помещенията.

Защитата при активно подслушване и наблюдение се осъществява чрез техническа или физическа проверка за сигурност на конструкцията, мебелировката, инсталациите, офис оборудването, включително машини, средства за комуникация и др.

- Защита срещу визуално наблюдение;
- Визуално наблюдение (системи за видеонаблюдение с камери);
- Сили за реагиране – звено за сигурност и охрана;

- Пожарогасителна или пожароизвестителна система.

Специални мерки

Специалните мерки за физическа сигурност на класифицираната информация се прилагат, когато се налага транспортиране на документи и материали, които поради своето естество или размери не могат да бъдат пренасяни по общия ред, предвиден в ППЗЗКИ. При транспортирането на материалния носител на класифицирана информация, ръководителят на организационната единица изпращач изготвя анализ на риска и план за транспортирането.

Да обобщим мерките за физическа сигурност. Те са общи, конкретни и специални и имат за цел:

- предотвратяване на нерегламентиран достъп или на опит за нерегламентиран достъп до класифицирана информация;
- предотвратяване, пресичане и установяване на действия, които поставят под съмнение надеждността на служителите;
- групиране на служителите съобразно издаденото им разрешение за достъп до класифицирана информация и в съответствие с принципа „необходимост да се знае”;
- своевременно установяване и противодействие при нарушаване или при опит за нарушаване на мерките за физическа сигурност.

Когато класифицираната информация се съдържа в самия разговор, който се провежда между лица, които имат разрешения за достъп до класифицирана информация се обособяват технически осигурени зони.

При тях се прилагат:

- всички мерки за физическа защита срещу подслушване и наблюдение;
- допълнителни мерки – контрол на физическия достъп.

Физически достъп се осъществява чрез технически и физически средства за защита. Регистрират се всички лица, пребивавали в зоната за сигурност. Водят се на отчет (списък) всички внасяни или изнасяни от зоната технически средства или оборудване и други.

- технически и физически проверки;
- проверка за наличие на подслушвателни устройства.

Проверките се извършват:

- при първоначално използване;
- преди и след провеждането на срещите;
- при наличието на нерегламентиран достъп или при опит за такъв;
- периодично, но най-малко веднъж на 6 месеца;
- след извършване на ремонтни или строително-монтажни дейности.

Обособяване на технически осигурени зони

При изграждането и експлоатацията им се прилагат всички мерки за физическа защита срещу подслушване и наблюдение, както и следните допълнителни мерки:

- контрол на физическия достъп;
- технически и физически проверки;
- проверка за наличие на подслушвателни устройства.

В технически осигурените зони се забранява:

- инсталирането и използването на комуникационни устройства;
- внасянето на мобилни телефони или други електромагнитни устройства;
- инсталирането и използването на средства за прием или предаване на данни;
- експлоатацията на записваща и озвучаваща апаратура;
- използването на електронно-изчислителна техника, имаща връзка с апаратури и мрежи извън технически осигурената зона (интернет).

Проверката за комплексна оценка на физическата защита срещу нерегламентирано прихващане на класифицираната информация на помещенията се извършва след писмено искане от ръководителя на организационната единица. Проверяващият орган по чл. 20 от ЗСРС (ДАТО, ДАНС, ДАР и МО) дава предписание за състоянието на проверявана зона.

Контрол на ключовете и шифровите комбинации на касите

- **Ключове за каси** – задължително се използват два ключа, единият се използва постоянно, а другият е резервен и се съхранява в друга каса, обикновено в дежурната част. Забранява се изнасянето на ключовете извън зоните за сигурност.
- **Шифрови комбинации** – при касите, в които се съхранява информация с ниво на класификация “Строго секретно” се използват и шифрови комбинации. Служителят е длъжен да възпроизведе писмено шифровата комбинация и заедно с резервния ключ да ги предостави в запечатан плик на дежурната част.

Шифровите комбинации се **променят:**

– при първоначално използване;
– в случай на смяна на някое от лицата;
– в случай на нерегламентиран достъп или опит за такъв;
– след извършен ремонт на касата или на заключващия механизъм;
– през период не по-дълъг от 12 месеца.

2. Способи за предотвратяване на заплахите за физическа сигурност

Анализ на риска

Това е непрекъснат аналитично-информационен процес по събирането на данни и техния анализ и оценка от гледна точка на физическата защита на класифицираната информация. Този анализ цели установяване на всяка заплаха или вреда, както и влиянието и последиците при тяхното проявление. Процесът по анализа включва:

- определяне на обекта, подложен на риск;
- установяване степента на застрашеност и уязвимост на обекта от нерегламентиран достъп до класифицирана информация;
- анализ на съществуващите мерки за физическа защита; изграждане и усъвършенстване на системата от мерки за физическа защита; определяне стойността на мерките;
- избор на вариант за осъществяване на физическа защита;
- описание на остатъчна заплаха и нейното допустимо проявление;
- изграждане и усъвършенстване на системата от мерки за физическа защита;
- описание на остатъчна заплаха и нейното допустимо проявление;
- периодични проверки, преразглеждане и преоценка.

План за осигуряване на физическата сигурност

След анализ на риска служителят по сигурността на информацията разработва план за физическа сигурност. Планът отчита особеностите на обекта и включва:

- целта на физическата защита – конкретно посочване на всички параметри на обектите, които изискват физическа защита;
- определяне на зоните за сигурност – посочване на конкретните мерки за физическа сигурност;
- органите, отговорни за планирането и прилагането на мерките;
- периодични проверки;
- контрол по изпълнението на плана.

Планът се съставя при спазване на принципа **„защита в дълбочина”,** разполагане на силите и средствата за защита в зоните за сигурност и включва: определяне на охраняваната територия и предотвратяване на нерегламентиран достъп до нея; регистриране на нерегламентиран достъп или опит за такъв и сигнализиране на силите за реагиране; забавяне и ограничаване на нарушителя до задържането му. Времето за реагиране следва да бъде по-малко от времето, необходимо на нарушителя за преодоляване на мерките за физическа сигурност.

Планът за осигуряване на физическата сигурност на класифицираната информация отчита особеностите на обекта и включва:

– целта на физическата защита;

– конкретно посочване на всички параметри на обектите, които изискват физическа защита;

– определяне на зоните за сигурност;

– посочване на конкретните мерки за физическа сигурност;

– органите, отговорни за планирането и прилагането на мерките;

– периодични проверки;

– контрол по изпълнението на плана.

Етапи на изграждане на средствата и системите за сигурност

- изработване на техническо задание и определяне на изпълнител;
- изготвяне на технически проект от кандидатите за изпълнители на технически проект;
- изграждане и сертифициране на системите за сигурност;
- проверка за изпълнение на изискванията за защита на класифицираната информация;
- получаване на удостоверение (сертификат) за всяко отделно средство и система с определена индентификация (производствен номер);
- последващ контрол за изпълнение на изискванията за физическа сигурност.

РАЗКРИВАНЕ, ФУНКЦИОНИРАНЕ И ЗАКРИВАНЕ НА РЕГИСТРАТУРИ ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Настоящата лекция има за цел да разгледа изискванията и процедурата по разкриване на регистратура за национална класифицирана информация в организационните единици, както и да обхване процесите, възникнали след разкриване на регистратурата, свързани с промяна в статута й и нейното закриване.

1. Процедура по разкриване, функциониране и закриване на регистратура (нормативна уредба)

Процедурата по Разкриване на регистратура за класифицирана информация е нормативно уредена в чл. 54 от Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ). Тя подробно е разписана стъпка по стъпка в Задължителните указания за разкриване, функциониране и закриване на регистратура за класифицирана информация, приети с Решение на ДКСИ № 55-I-17/28.07.2016 г., изм. с Решение на ДКСИ № 83-II/19.10.2017 г.

Определението за регистратура е дадено в т. 7 от § 1 на Допълнителните разпоредби на ЗЗКИ – „Регистратура е обособена структура, в която се регистрира, получава, изпраща, разпределя, изработва, размножава, предоставя и съхранява класифицирана информация”.

2. Разкриване на регистратура за класифицирана информация – същност и особености

Решението за разкриване на регистратура се взема от ръководителя на организационната единица въз основа на анализ и преценка относно необходимостта за получаване, създаване, регистриране, обработване, разпределяне, предоставяне, размножаване и съхраняване на класифицирана информация. Разкриването на регистратура се осъществява след назначаване на комисия по чл. 54, ал. 2 от ППЗЗКИ и извършване на проверка, изготвяне на протокол и изпращането му.

В областта на физическата сигурност на класифицираната информация **документите** необходими за разкриване и функциониране на регистратура за класифицирана информация са следните: Анализ на риска, План за физическата сигурност, Заповед за изграждане на зоните за сигурност, Инструкция за действия на служителите при нерегламентиран достъп, Заповед за контрол на ключовете и шифровите комбинации, Инструкция за пропускателния режим, Вътрешни правила за правилното определяне на нивото на класификация, както

и неговата промяна или премахване, План за защита на класифицираната информация при положение на война, бедствия и аварии.

Принципите, прилагани при оборудване на регистратурата са:

- да се гарантира защитата на класифицирана информация от нерегламентиран достъп;
- да не се позволи разкриването на вида и характера на извършената в тях дейност.

Достъп до помещенията на регистратурите за класифицирана информация имат:

- служители от регистратурата, ръководителят на организационната единица, служителят по сигурността на информацията и лицата, определени със заповедта по чл. 12 от ЗЗКИ;
- други лица – при необходимост след писмено разрешение от служителя по сигурността на информацията за достъп до помещенията на регистратурите за класифицирана информация

При бедствия и аварии достъпът до регистратурите за класифицирана информация в работно време се осигурява от завеждащия регистратурата за класифицирана информация, а в извън работно време – от упълномощено длъжностно лице от организационната единица.

Нивото на съответната регистратура се определя в зависимост от най-високото ниво на класификация на класифицираните документи, които ще се създават или съхраняват в нея. Правото на преценка е на ръководителя на организационната единица, а не на ДКСИ или органа по прекия контрол. Ако след разкриването на регистратурата и получаването на уникален идентификационен номер (УИН) се установи, че нивото не съответства на реално необходимото могат да бъдат направени промени в статута на регистратурата, както в посока сваляне на нивото, така и за повишаване нивото на класификация. Това би следвало да стане въз основа на анализ на документите, създадени или получени в регистратурата.

При необходимост в една и съща организационна единица може да се създават повече от една регистратури. В структурата на регистратурата при необходимост може да се включат и други звена, работещи с класифицирана информация, като машинописно, размножително, библиографско, стенографско, чертожно, редакторско, разпределително-куриерско и др.

Проверката за разкриване на регистратура се извършва от комисия, назначена от ръководителя на организационната единица, която включва лицата, изброени в чл. 54, ал. 2 от ППЗЗКИ, а именно служителя по сигурността на информацията, представител на съответната организационна единица и

представител на службата за сигурност – Държавна агенция „Национална сигурност” (ДАНС).

В проверката следва да участва служителят по сигурността на информацията на съответната организационна единица, но само след като самият той има издадено разрешение за достъп до класифицирана информация от ДКСИ и след като бъде назначен на тази длъжност от ръководителя й. Участие на лице в качеството на служител по сигурността на информацията, което няма надлежно издадено разрешение за достъп от ДКСИ, съответстващо на нивото на класификация на регистратурата, прави проверката нищожна.

Представителят на организационната единица, включен в комисията, също трябва да има издадено разрешение за достъп до определеното ниво на класификация на изградената регистратура.

Специално внимание заслужават способите за предотвратяване на заплахите, а именно анализът на риска и планът за осигуряване на физическа сигурност. Целта на тези способи е насочена към създаване на ефективни методи за противодействие на заплахите за физическата сигурност чрез използване на защитни мерки.

Съгласно разпоредбите на чл. 51, ал. 5 от ППЗЗКИ при необходимост временно **могат да се откриват контролни пунктове** (КП), които са поделения на съответната регистратура. Тези пунктове трябва да са създали условия за създаване, получаване, регистриране, разпространяване, размножаване и охрана на класифицираната информация, получена от същата регистратура, а когато са упълномощени от ДКСИ – и от други регистратури. Контролният пункт води на отчет движението на материалите – носители на класифицирана информация, които са регистрирани в него.

За контролен пункт се осигуряват помещения, намиращи се в съответни на нивата на класификация на информацията зони за сигурност и защитени с необходимите по ЗЗКИ и ППЗЗКИ мерки за защита на класифицираната информация.

При необходимост в организационната единица може да се разкриват и **специализирани звена за съхраняване на материали, съдържащи класифицирана информация (**СЗСКИ), на основание чл. 52 от ППЗЗКИ от ръководителя на организационната единица, съгласувано с ДКСИ.

За СЗСКИ се ползват помещения, намиращи се в зона за сигурност на организационната единица при прилагане на мерките за физическа сигурност.

В задграничните представителства на Р България, съгласувано с ДКСИ могат да се разкриват специализираните звена за създаване, обработване, съхраняване и унищожаване на материали, съдържащи класифицирана информация.

Ръководителят на организационната единица определя начина за работа с класифицираните материали в СЗСКИ в съответствие с изискванията на ЗЗКИ и всички подзаконови актови в областта на защитата на класифицираната информация.

Анализ на риска

Основополагащ документ е Анализът на риска. По своята същност способът „Анализ на риска" е оценка на заплахите и представлява непрекъснат аналитично-информационен процес по събирането на данни и техния анализ и оценка. Анализът на риска цели установяване на всяка заплаха или вреда в резултат на нерегламентиран достъп, опит за нерегламентиран достъп, терористична дейност или саботаж, както и влиянието и последиците при тяхното проявление.

Анализът на риска включва в себе си следните раздели:

- Цел – установяване на заплаха или вреда в резултат на нерегламентиран достъп, терористична дейност или саботаж, причините, които пораждат и условията, спомагащи този достъп, както и влиянието и последиците при тяхното проявление.
- Параметри, при които се извършва оценката на риска:

– нивото на класификация на информацията, с което ще се работи в регистратурата;

– обема на класифицирана информация и вида на нейните носители в регистратурата;

– видовете носители на класифицирана информация, с които ще се работи в регистратурата;

– броя на издадените разрешения за достъп и нивата на класификация, за които са издадени, при спазване на принципа „необходимост да се знае" – разделени по нива и по видове (за национална и чуждестранна класифицирана информация).

– обекти, подложени на риск, помещения, в които ще се работи с класифицирана информация в организационната единица – регистратурата, кабинети, хранилища и работни помещения.

- Процес по анализ на риска:

– определяне състоянието на обекта като цяло (сградата), в която ще се създава, съхранява, обработва и предоставя класифицирана информация, подложен на риск.

– описват се стените, подовете и тавани и тяхната пожароустойчивост;

– вратите и прозорците и наличието на метални решетки;

– водопроводи и канализация;

– отстояние на регистратурата от покрива и от земята от гледна точка на нейната безопасност както и изпълнението на изискванията на чл. 14 от Наредбата за системата от мерки, способи и средства за физическа сигурност на класифицираната информация и за условията и реда за тяхното използване (нар. по-нататък Наредбата) за избор на оптимално помещение с цел защита на класифицираната информация;

– описва се вида на отоплението, вентилация и климатизация, ако съществуват такива.

- Анализ на съществуващите мерки за физическа сигурност (общи и конкретни).
- Описване на остатъчния риск и мерки, които ще се приложат за усъвършенстване на системата за физическа сигурност.

– определяне стойността на мерките за физическа защита;

– избор на вариант за осъществяване на физическа защита от звеното за сигурност и охрана;

– описание на остатъчната заплаха и нейното допустимо проявление;

– периодичност на проверките, преразглеждане и преоценка.

План за физическа сигурност

В изпълнение на задълженията си по чл. 22, ал. 1, т. 3 от Закона за защита на класифицираната информация (ЗЗКИ), въз основа на Анализа на риска, служителят по сигурността на информацията изготвя план за физическата сигурност, който се утвърждава от ръководителя на организационната единица.

В плана се описват физическите и техническите средства, чрез които се осъществява физическата защита на класифицираната информация и видовете контрол по неговото изпълнение.

Планът отчита особеностите на обекта на защита и включва:

- цел на физическата защита;
- параметри на обектите, които изискват физическа защита;
- определените със заповед на ръководителя на организационната единица зони за сигурност и техният обхват;
- конкретните мерки за физическа сигурност по смисъла на Наредбата;
- органите или лицата, отговорни за планирането и прилагането на мерките за сигурност;
- периодичност на проверки (ежедневни, седмични и месечни);
- контрол по изпълнението на плана.

Планът за физическа сигурност на организационната единица се изготвя при спазване на принципа „защита в дълбочина”, съобразно който силите и

средствата се разполагат в зоните за сигурност и включват: определяне на охраняваната територия, предотвратяване на нерегламентиран достъп до нея, регистриране на нерегламентиран достъп или опит за такъв, сигнализиране на силите за реагиране, забавяне и ограничаване на нарушителя до задържането му, като времето за реакция на силите за реагиране следва да бъде по-малко от времето, необходимо на нарушителя за преодоляване на мерките за физическа сигурност.

В изпълнение на чл.74 от ЗЗКИ ръководителят на организационната единица с помощта на служителя по сигурността на информацията следва да определят със заповед зоните за сигурност и административните зони. Тези зони са с определен периметър и осигурен контрол на входа и изхода им. Системата за контрол на физическия достъп се изгражда, така че да позволява влизането само на лица, притежаващи разрешение за достъп до съответното ниво на класификация на информацията и при спазване на принципа „необходимост да се знае". За всички останали лица се осигурява придружител.

Изискванията за зоните за сигурност (в които се създава, съхранява, обработва или предоставя класифицирана информация, представляваща държавна тайна) са подробно указани в гл. III „Изграждане на зони за сигурност" на Наредбата. Около зоните за сигурност клас I и клас II се изгражда административна зона, в която може да се създава, обработва, съхранява или предоставя единствено класифицирана информация, представляваща служебна тайна.

В няколко текста от ЗЗКИ и ППЗЗКИ, отнасящи се до задълженията на завеждащ регистратурата и служителя по сигурността на информацията (ССИ) е указано какви действия следва да се предприемат при установяване на нерегламентиран достъп до класифицирана информация. В рамките на организационната единица тези действия трябва да бъдат регламентирани със заповед.

Завеждащият регистратура съгласно чл. 62, ал. 2, т. 1 от ППЗЗКИ е задължен периодично да проверява наличността и начина на съхраняване на материалите, съдържащи класифицирана информация, които се намират при служителите от организационната единица. При установяване на нарушения или на нерегламентиран достъп до класифицирана информация той трябва да докладва писмено на служителя по сигурността на информацията и ръководителя на организационната единица. В изпълнение на чл. 63 от ППЗЗКИ при установяване на нарушения на съответните мерки за физическа сигурност в помещенията на регистратурата служителите, работещи в нея, са задължени незабавно да уведомяват служителя по сигурността на

информацията и звеното за охрана на организационната единица, като вземат мерки за запазване на фактическата обстановка.

В изпълнение на т. 3, 4 и 5 от чл. 74 от ЗЗКИ служителят по сигурността на информацията следва да регламентира начина, по който се осъществява контрола на ключовете и шифровите комбинации. Основните изисквания за контрола на ключовете и шифровите комбинации са разработени в гл. V на Наредбата. При подготовката на тези документи следва да бъде акцентирано на конкретните условия за защита на класифицираната информация в организационната единица, както и да се конкретизират задълженията на длъжностните лица.

Задължителен документ при разкриване на регистратура за класифицирана информация, който е от съществено значение за недопускане на нарушения на документалната сигурност и се оформя като заповед на ръководителя на организационната единица са Вътрешни правила за правилното определяне на нивото на класификация, както и неговата промяна или премахване. Тези правила се издават на основание чл. 81 от ЗЗКИ и чл. 49 от ППЗЗКИ.

Въпреки, че тези въпроси са подробно регламентирани в гл. V „Документална сигурност“ на ППЗЗКИ, прилагането на отделните изисквания, съобразени с конкретните специфики в организационната единица имат голямо практическо значение. Без да се опитваме да шаблонизираме изготвянето на такива правила, обобщавайки практическия опит на няколко експерти препоръчваме следната им структура:

- цел;
- обхват;
- принципи и основни изисквания към дейността;
- отговорности;
- класифициране на информацията;
- маркиране на информацията
- ред за ползване на класифицираната информация в организационната единица;
- размножаване на класифицираната информация;
- задължения на служителите;
- контрол върху изпълнение на дейностите;
- приложения.

Друг документ, който комисията по чл. 54 от ППЗЗКИ проверява дали е изготвен е План за защита на класифицираната информация при положение на война, бедствия и аварии. Той трябва да е съобразен с общия план на

ведомството. В него трябва да са указани действията на служителите от организационната единица при различните видове тревога, както и да е посочено транспортното, медицинското и химическото обезпечаване при видовете тревоги.

Процедурата за извършване на проверката по разкриване на регистратура за класифицирана информация задължително трябва да включва констатации по отношение и на следните обстоятелства:

- изпълнение на изискванията за защита на класифицираната информация в съответната регистратура;
- реда и условията за работа в регистратурата;
- изпълнение изискванията на чл. 37 от ЗЗКИ за наличие на утвърден и изпратен списък на длъжностите и задачите, за които се изисква достъп до съответното ниво на класифицирана информация;
- дали назначените служители за работа в регистратурата отговарят на изискванията на чл. 38, ал. 1, т. 1 и 2 от ЗЗКИ и на чл. 61 от ППЗЗКИ – да са проучени за надеждност, да са преминали обучение по защита на класифицираната информация, преди започване на работа в регистратурата;
- дали са въведени в експлоатация и начина на водене на новите регистри по ППЗЗКИ;
- проверка на наличните документи и начина им на съхранение в регистратурата;
- проверка дали регистратурата отговаря на изискванията за физическа сигурност по ЗЗКИ, ППЗЗКИ и Наредбата.
- средствата за физическа сигурност следва да са сертифицирани за всяко ниво на класификация съгласно изискванията на чл. 4 от Наредбата;
- проверка дали начинът на унищожаване на документи съответства на изискванията на ЗЗКИ и ППЗЗКИ;
- проверка за съответствие със законовите изисквания на определяне грифовете за сигурност на създаваните в регистратурата документи (дали е приложен § 9 от Преходните и заключителни разпоредби на ЗЗКИ);
- проверка за спазване на задължителните специфични изисквания за сигурност на КИС;
- проверка дали са изготвени и утвърдени от ръководителя на организационната единица задължителните документи за функционирането на регистратурата.

За да може всяка една регистратура за класифицирана информация да функционира нормално, е необходимо да има определен със заповед на ръководителя на организационната единица заместник на завеждащия

регистратурата, който да отговаря на условията за работа в регистратурата – да има разрешение за достъп до съответното ниво и да е преминал обучение .

Назначената комисия по чл. 54 от ППЗЗКИ изготвя протокол в 3 екземпляра след извършване на проверката – за ДКСИ, за службата за сигурност (ДАНС) и за организационната единица.

След получаване на протокола ДКСИ взема решение за разкриване на регистратурата и издаване на УИН. Издава се сертификат на регистратурата, който трябва да бъде поставен в зоната за сигурност клас II в съответната регистратура.

За всички промени, свързани със статута на регистратурата за класифицирана информация, както и при откриване на контролните пунктове следва да бъде отправено писмено уведомление до ДКСИ и органа по прекия контрол. Потвърждаването на УИН на изградена и сертифицирана регистратура за класифицирана информация, както и при контролните пунктове се извършва от ДКСИ в случаите на промяна на местоположението, нивото на сигурност и промяна в наименованието на организационната единица, вследствие преструктуриране и/или преобразуване.

В случаите, когато **промяната е свързана с местоположението** или повишаване нивото на сигурност**,** ръководителят на организационната единица назначава комисия по реда на чл. 54, ал. 2 от ППЗЗКИ. След извършване на проверка за изпълнение изискванията за защита на класифицираната информация комисията изготвя протокол, екземпляр от който съгласно чл. 54, ал. 3 от ППЗЗКИ се изпраща на ДКСИ и органа по прекия контрол. ДКСИ разглежда на свое заседание отразените в протокола констатации на комисията и взема решение за потвърждаване на издадения УИН.

В случаите, когато се **понижава нивото на сигурност**, към изготвения протокол по чл. 54 от ППЗЗКИ се прилага протокол за преразглеждане или унищожаване на документите, съдържащи класифицирана информация с по-висок гриф на сигурност, съхранявани в регистратурата (контролния пункт) към момента на разкриването ѝ или опис на предадените в друга регистратура документи, при спазване на съответните нормативни изисквания.

В случаите, когато се **променя наименованието на организационната единица**, вследствие преструктуриране и/или преобразуване, както и при други обстоятелства, ръководителят на организационната единица изпраща уведомително писмо до ДКСИ, което съдържа потвърждение (декларация), че в регистратурата (контролен пункт) са запазени мерките за физическа сигурност при изграждането ѝ. Към писмото следва да бъде приложено и съдебно решение или друг документ за промените в статута и наименованието на организационната единица, независимо от правноорганизационната ѝ форма.

Във всички случаи ДКСИ извършва актуализация на данните в информационните си масиви за съответната регистратура (контролен пункт), респективно организационна единица.

Издадените сертификати за регистратурите за класифицирана информация (контролен пункт) се преиздават с новите данни след връщането на предходно издадения сертификат.

3. Закриване на регистратура за класифицирана информация – същност и особености

Регистратура за класифицирана информация се закрива, когато в нея не се създава, обработва, съхранява или предоставя класифицирана информация, поради връщане на информацията на организационните единици, от които е била получена, унищожаване или предаване в архив по правилата на гл. V, раздел IX или по други причини по реда на чл. 54 б от ППЗЗКИ.

Предложението за закриване на регистратурата се изготвя от служителя по сигурността на информацията освен при обективна невъзможност и се утвърждава от ръководителя на организационната единица, съгласно изискванията на чл. 54б от ППЗЗКИ.

Към предложението за закриване на регистратурата се прилага издадения от ДКСИ сертификат на съответната регистратура за класифицирана информация.

В предложението задължително се посочва броят на съхраняваните в регистратурата документи и материали през времето на нейното функциониране и причината за закриване на регистратурата. Екземпляр от предложението се изпраща до ДКСИ и органа по прекия контрол (ДАНС).

Органът по прекия контрол задължително извършва проверка по правилата на Наредбата за реда за извършване на проверките за осъществяване на пряк контрол по защита на класифицираната информация (тематична инцидентна проверка). След приключване на проверката органът по прекия контрол изпраща до ДКСИ доклад за извършената проверка.

Въз основа на данните от предложението и доклада ДКСИ взима решение за анулиране на уникалния идентификационен номер, за което уведомява организационната единица и органа по прекия контрол .

При необходимост ДКСИ може да изисква допълнителна информация от задължените по ЗЗКИ субекти, която те са длъжни да предоставят.

ДОКУМЕНТАЛНА СИГУРНОСТ

1. Същност и особености на документалната сигурност

Понятието „**класифицирана информация**“ се въвежда за първи път със Закона за защита на класифицираната информация (ЗЗКИ), обнародван в ДВ бр.45 от 30.04.2002 г. Това е общо понятие, което включва информацията, представляваща държавна тайна, служебна тайна и чуждестранна класифицирана информация.

С приемането на ЗЗКИ на законодателно ниво е реализиран един от основните приоритети на Концепцията за национална сигурност на Република България, а именно със специален закон да се гарантира защитата на държавния информационен ресурс от изтичането на важна за страната политическа, икономическа, научно-техническа и друга информация. Основната цел на закона е защитата на класифицираната информация от нерегламентиран достъп, който би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика, защитата на конституционно установения ред или друг правно защитен интерес.

Мерките за защита на класифицираната информация, предвидени в нормативната уредба са групирани съобразно източниците на заплаха. По този начин се обособяват отделните видове сигурност на класифицираната информация, разбирани като съчетание на принципи, способи и средства за защита. Тези принципи трябва да осигурят защитата на важната за държавата информация от заплахите, създавани от различни фактори.

Легалното определение на понятието „**документална сигурност**“ се съдържа в чл. 80, ал.1 на Раздел II от ЗЗКИ. Според цитираната разпоредба документалната сигурност е система от мерки, способи и средства за защита на класифицираната информация при създаването, обработването и съхраняването на документи, както и при организирането и работата на регистратурите за класифицирана информация.

Конкретната уредба на мерките, способите и средствата за защита, формиращи системата на документалната сигурност са регламентирани в Раздел V от Правилника за прилагане на Закона за защита на класифицираната информация.

Документалната сигурност обхваща дейността по класифициране на информацията, условията и реда за маркиране и обозначаване на класифицирана информация, разкриване на регистратури за класифицирана информация и контрола върху тях, начините за регистриране и отчет на материалите, съдържащи класифицирана информация, копирането и правенето на извадки от документи, съдържащи класифицирана информация, както и

условията за изпращане, предаване, пренасяне и приемане на класифицирана информация. Преразглеждането, удължаването и унищожаването на документи, съдържащи класифицирана информация, са също част от документалната сигурност. Така установената система от мерки, способи и средства цели да защити класифицираната информация от разгласяване, злоупотреба, промяна, увреждане, унищожаване, както и всякакви други действия, водещи до нарушаване на защитата й или до загубване на такава.

2. Класифициране на информацията

Класифицирането на информацията е дейност, при която се установява дали конкретна информация представлява държавна или служебна тайна. Самата процедура е строго регламентирана в ЗЗКИ и ППЗЗКИ и предполага наличието на няколко кумулативни предпоставки (чл. 46 от ППЗЗКИ).

Държавна тайна е информацията, попадаща в списъка по Приложение №1 към чл.25 от ЗЗКИ (Списък на категориите информация, подлежаща на класификация като държавна тайна), нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

Освен попадането на дадена информация в гореуказания списък трябва да е налице заплаха или опасност от увреждане на интересите в съответна степен.

Поставянето в опасност на интересите, посочени по-горе и настъпването на евентуални вреди в областта на националната сигурност, отбраната, външната политика и защитата на конституционно установения ред, трябва да бъдат свързани с нерегламентирания достъп до информацията. Това означава, че разкриването на информацията и нерегламентираният достъп до нея биха рефлектирали върху сигурността на страната, поради което е необходимо ограничаването на достъпа до нея.

Също така трябва да са налице обществени интереси, подлежащи на защита чрез класифициране на информацията като държавна тайна. В този смисъл ограничаването на достъпа до конкретната информация трябва да защитава реални интереси на Република България, свързани с националната сигурност.

Така реалното съществуване на обществени интереси в посочените насоки оправдава ограничаването на правото на гражданите на достъп до информация.

За да се определи информацията като държавна тайна, посочените по-горе четири критерия трябва да бъдат приложени в тяхната съвкупност. Факт е, че само попадането на информацията в списъка по чл. 25 от ЗЗКИ е обективен

критерий. Останалите три са изцяло субективни, което дава основание да се направи извод, че намирането на точното ниво на класификация е сложен процес, вследствие на който се определя и цикъла на движение на документа или материала, съдържащ класифицирана информация.

Съгласно разпоредбите на чл. 26 от ЗЗКИ и чл. 21 от ППЗЗКИ информация, класифицирана като служебна тайна могат да създават и съхраняват само държавните органи, органите на местното самоуправление и търговските дружества с над 51 на сто държавно участие. Служебната тайна има за цел да защити държавните органи и органите на местното самоуправление от разкриване на специфичните методи, средства и планове за действие, нерегламентираният достъп до които ще доведе до невъзможност или ще затрудни осъществяването на тяхната дейност.

Информацията, подлежаща на класификация като служебна тайна се определя със закон. Въз основа на това ръководителят на организационната единица обявява със заповед списък на категориите информация, подлежащи на класификация като служебна тайна. При създаването на списъка ръководителят на организационната единица трябва да се позове на онези закони, които регламентират дейността на организационната единица и които посочват, че определена информация, свързана със специфичната сфера на дейност на организационната единица подлежи на класификация.

Предпоставки за класифицирането като служебна тайна

- информацията да е обявена като подлежаща на класификация като служебна тайна в специален закон;
- да е включена в обхвата на списъка на категориите информация, подлежащи на класификация като служебна тайна за сферата на дейност на организационната единица (чл. 21 от ППЗЗКИ);
- класифицирането да се извърши от лице, заемащо длъжност или изпълняващо задача, налагаща достъп до класифицирана информация – служебна тайна, която е включена в списъка по чл. 23 от ППЗЗКИ.

На основата на така изведените дефиниции за видовете класифицирана информация – държавна и служебна тайна, като обединяващ признак може да бъде изведено засягането или заплахата от увреждане на определен държавен интерес, вследствие на нерегламентиран достъп до съответната информация.

В зависимост от вредите, които биха настъпили, лицето, което има право да подписва документа, ще постави съответния гриф за сигурност, колкото са по-големи вредите, толкова ще е по-високо нивото на класификация. Лицето, създало документа или материала, съдържащ класифицирана информация, в случай, че е различно от лицето, което го подписва е длъжно да постави гриф за сигурност, валиден до окончателното му определяне.

Принципното положение, което важи при определянето дали дадена информация представлява държавна или служебна тайна е, че информацията се класифицира на база собственото си съдържание, а не според класификацията на информацията, за която се отнася или на която се базира. Във всеки конкретен случай трябва да се анализира собственото съдържание на информацията и само ако за него могат да се приложат предпоставките за класифициране на информацията, ограничаването на достъпа до тази информация е правомерно.

Правилното класифициране на информацията е един от най-трудните за решаване проблеми по защитата на класифицираната информация. Затрудненията възникват поради липсата в действащото законодателство на достатъчно обективни критерии за класифицирането й. Освен кумулативните условия на чл. 46 от ППЗЗКИ останалите констатации са оставени на субективната преценка на лицата, отговорни за класифицирането.

Правилното определяне на нивото на класификация е изключително важно, тъй като от тук се определя последващото движение на документите и материалите. При едно по-високо ниво на класификация се затруднява достъпът до информацията, която на база на собственото си съдържание не представлява държавна тайна. Неправилното поставяне и определяне на грифа за сигурност е нерегламентиран достъп съгласно § 1, т. 6 от Допълнителните разпоредби на ЗЗКИ.

В рамките на задължителното обучение по чл. 38, ал. 1, т. 2 от ЗЗКИ организационните единици подготвят служителите си как да определят дали дадена информация е класифицирана, какво да бъде нивото на класификация, както и условията и реда за неговата промяна или премахване.

Ръководителите на организационните единици определят вътрешни правила, при спазване на законовите изисквания за правилното определяне на нивото на класификация, както и за неговата промяна или премахване. Със степенуването на възможните вреди, които настъпват при нерегламентиран достъп се постига ограничаване на субективизма при определяне съответното ниво на сигурност (чл. 49 от ППЗЗКИ).

При установяване на случаи на неправилно класифициране на документи се уведомяват ръководителите на организационните единици или се инициират проверки от органа по прекия контрол.

Нивата на класификация за сигурност на информацията и техният гриф за сигурност, съгласно чл. 28 от ЗЗКИ са:

1. „Строго секретно”
2. „Секретно”

3. „Поверително”
4. „За служебно ползване”

Информация, класифицирана като държавна тайна се маркира с гриф за сигурност:

1. „Строго секретно“
2. „Секретно“
3. „Поверително“

Информацията, класифицирана като служебна тайна се маркира с гриф за сигурност:

1. „За служебно ползване“

Съгласно чл. 34 от ЗЗКИ сроковете на защита на класифицираната информация, считани от датата на създаването са следните:

- за информация, маркирана с гриф за сигурност „Строго секретно“ – 30 години;
- за информация, маркирана с гриф за сигурност „Секретно“– 15 години;
- за информация, маркирана с гриф за сигурност „Поверително“ – 5 години;
- за информация, маркирана с гриф за сигурност „За служебно ползване“ – 6 месеца.

Лицето, което създава документа може да посочи срок за защита на класифицираната информация, различен от посочените. В този случай лицето посочва датата на изтичане срока на защита на класифицираната информация в грифа за сигурност.

Съгласно чл. 50, ал. 1 от ППЗЗКИ ръководителят на организационната единица създава организация и определя ред за периодично преразглеждане на създадената в организационната единица класифицирана информация с цел промяна или премахване на нивата на класификация или удължаване на сроковете на защита.

Когато националните интереси налагат удължаване на сроковете на защита, същите могат да се удължат еднократно, но с не повече от първоначално определените. За целта е необходимо да се изпрати до ДКСИ писмено мотивирано искане от организационната единица, съгласно чл. 50, ал. 2 от ППЗЗКИ. Удължаването на сроковете се извършва с разрешение на ДКСИ, което е окончателно и не подлежи на обжалване.

Премахване нивото на класификация

Премахване нивото на класификация се извършва:

- след изтичането на съответния срок съгласно чл. 34 от ЗЗКИ;
- след изтичането на указания срок в грифа за сигурност;
- при отпадане на основанията за защита на класифицираната информация.

Една от по-сложните хипотези, при която се премахва нивото на класификация е при отпадане на основанието за защита на класифицираната информация. Доколкото законодателят говори за „отпадане на основанието на защита“, а не за „отпадане на правното основание за класифицирането“ отговор на въпроса кои са тези основания може да се даде като се започне от реда за класифициране на информацията.

Основният принцип при класифицирането на информацията е, че тя се класифицира според собственото си съдържание. Когато се създава документ, включващ класифицирани предложения, нивото на документа съответства поне на най-високото ниво на класификация на тези приложения.

Процедурата по класифициране изисква наличието на няколко кумулативни предпоставки.

Ако към момента на извършване на преценката дали дадена информация е класифицирана или не, някое от четирите условия, указани в чл. 46 от ППЗЗКИ не е налице, то на информацията не следва да се поставя гриф за сигурност.

В този смисъл отпадане на основанието за защита на класифицираната информация ще имаме винаги, когато едно от изискванията не е налице.

Промяна в нивото на класификация

Промяна в нивото на класификация се извършва:

- при промяна в основанията за определяне нивото на класификация за сигурност (чл. 50, ал. 6, т. 1 от ППЗЗКИ);
- при неправилно определяне нивото на класификация (чл. 50, ал. 6, т. 2 от ППЗЗКИ).

Възможно е информацията да е била неправилно класифицирана и маркирана с гриф за сигурност или да настъпят такива изменения във фактическата обстановка, които да променят основанията за определяне нивото на класификация на информацията. В тези два случая чл. 50, ал. 6 от ППЗЗКИ предвижда нивото на класификация да се промени в съответствие с

действителното положение. Неправилното определяне на нивото на класификация може да се установи по различни начини. Например при извършване на периодично преразглеждане на създадената в съответната организационна единица класифицирана информация или чрез уведомление от други лица. Важно е да се отбележи, че ЗЗКИ дава право на лицата да уведомяват автора на документа или неговия висшестоящ ръководител за неправилно определеното ниво на класификация (чл. 31, ал. 8 от ЗЗКИ).

Промяната на поставения гриф за сигурност се извършва чрез зачертаване с една хоризонтална черта на всеки елемент от грифа, с изключение на датата на създаване на документа по начин, позволяващ разчитането му, след което се поставя нов гриф за сигурност.

Новият гриф за сигурност се поставя непосредствено до стария, като се отбелязват: новото ниво на класификация; датата на промяната; новата дата на изтичане на срока за защита на класифицираната информация, когато той е различен от посочените в закона, правното основание за извършване на промяната; длъжността; името, фамилията и подписът на извършващия промяната.

Не се разрешава изтриване, заличаване, физическо премахване или замазване на гриф за сигурност, подлежащ на промяна.

При премахване на класификацията на информацията грифът за сигурност се заличава, като всеки елемент от грифа се зачертава с една хоризонтална черта по начин, позволяващ разчитането му, без да се поставя нов гриф за сигурност.

При премахването на класификацията се отбелязват датата, правното основание за премахването, длъжността, името, фамилията и подписът на извършващия премахването.

В случаите на премахване на класификацията поради изтичане на сроковете за защита на класифицираната информация грифът за сигурност се счита за заличен с изтичането на съответния срок и няма необходимост да се отбелязва върху документа (чл. 36, ал. 3 от ППЗЗКИ). Промяната на грифа за сигурност се отразява в съответния регистър.

Организационната единица незабавно уведомява ДКСИ и всички получатели при промяна или премахване нивото на класификация на информацията, съдържаща се в съответен материал или документ (чл. 50, ал. 8 от ППЗЗКИ).

Уведомлението до ДКСИ и получателите на даден класифициран документ се извършва в тримесечен срок и трябва да съдържа:

- наименование на организационната единица, в която е създаден документът;
- уникалния регистрационен номер на документа;
- правно основание за промяна нивото на класификация и новия гриф за сигурност, респ. правно основание за премахване на нивото;
- дата на извършване на промяната/премахването на нивото на класификация.

В случаите на липса на уведомление в указания срок се счита, че не е извършено удължаване на срока на защита, промяна или премахване на нивото на класификация.

Тук трябва да отбележим, че законодателят е дал възможност на автора на документа винаги, когато е възможно, да отбелязва върху материала разпореждания за премахване или промяна на нивото на класификация при изтичането на определен срок или при настъпване на определено събитие.

Във всички случаи получателите незабавно отбелязват промяната или премахването на грифа за сигурност върху материала и отразяват това обстоятелство в съответните регистри.

3. Маркиране на класифицираната информация и обозначения върху материалите, съдържащи класифицирана информация

Всяка класифицирана информация, представляваща **държавна** или **служебна** тайна, се маркира, като върху материала се поставя съответен гриф за сигурност.

Обстоятелството, че класифицираната информация е маркирана, означава, че:

- е създаден материал, съдържащ класифицирана информация, върху който е поставен гриф за сигурност;
- материалът и класифицираната информация са обект на съответни на нивото на класификация мерки за защита, определени в ЗЗКИ и в актовете по прилагането му;
- достъп до класифицирана информация се дава на друга организационна единица при спазване на принципа „необходимост да се знае";
- класифицираната информация и грифът за сигурност върху материала може да се изменят само със съгласието на лицето, което подписва документа или на неговия висшестоящ ръководител.

Грифът за сигурност се определя от лицето, което има право да подписва документа, съдържащ класифицирана информация. Ако лицето, създало

документа или материала е различно от лицето, което го подписва то е длъжно да постави гриф за сигурност, валиден до окончателното му определяне. Прието е този гриф за сигурност да се нарича „временен гриф за сигурност” и функционалното му предназначение е да защити информацията до окончателното подписване на документа.

Грифът за сигурност се поставя на видно място чрез напечатване, принтиране, написване, изобразяване, поставяне на етикети, стикери или по друг начин, трайно, ясно, четливо, разбираемо и без съкращения.

Грифът за сигурност се поставя отделно от всички останали обозначения върху материала по начин, който не го уврежда.

Върху материала на видно място се поставя уникален регистрационен номер чрез напечатване, принтиране, написване, изобразяване, поставяне на етикети, стикери или по друг начин, трайно, ясно, четливо, разбираемо и без съкращения.

Регистрационният номер се състои от:

- уникалния идентификационен номер на регистратурата;
- номенклатурен номер на регистър от Номенклатурния списък на регистрите;
- поредния номер на материала за текущата година по регистъра (приложение № 2, чл. 68, ал. 2 от ППЗЗКИ);
- датата на регистриране.

Уникалният регистрационен номер се изписва в следния формат: уникалният идентификационен номер на регистратурата/номенклатурният номер на регистъра (от Номенклатурния списък) – пореден номер на материала в регистъра/ДД.ММ.ГГГГ.

Уникалният регистрационен номер на документа или материала не се променя през времето на неговото съществуване.

Документ на хартиен носител, съдържащ класифицирана информация се оформя, като се поставят следните обозначения:

На първата страница

- в най-горната част, центрирано, се поставят наименованието и адресът на организационната единица, в която е създаден документът на хартиен носител;
- в горния ляв ъгъл непосредствено под наименованието и адреса на организационната единица се поставят уникалният регистрационен номер на документа, номенклатурният номер на регистъра и поредният номер на екземпляра от него; в случай, че документът е изготвен в един екземпляр, се записва: „Екземпляр единствен“;

- в случаите на размножаване на документа върху направеното копие под уникалния регистрационен номер се отбелязва поредният номер на копието;
- в горния десен ъгъл непосредствено под наименованието и адреса на организационната единица се поставя грифът за сигурност, който съдържа следните елементи:

– ниво на класификация;

– датата на класифициране;

– дата на изтичане на срока на класификация, когато е различна от посочените в закона;

– правното основание за класифициране.

– в долния десен ъгъл се поставят номерът на страницата и броят на страниците на целия документ, разделени със символа "/".

На втора и следващи страници

- в горния десен ъгъл се поставя нивото на класификация;
- в долния ляв ъгъл се поставя уникалният регистрационен номер на документа, номерът на екземпляра, в случай на размножаване върху направеното копие се поставя и поредният номер на копието;
- в долния десен ъгъл се поставят номерът на страницата и броят на страниците на целия документ, разделени със символа „/“.

На последната страница

- в горния десен ъгъл се поставя нивото на класификация;
- в долния ляв ъгъл се поставя уникалният регистрационен номер на документа;
- в долния десен ъгъл се поставят номерът на страницата и броят на страниците на целия документ, разделени със символа "/".

След края на основния текст

- опис на приложенията със следните данни: номер на приложението (заглавие); ниво на класификация; брой страници;
- длъжност, подпис, име и фамилно име на лицето, което подписва документа, дата на подписването на документа;
- броят на отпечатаните екземпляри и адресатът за всеки от тях;
- име и фамилно име на лицето, изготвило документа или личен кадрови номер за служителя (служители от службите за сигурност, службите за обществен ред и Бюрото по защита при главния прокурор), дата на изготвянето

на документа – само ако това лице е различно от лицето, което подписва документа;

- име и фамилно име на лицето, отпечатало документа или личен кадрови номер за служителя (служители от службите за сигурност, службите за обществен ред и Бюрото по защита при главния прокурор), дата на отпечатването на документа – само ако това лице е различно от лицето, което подписва документа;
- думата „Съгласувано“:, подпис, име и фамилно име на лицата, които съгласуват документа, дата на съгласуване на документа;
- брой на копията и адресатът за всяко от тях.

Приложенията към документа

На първата страница в горния десен ъгъл се изписва „Приложение № ... към документ № ...“; под този текст се изписва нивото на класификация.

На първата страница в долния десен ъгъл се изписват номерът на страницата и броят на страниците на приложението, разделени със символа „/“; приложението се номерира отделно от основния документ.

На втората и следващите страници се поставят обозначенията:

- в горния десен ъгъл се поставя нивото на класификация;
- в долния ляв ъгъл се поставя уникалният регистрационен номер на документа;
- в долния десен ъгъл се поставят номерът на страницата и броят на страниците на приложението, разделени със символа „/“.

Авторът може да впише върху документа следните разпореждания до адресатите:

1. „Даването на информация, съдържаща се в документа, без писменото съгласие на лицето, подписало документа, е забранено“;
2. „Размножаването без писменото съгласие на лицето, подписало документа, е забранено“;
3. „Преписването без писменото съгласие на лицето, подписало документа, е забранено“;
4. „Правенето на извадки без писменото съгласие на лицето, подписало документа, е забранено“.

Върху документа могат да се поставят и други разпореждания, отнасящи се до работата с него.

При необходимост по предложение на служителя по сигурността на информацията ръководителят на организационната единица може да разрешава поставянето и на допълнителни обозначения върху материалите, които се отнасят и са валидни само за организационната единица.

4. Регистратури за класифицирана информация

Ръководителят на организационната единица, в която се получава, създава, регистрира, обработва, съхранява, разпределя, предоставя и размножава класифицирана информация, създава регистратура за класифицирана информация като отделно организационно звено.

Щатното обособяване, структурата, числеността състав и мерките за защита на регистратурата се определят в зависимост от нивата на класификация и обема на класифицираната информация.

При необходимост в организационната единица могат да се създават и повече от една регистратури.

В структурата на регистратурата при необходимост могат да се включат и други звена, работещи с класифицирана информация, като машинописно, размножително, библиографско, стенографско, чертожно, редакторско, разпределително-куриерско и др.

При необходимост временно могат да се откриват контролни пунктове, които са поделения на съответната регистратура и осигуряват условия за създаване, получаване, регистриране, разпространяване, размножаване и охрана на класифицирана информация, получена от същата регистратура, а когато са упълномощени от ДКСИ – и от други регистратури.

Ръководителят на организационната единица, в която се съхранява и обменя чуждестранна класифицирана информация, организира под ръководството на ДКСИ регистратура в областта на международните отношения.

Дейността на регистратурите за чуждестранна класифицирана информация се организира в съответствие със сключения международен договор и правилата за защита на класифицираната информация на съответната международна организация или на държавата – източник на класифицираната информация.

В ДКСИ се създава централна регистратура в областта на международните отношения.

Регистратурите се оборудват така, че:

- да се гарантира защитата на класифицираната информация от нерегламентиран достъп;

- да не се позволи разкриването на вида и характера на извършваната в тях работа.

Регистратурите се откриват след проверка за изпълнение на изискванията за защита на класифицираната информация и получаване на уникален идентификационен номер от ДКСИ.

Проверката се извършва от комисия, назначена от ръководителя на организационната единица, която включва служителя по сигурността на информацията, представител на съответната организационна единица и представител на съответната служба за сигурност.

Комисията изготвя протокол в 3 екземпляра – по един за ДКСИ, за службата за сигурност и за регистратурата на организационната единица.

Незабавно след получаване на протокола ДКСИ изпраща на организационната единица уникален идентификационен номер на регистратурата.

В помещенията на регистратурите, които не са определени за работа със съответните потребители от организационната единица, могат да влизат само служителите от регистратурата, ръководителят на организационната единица, служителят по сигурността на информацията и лицата, определени със заповедта по чл. 12 от ЗЗКИ .

При необходимост служителят по сигурността на информацията издава писмено разрешение за достъп до посочените помещения на регистратурата и на лица извън посочените.

Класифицирана информация може да се ползва, обработва и съхранява в служебните помещения на потребителите от организационната единица само ако са в съответната зона за сигурност и са защитени с необходимите мерки за сигурност на информацията.

Работата с материали, съдържащи класифицирана информация, съхранявани в регистратурите, се извършва само в определеното работно време.

Изключение се допуска с писмено разрешение на служителя по сигурността на информацията.

Работата с материали, съдържащи класифицирана информация, извън съответните зони за сигурност в организационната единица се разрешава от служителя по сигурността на информацията, който определя и съответните мерки за сигурност при пренасянето, ползването и съхраняването им.

Дейността в регистратурата и служителите в нея се ръководят от завеждащ регистратурата, който е пряко подчинен на служителя по сигурността на информацията. В случаите, когато в регистратурата има само един щатен служител, ръководителят на организационната единица определя със заповед и

друг служител, който отговаря на условията за работа в регистратурата. Определеният със заповед служител се обучава относно мерките за сигурност в регистратурата, правата и задълженията на работещия в нея и изпълнява задълженията на служител в регистратурата в случаите на отсъствие на титуляря.

В регистратурата се назначават служители, които притежават разрешение за достъп до класифицирана информация с най-високото ниво на класификация на информацията, с която ще се работи в регистратурата. Преди да започнат работа, служителите в регистратурата задължително трябва да бъдат обучени за работа в нея.

5. Завеждащият регистратура и служителите в регистратурите:

– отговарят за наличността и за правилното отчитане, приемане, използване, разпределяне, раздаване, събиране и съхраняване на материали, съдържащи класифицирана информация;

– отговарят за отчетността и съхраняването на материалите, съдържащи класифицирана информация, намиращи се в машинописни, размножителни и чертожни бюра, печатници, фотолаборатории, хранилища и други;

– съхраняват списъците на служителите, допуснати до работа с материали, съдържащи класифицирана информация (приложение № 1 към чл. 62, ал.1, т. 3 от ППЗЗКИ);

– следят за сроковете за защита на класифицираната информация и докладват на служителя по сигурността на информацията за изтичането им;

– организират своевременното предаване в архива на материалите с премахнато ниво на класификация;

– предлагат на служителя по сигурността на информацията конкретни мерки за отстраняване на съществуващи слабости и нарушения и участват в организирането и провеждането на съвещания, профилактични и други мероприятия, отнасящи се до подобряването на работата за защита на класифицираната информация.

При установяване нарушения на съответните мерки за физическа сигурност на помещенията на регистратурата служителите в регистратурата незабавно уведомяват служителя по сигурността на информацията и звеното за охрана на организационната единица, като вземат мерки за запазване на фактическата обстановка.

При наличие на опит за нерегламентиран достъп до класифицирана информация или при осъществен такъв достъп ръководителят на организационната единица уведомява компетентната служба за сигурност и ДКСИ.

Съгласно § 1, т. 6 от Допълнителните разпоредби на ЗЗКИ „Нерегламентиран достъп до класифицирана информация“ е разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата и/или до загубване на такава информация. За нерегламентиран достъп се счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това.

Организационната единица извършва оценка на нанесените вреди и предприема действия за ограничаването им. При наличие на данни за извършено престъпление от общ характер се уведомява съответната прокуратура.

Когато окончателният доклад от проверката на компетентната служба за сигурност показва, че материал, съдържащ класифицирана информация, е безвъзвратно изгубен, ДКСИ го сваля от отчет. Безвъзвратно изгубеният материал се счита за унищожен по смисъла на чл. 33 от ЗЗКИ.

Завеждащият регистратурата има следните допълнителни задължения:

- периодично проверява наличността и начина на съхраняване на материалите, съдържащи класифицирана информация, които се намират при служителите от организационната единица; при установяване на слабости и нарушения докладва писмено на служителя по сигурността на информацията и на ръководителя на организационната единица;
- незабавно докладва на служителя по сигурността на информацията за случаите на нерегламентиран достъп до материали, съдържащи класифицирана информация, и взема мерки за недопускане или ограничаване на вредните последици; за случаите на нерегламентиран достъп до материали с ниво на класификация "поверително" и по-високо чрез служителя по сигурността на информацията уведомява съответната служба за сигурност;
- взема мерки за връщане в регистратурата на материали, съдържащи класифицирана информация, които не са върнати до края на работното време, освен в случаите когато има писмено разрешение от служителя по сигурността на информацията.

6. Регистриране и отчет

За регистриране и отчет на материалите, съдържащи класифицирана информация, в регистратурите се водят отчетни документи.

Всеки окончателно изготвен материал, съдържащ класифицирана информация, представляваща държавна или служебна тайна, се регистрира с уникален регистрационен номер в съответната регистратура в регистър (приложение № 2, чл. 68, ал. 1 от ППЗЗКИ).

В регистратурите се водят следните **основни отчетни документи:**

- регистри за регистриране на материалите, съдържащи класифицирана информация (приложение № 2);
- регистри за регистриране на отчетните документи и/или сборовете от документи (приложение № 3, чл. 70, т.2 от ППЗЗКИ);
- номенклатурен списък на видовете регистри по т. 1 и 2;
- тетрадки за отразяване движението на материалите в рамките на организационната единица (приложение № 4, чл. 70, т. 4 от ППЗЗКИ);
- контролни листове за отразяване на запознаването с документите (приложение № 5, чл. 70, т. 5 от ППЗЗКИ);
- картон-заместители (приложение № 6, чл. 70, т.6 от ППЗЗКИ) за работа със сборове от документи или с отделни документи от тях в рамките на организационната единица;
- описи за предаване и получаване на материали, съдържащи класифицирана информация (приложение № 7, чл. 70, т. 7 от ППЗЗКИ);
- получаването от куриери на документи и материали, съдържащи класифицирана информация се осъществява с раздавателни описи (приложение № 8, чл. 70, т. 8 от ППЗЗКИ);
- експедиционни писма (чл. 70, т. 9 от ППЗЗКИ) за изпращане на материали, съдържащи класифицирана информация, представляваща държавна тайна.

За подобряване на отчета и защитата на материалите, съдържащи класифицирана информация, по решение на служителя по сигурността на информацията в организационната единица могат:

- да се допълват основните отчетни документи с данни и обозначения, които не са посочени в образците;
- да се водят и други отчетни документи освен задължителните.

Отчетните документи на хартиени носители трябва да са надлежно скрепени, с поредно номерирани листа и заверени с подписа на служителя по сигурността на информацията.

Отчетните документи на хартиени носители се водят със син химикал (мастило), точно, ясно и четливо, на български език, освен в случаите, предвидени в правилника.

При промяна на грифа за сигурност новите данни се нанасят под старите, като старите се зачертават с две хоризонтални черти по начин, позволяващ прочитането на зачертаната информация.

При допуснати грешки всички поправки се правят от завеждащия регистратурата с червен химикал (мастило) и се заверяват с неговия подпис.

Данните, нанесени в отчетните документи, не се изтриват, а се зачертават с две хоризонтални черти по начин, позволяващ прочитането на зачертаната информация.

В организационната единица в зависимост от конкретната необходимост могат да се водят различни **видове регистри** (приложение № 2), както следва:

- за всички материали, съдържащи класифицирана информация;
- за входящи материали, съдържащи класифицирана информация;
- за изходящи материали, съдържащи класифицирана информация;
- за материални носители за многократен запис на класифицирана информация;
- за предмети, представляващи държавна или служебна тайна.

Материали, съдържащи класифицирана информация с ниво на класификация **„Строго секретно”,** се регистрират в отделни регистри (приложение № 2).

Предназначението на отделните регистри (приложение № 2) се определя от служителя по сигурността на информацията.

В края на всяка календарна година регистрите (приложение № 2) се приключват чрез изцяло подчертаване на последния регистриран материал и по този начин се приключва даването на нови поредни номера за съответната година. Под чертата се описва броят на използваните регистрационни номера и се полагат подписите на служителя от регистратурата, водещ съответния регистър, и на завеждащия регистратурата.

В регистрите (приложение № 3) се регистрират задължително всички томове (части) на регистрите (приложение № 2), на сборовете от документи и тетрадките (приложение № 4), които се водят в регистратурата.

Служителят по сигурността на информацията определя кои от останалите отчетни документи да се завеждат в регистър (приложение № 3) и предназначението на отделните регистри (приложение № 3).

Регистрите (приложение № 3) не се приключват и номерата продължават непрекъснато.

Номенклатурният списък на регистрите приложения № 2 и 3 и на сборовете от документи се подписва от служителя по сигурността на информацията в организационната единица и съдържа таблица със следните графи:

- номенклатурен номер на регистъра;
- тема (предназначение) на регистъра (например: за входящи документи; за електронни носители; за сборове от документи; за отчетни документи и т. н.);
- ниво на класификация на регистъра, ако има такова.

Документи, съдържащи класифицирана информация, по които работата е приключена могат да се събират по определена тема в сбор от документи.

Към всеки сбор от документи се изготвя и поставя **опис**, който съдържа:

- уникалния идентификационен номер на регистратурата;
- номенклатурния номер на сбора от документи;
- номера на тома на сбора от документи;

Таблицата е със следните графи:

– номер по ред;

– уникален регистрационен номер на документа;

– наименование и кратко описание на съдържанието на документа;

– брой листове на документа.

- подпис, собствено и фамилно име на завеждащия регистратурата.

Към всеки сбор от документи може да се поставя списък на служителите, имащи право да получават и да работят със сбора от документи и нивото на класифицирана информация, до която те имат разрешение за достъп. Документите се подреждат в сборовете от документи по реда на изготвянето им. От изготвените в организационната единица документи се поставят първите екземпляри.

Към всеки сбор от документи се прикрепя картон-заместител (приложение № 6) за работа със сборове от документи или с отделни документи от тях в рамките на организационната единица.

Ползването на сборовете от документи или на отделни документи от тях се извършва срещу подпис в картона-заместител.

Контролният лист (приложение № 5) съпровожда материала до предаването му в архив или унищожаването му.

Контролният лист е отделен документ, който се унищожава с предаването в архив или с унищожаването на материала, съдържащ класифицирана информация, представляваща държавна или служебна тайна, във връзка с който той е издаден.

Тетрадката (приложение № 4) е предназначена за ползване в регистратурите и за ползване от служителите в организационната единица. Когато се използва от служител, в нея се водят:

- материалите, предоставени на служителя или получени от него;
- материалите, съхранявани от служителя.

Конкретното предназначение на тетрадките по ал. 1, които се водят в регистратурата, се определя от служителя по сигурността.

В регистратурата могат да се водят отделни тетрадки (приложение № 4) за отразяване движението на документите по нива на класификация – за носителите за многократен запис, за предмети, представляващи държавна или служебна тайна, и др.

Отчетните документи по този раздел се водят винаги, когато е налице техническа възможност, в електронен вид в комуникационна и информационна система (КИС), която е акредитирана по реда на чл. 91 от ЗЗКИ или е елемент от такава акредитирана КИС.

Комуникационната и информационна система трябва да отговаря на следните условия:

- да е сертифицирана или да е елемент от сертифицирана КИС;
- да осигурява поддържане и отпечатване на данните, указани в образците отчетни документи;
- да осигурява изход на данни във формат, установен от ДКСИ, за автоматизирано водене на регистъра по чл. 35 от ЗЗКИ.

След приключването на календарната година регистрите, водени в електронен вид, се разпечатват на хартиен носител и се оформят по указания начин. Разпечатване на тези регистри може да се извършва и след писмено разрешение от служителя по сигурността на информацията. При разпечатване на регистрите се допуска разделяне на различните типове данни.

7. Условия и ред за изпращане, предаване, пренасяне и приемане на класифицирана информация.

Документите, съдържащи класифицирана информация, които се изпращат на други организационни единици получатели, се изготвят най-малко в два екземпляра.

Първият екземпляр, наречен оригинал, се съхранява в регистратурата на организационната единица, в която е създаден документът, а останалите екземпляри се изпращат на адресатите.

Всички документи, изпращани до други организационни единици, се подпечатват с печат на организационната единица.

Пренасянето на материали, съдържащи класифицирана информация се извършва чрез:

- дирекция „Специална куриерска служба” при ДКСИ;
- куриер от организационната единица;
- комуникационни и информационни системи;

- по пощата;
- военна пощенска свръзка при обявено военно положение или положение на война.

Материали, съдържащи класифицирана информация с ниво на класификация **„Строго секретно“,** се пренасят само чрез дирекция „Специална куриерска служба” при ДКСИ, с изключение на Въоръжените сили, Министерството на вътрешните работи, Държавна агенция „Разузнаване” и Националната служба за охрана, които могат да пренасят тези материали и със свои куриери.

Материали, съдържащи класифицирана информация с ниво на класификация **„Секретно“** или **„Поверително“,** се пренасят чрез дирекция „Специална куриерска служба“ при ДКСИ, чрез куриер от организационната единица или чрез КИС.

Материали, съдържащи класифицирана информация с ниво на класификация **„За служебно ползване“**, могат да се изпращат по всички изброени начини.

Изпращането на материалите по пощата се извършва само препоръчано с обратна разписка, която се съхранява една година в регистратурата, която е изпратила материала.

Чуждестранна класифицирана информация се пренася чрез:
- дирекция „Специална куриерска служба“ при ДКСИ;
- куриер от организационната единица;
- КИС;
- ред, регламентиран в международен договор, по който Република България е страна.

Образци за оформяне на пликове

Материалите, съдържащи класифицирана информация, представляваща държавна тайна, които се пренасят по куриер, се опаковат в пакети.

Пакетите представляват две здрави, непрозрачни, поставени една в друга опаковки или пликове, надеждно запечатани и облепени по начин, непозволяващ изваждане на материалите от опаковките, без да се повредят съдържанието или печатите на тези опаковки.

Материалите се поставят във вътрешната опаковка, а експедиционното писмо - между двете опаковки на пакета.

Върху **външната опаковка на пакета** се изписват без съкращения:
- в горната лява част - подателят и неговият точен адрес;

- в долната дясна част - получателят и неговият точен адрес;
- в горната дясна част - номерът на експедиционното писмо, който се счита за номер на пакета.

При пренасянето чрез куриер на външната опаковка се изписва „Само чрез куриер“.

Върху **вътрешната опаковка** се изписват без съкращения:

- в горната лява част - подателят;
- в долната дясна част - получателят;
- в горната и долната част – подходящо ниво на класификация, но не по-ниско от най-високото ниво на документите, които се съдържат в пакета.

При необходимост върху вътрешната опаковка се изписва „Да се отвори от ...“, като се посочват името и длъжността на лицето, до което е адресиран материалът.

Пакетите с материали, съдържащи класифицирана информация, се приемат от определен служител от регистратурата на организационната единица.

В извънработно време, по изключение, пакетите се приемат от дежурния на организационната единица и се завеждат на отчет в книга по образец, утвърден от служителя по сигурността. Пакетите се съхраняват в отговарящо на изискванията за физическа сигурност място (помещение, шкаф, сейф) и се предават незабавно, без да се разпечатват, при започване на работното време на служителя от регистратурата срещу подпис.

При приемането на пакетите служителят от регистратурата проверява съответствието на номерата на пакетите (пликовете) с посочените в описа, адреса, целостта на печатите и опаковката, след което заверява с подпис екземпляра от описа за приносителя, като написва четливо фамилното си име, датата и часа на получаването и поставя печат на организационната единица.

При констатирани неизправности или несъответствия в оформянето на външните опаковки или съпровождащите ги описи те се отстраняват на място или пакетите не се приемат. Неприетите пакети се зачертават в описа по начин, позволяващ прочитане на зачертаното, след което описът се заверява с подписа на куриера, с печат и дата.

Получени пакети с надпис „Да се отвори от ...“ не се отварят от лице, различно от посоченото в надписа. Служителят от регистратурата ги завежда неотворени в регистър (приложение № 2) и ги предава по най-бързия начин на получателя.

При липса на указания служителят от регистратурата е длъжен да отвори всеки пакет, да сравни номерата на материалите с номерата от

експедиционното писмо и да провери броя на листовете на документите и приложенията.

При констатирани неизправности и/или несъответствия незабавно се уведомява служителят по сигурността на информацията и се изготвя протокол. Копие от протокола се изпраща на подателя.

Ако след отварянето на пакета се установи, че материалът е бил предназначен за друг получател, погрешният получател незабавно го връща обратно на подателя. Върху новата опаковка на материала се изписва „Пристигнало погрешка“ и се добавят наименованието и адресът на организационната единица, която е получила погрешка материала, датата и подписът на служителя от регистратурата.

Всички получени в регистратурата материали, съдържащи класифицирана информация, незабавно се завеждат на отчет в регистъра (приложение № 2).

Материали, съдържащи класифицирана информация, не се докладват и предават за изпълнение, преди да са заведени на отчет.

При необходимост към документите се прикрепват контролни листове (приложение № 5).

Експедиционни писма

За изпращане на материали, съдържащи класифицирана информация, представляваща държавна тайна, до определен получател се изготвя експедиционно писмо в два екземпляра: първият остава на съхранение в регистратурата, а вторият се изпраща на получателя.

Експедиционното писмо съдържа:

- наименованието на получателя;
- уникалните регистрационни номера на материалите;
- нивото на класификация на всеки от материалите;
- броя страници на всеки от документите; в случай, че документът има приложения, записват се общият брой страници, включително на приложенията, броят на приложенията и общият брой страници на приложенията във формат "общ брой страници, включително приложенията + брой на приложенията/общ брой страници на приложенията".

Експедиционното писмо получава регистрационен номер от регистратурата от Регистъра за експедиционни писма към чл. 94, ал. 3 от ППЗЗКИ. Регистрационният номер съдържа номенклатурен номер на регистъра за експедиционни писма и пореден номер от този регистър.

Експедиционното писмо се поставя между външната и вътрешната опаковка на пакета, съдържащ класифицирана информация.

8. Размножаване на документи, съдържащи класифицирана информация, се извършва:

1. ако няма изрично разпореждане, забраняващо размножаването на документа;

2. след разпореждане за размножаване, дадено от ръководителя на организационната единица или от лице, определено с негова заповед;

3. документите с ниво на класификация „Строго секретно“ се размножават само след предварително писмено разрешение на лицето по чл. 31, ал. 1 от ЗЗКИ или на организационната единица, от която произхожда документът, което се прилага към него;

4. за документи с ниво на класификация „За служебно ползване“ - след разрешение на прекия ръководител на лицето, извършващо размножаването.

Документи, съдържащи класифицирана информация, се размножават в помещения, които се намират в съответни на нивото на класификация зони за сигурност и при съответни мерки за защита на информацията.

Служителите, които могат да размножават документи, съдържащи класифицирана информация, трябва да имат разрешение за достъп до съответното ниво на класифицирана информация.

Върху документа, съдържащ класифицирана информация, от който се правят копия, се отбелязват:

- датата на изготвянето им;
- броят на копията;
- причината за размножаването;
- името на лицето, дало разрешение за размножаване;
- и името и подписът на лицето, което е направило копията.

На първа страница на всяко копие горе вляво се поставя пореден номер на копието.

На втора и следваща страница в долния ляв ъгъл се поставя и поредния номера на копието.

В съответния регистрационен дневник (приложение № 2) в графа „Забележка“ срещу регистрационния номер на документа, от който се правят копията, се записват **датата и броят на направените копия.**

Извадки от документи

Правенето на извадки от документи, съдържащи класифицирана информация, се извършва:

- ако няма изрично разпореждане, забраняващо преписването или правенето на извадки от документа, **и**
- само в заведени в регистратурата работни тетрадки или бележници със съответното ниво на класификация, **или**
- чрез създаване на нов документ, който се маркира и регистрира по установения ред.

При създаването на нов документ, съдържащ извадки от други документи, новосъздаденият документ получава ниво на класификация, съответстващо на най-високото ниво на класификация измежду документите, от които са направени извадките.

Служителите, получили разрешения за достъп до класифицирана информация

Отговарят за тяхната наличност, като в края на работата с тях лично ги предават в регистратурата срещу подпис.

При загубване на материали, съдържащи класифицирана информация, незабавно уведомяват завеждащия регистратурата и служителя по сигурността на информацията.

Нямат право да разгласяват и да изнасят класифицирана информация извън организационната единица в нарушение на законоустановения ред.

Нямат право да записват класифицирана информация на нерегистрирани предварително на отчет магнитни носители;

Нямат право да използват материали, съдържащи класифицирана информация, за явни публикации, дипломни работи, дисертации, доклади и др.

Нямат право да размножават и унищожават материали, съдържащи класифицирана информация, в нарушение на установения за това ред.

Предаването и получаването на класифицирани материали от служителите получили разрешение за достъп до класифицирана информация се извършва лично срещу подпис в тетрадка (приложение № 4), водена в регистратурата или в картон-заместител. Запознаването и работата с материали, съдържащи класифицирана информация, се извършва в регистратурата или в работните помещения на служителите, ако се намират в съответните зони за сигурност.

Служителят, получил материал, съдържащ класифицирана информация, или който изготвя такъв материал, го **отбелязва в личната си тетрадка**

(приложение № 4). Отбелязването се извършва веднага след приемането на материала или след даването на регистрационен номер за новосъздаден материал, съдържащ класифицирана информация.

Служителят, който само се запознава с материал, съдържащ класифицирана информация, без да го получава за работа, не прави **отбелязване в личната си тетрадка** (приложение № 4), а само се подписва в контролния лист (приложение № 5).

След приключване на работата с документа служителят написва на първа страница номенклатурния номер на сбора от документи, към който да бъде приложен, и се подписва.

При служебна необходимост срещу подпис в личната тетрадка (приложение № 4) служителят може да дава за временно ползване материали, съдържащи класифицирана информация, на други служители от същата организационна единица, които имат съответното разрешение за достъп до класифицирана информация.

Бележки или записки, съдържащи класифицирана информация, се записват:

- в работни тетрадки или бележници, които са надлежно подвързани, с поредно номерирани листове и заведени на отчет в регистратурата;
- на носители, използвани в сертифицирана КИС и заведени на отчет в регистратурата.

9. Контрол върху регистратурите

Ръководителят на организационната единица, служителят по сигурността на информацията и лицата, определени по реда на чл. 12 от ЗЗКИ (Държавна агенция „Национална сигурност“), осъществяват контрол върху цялостната дейност и състоянието на регистратурата.

Видове контрол - текущ и периодичен

Текущият контрол се организира от ръководителя на организационната единица и от служителя по сигурността на информацията и включва планови и извънпланови, годишни, частични и цялостни проверки.

Периодичният контрол е пряк контрол и се осъществява от лицата по чл. 12 ЗЗКИ (ДАНС).

Годишни и ежемесечни вътрешни проверки

Ежемесечни вътрешни проверки се извършват от завеждащия регистратурата за класифицирана информация, при които се проверяват:

- наличността на изработените и получените материали, съдържащи класифицирана информация;
- наличността на материалите, съдържащи класифицирана информация, намиращи се в служителите;
- воденето на отчетните документи;
- състоянието на регистратурата.

Завеждащият регистратурата за класифицирана информация изготвя протокол за резултатите от проверката, който се предоставя на служителя по сигурността на информацията.

Ръководителят на организационната единица със заповед ежегодно назначава комисия за извършване на годишна проверка на регистратурата.

Годишната проверка на регистратурата се извършва чрез сверяване по отчетните документи за фактическите наличности на материалите, а също и с актовете за унищожаване на материали за текущата година и с описите за получаване и изпращане на материали.

За резултатите от годишната проверка на регистратурата комисията изготвя протокол, който се предоставя на служителя по сигурността на информацията и на Държавна агенция „Национална сигурност“.

Цялостна проверка на регистратурата задължително се извършва при смяна на завеждащия регистратурата или при констатиране на нерегламентиран достъп до документ и/или материал, носител на класифицирана информация, заведен в същата регистратура.

При смяна на завеждащия регистратурата всички материали, съдържащи класифицирана информация, се предават/приемат с комисия, назначена със заповед на ръководителя на организационната единица.

Комисията, предаващият и приемащият проверяват наличността на всички материали, съдържащи класифицирана информация.

Комисията изготвя протокол за предаване и приемане, в който се отразяват наличността на материалите, състоянието на регистратурата и констатираните нарушения, ако има такива.

Предаването и приемането се счита за завършено след утвърждаване на протокола от ръководителя на организационната единица.

ПРЕРАЗГЛЕЖДАНЕ НА ДОКУМЕНТИ И МАТЕРИАЛИ, СЪДЪРЖАЩИ КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

1. Преразглеждането на документи и материали, съдържащи класифицирана информация – същност и особености

Преразглеждането на документи и материали, съдържащи класифицирана информация е оценъчна дейност, при която се извършва едно от следните действия – промяна или премахване на нивата на класификация или удължаване на сроковете за защита със запазване на нивата на класификация.

Правната уредба, прилагана при преразглеждането на документи и материали, е уредена в Закона за защита на класифицираната информация (ЗЗКИ), Правилника за прилагане на ЗЗКИ (ППЗЗКИ) и в „Задължителните указания на ДКСИ относно привеждане на заварени правоотношения в съответствие със ЗЗКИ и подзаконовите нормативни актове по прилагането му“.

Съществуват два основни режима – за документи и материали, създадени преди влизане в сила на ЗЗКИ и за документи и материали, създадени съгласно сега действащата нормативна уредба.

Преди влизането в сила на ЗЗКИ, класифицираната информация е маркирана със степени на секретност. Привеждането от степен на секретност към ниво на класификация на документи, носители на класифицирана информация, създадени преди влизане в сила на ЗЗКИ е уредена с разпоредбите на § 9 от Преходните и заключителни разпоредби (ПЗР) на ЗЗКИ. В допълнение са изготвените „Задължителни указания на ДКСИ относно привеждане на заварени правоотношения в съответствие със ЗЗКИ и подзаконовите нормативни актове по прилагането му“.

Разпоредбите на § 9 от ПЗР на ЗЗКИ установяват различен режим за преразглеждането в зависимост от това, кой е автор на съхраняваните в организационната единица документи и степента на секретност с която те са маркирани. На всички съхранявани в организационната единица документи се извършва привеждане на степените на секретност с нива на класификация.

Преразглеждане на документи по ал. 1 на § 9 от Преходните и заключителните разпоредби на ЗЗКИ

Спрямо всички съхранявани в организационната единица документи се извършва автоматично приравняване на степените за секретност с нивата на класификация, като сроковете на защита, императивно установени в чл. 34, ал. 1 от ЗЗКИ, се броят от датата на създаване на документите. Горецитираната законова разпоредба се прилага към всички съхранявани в организационната единица документи, маркирани със степени на секретност „Секретно“, „Строго секретно“ и „Строго секретно от особена важност“. След приравняването на степените на секретност, нивата на класификация са съответно „Поверително“, „Секретно“ и „Строго секретно“. Извършеното приравняване се отбелязва както върху самите документи, така и в отчетните документи съгласно изискванията на Глава V от ППЗЗКИ. Процедурата приключва с протокол, като екземпляр от него се изпраща за сведение в ДКСИ. В случай, че сроковете на защита на преразглежданите документи, създадени преди влизането в сила на ЗЗКИ са изтекли, същите се считат с премахнати нива на класификация.

При условие, че в организационната единица получател постъпи уведомление от автора на даден класифициран документ за извършена промяна или премахване нивото на класификация, за получателя възниква задължение съгласно чл. 50, ал. 9 от ППЗЗКИ незабавно да отбележи това върху документа, както и в съответния регистър. В тази хипотеза е възможно входящи за организационната единица документи, които са запазили статута си на класифицирана информация след автоматичното приравняване да бъдат с премахнато ниво на класификация, тъй като такава е преценката на техния автор.

Възможно е някои от документите да имат ниво на класификация, което не е указано в ал. 1 на § 9, като напр. „Лично строго поверително”, „Строго поверително” или „Поверително от особена важност”. В тези случаи директно се преминава към прилагане на хипотезата за преразглеждане на съдържанието на документа по същество.

Преразглеждане на собствена информация

Документите, които представляват собствена информация, подлежат на преразглеждане по същество. Това означава, че в зависимост от съдържанието им, а не единствено въз основа на формални критерии – каквито са срокът на защита и обозначената степен на секретност, ще се прецени дали съдържанието им представлява класифицирана информация по действащата правна уредба. Съвкупната преценка за това се извършва след проверка за съответствие на

четирите кумулативно свързани условия за класифициране посочени в чл. 46 от ППЗЗКИ:

- попада ли конкретната информация в списъка на категориите информация, определяни като държавна или служебна тайна (Приложение № 1 към чл. 25 ЗЗКИ или списъка по чл. 26, ал. 3 от ЗЗКИ);
- налице ли са обществените интереси, подлежащи на защита.
- налице ли е заплаха или опасност от увреждане на информацията или интересите на страната, както и каква ще бъде степента на нанесените вреди (§ 1, т. 15 от допълнителните разпоредби на ЗЗКИ);
- дали нерегламентираният достъп до информацията би създал опасност за сигурността и интересите на страната.

За всички документи, които са били обект на преразглеждане и за които е направен изводът, че същите представляват класифицирана информация, следва да се определи конкретното правно основание за класифициране. Основният принцип при класифицирането на информацията е, че тя се класифицира според собственото си съдържание. Процедурата по класифициране изисква наличието на представените кумулативни предпоставки. Към момента на извършване на преценката трябва да се установи, че са налице и четирите условия, указани в чл. 46 от ППЗЗКИ, като се постави съответният гриф за сигурност.

В този случай, правното основание за класификация на информацията като държавна тайна се състои в указването на раздел и конкретна точка от Приложение № 1 към чл. 25 от ЗЗКИ, а за информацията, класифицирана като служебна тайна – изписването на точка от списъка за всяка организационна единица, изготвен при спазването на разпоредбите на конкретния за нея специален закон (списъка по чл. 26, ал. 3 от ЗЗКИ).

Едно от основните задължения на ръководителя на организационната единица е минимум на две години да създаде организация и да определи реда за периодично преразглеждане на създадената в организационната единица класифицирана информация с цел промяна или премахване на нивата на класификация или удължаване на сроковете за защита със запазване на нивата на класификация.

Процедурата включва следните дейности:

Ръководителят на организационната единица със своя заповед създава организация и определя ред за преразглеждане на създадените в организационната единица документи и материали, носители на класифицирана информация. Преразглеждането се извършва от лица, притежаващи разрешения

за достъп, съответстващо на нивото на информацията. Извършва се фактическото действие по преразглеждането, след което се съставя протокол в три екземпляра – първият за организационната единица, а с изпращането на втория и третия се уведомява ДКСИ и адресатът, ако има такъв (чл. 50, ал. 8 от ППЗЗКИ, във връзка с чл. 35, ал. 3 от ЗЗКИ).

При документи, за които се констатира, че срокът на защита е изтекъл, процедурата приключва със списък, който се изпраща само до ДКСИ.

Когато националните интереси налагат удължаване на сроковете на защита, същите могат да се удължат еднократно, но с не повече от първоначално определените. За целта е необходимо да се изпрати до ДКСИ писмено мотивирано искане от организационната единица. Удължаването на сроковете се извършва с разрешение на ДКСИ, което е окончателно и не подлежи на обжалване. Искането за удължаване на сроковете на защита трябва да се подаде най-малко три месеца преди да е изтекъл срокът на защита за конкретните документи (чл. 50, ал. 2, ал. 3 и ал. 4 от ППЗЗКИ).

Нивото на класификация се премахва (чл. 50, ал. 5 от ППЗЗКИ):

- след изтичането на съответния срок съгласно чл. 34 от ЗЗКИ;
- след изтичането на указания срок в грифа за сигурност (поставен от автора при изготвяне на документа);
- при отпадане на основанията за защита на класифицираната информация.

При документи, попадащи в хипотезата на първите две от гореописаните условия, процедурата по преразглеждане с цел премахване нивото на класификация приключва със списък, който се изпраща само до ДКСИ. Грифът за сигурност на тези документи се счита за заличен и няма необходимост това да се отбелязва върху тях (чл. 36, ал. 3 от ППЗЗКИ). Промяната на грифа за сигурност се отразява в съответния регистър.

Една от по-сложните хипотези, при която се премахва нивото на класификация е при „отпадане на основанието за защита на класифицираната информация”. Доколкото законодателят говори за „отпадане на основанието за защита”, а не за „отпадане на правното основание за класифицирането”, отговор на въпроса кои са тези основания може да се даде като се започне от реда за класифициране на информацията.

Основният принцип при класифицирането на информацията е, че тя се класифицира според собственото си съдържание.

Процедурата по класифициране изисква наличието на няколко кумулативни предпоставки съгласно чл. 46 от ППЗЗКИ.

Ако към момента на извършване на преценката дали дадена информация е класифицирана или не, и не е налице някое от четирите условия, указани в чл. 46 от ППЗЗКИ, то на информацията не следва да се поставя гриф за сигурност. В този смисъл отпадане на основанието за защита на класифицираната информация ще има винаги, когато едно от изискванията на чл. 46 не е изпълнено.

Правното основание за класификация на информацията като държавна тайна се състои в указването на раздел и конкретна точка от Приложение № 1 към чл. 25 от ЗЗКИ, а за информацията, класифицирана като служебна тайна изписването на конкретната разпоредба на специален закон.

В този контекст промяна на „правното основание за класифицирането" на информацията може да имаме в случай на законодателно изменение на специалния закон или текстовете на Приложение № 1, с което кръгът на категориите информация, подлежащи на класификация като служебна или държавна тайна се стеснява.

Нивото на класификация се променя (чл. 50, ал. 6 от ППЗЗКИ):

- при промяна в основанията за определяне нивото на класификация за сигурност;
- при неправилно определяне нивото на класификация.

Възможно е информацията да е била неправилно класифицирана и маркирана с гриф за сигурност или да настъпят такива изменения във фактическата обстановка, които да променят основанията за определяне на нивото на сигурност на информацията. В тези два случая чл. 50, ал. 6 от ППЗЗКИ предвижда нивото на класификация да се промени в съответствие с действителното положение. Неправилното определяне на нивото на класификация може да се установи по различни начини. Например при извършване на периодично преразглеждане на създадената в съответната организационна единица класифицирана информация или чрез уведомление от други лица. Важно е да се отбележи, че ЗЗКИ дава право на лицата да уведомяват автора на документа или неговия висшестоящ ръководител за неправилно определеното ниво на класификация (чл. 31, ал. 8 от ЗЗКИ).

Промяната на поставения гриф за сигурност се извършва чрез зачертаване с една хоризонтална черта на всеки елемент от грифа, с изключение на датата

на създаване, по начин, позволяващ разчитането му, след което се поставя нов гриф за сигурност.

Новият гриф за сигурност се поставя непосредствено до стария, като се отбелязват: новото ниво на класификация; датата на промяната; новата дата на изтичане на срока за защита на класифицираната информация, когато той е различен от посочените в закона; правното основание за извършване на промяната; длъжността, името, фамилията и подписът на извършващия промяната.

Не се разрешава изтриване, заличаване, физическо премахване или замазване на гриф за сигурност, подлежащ на промяна.

При премахване на класификацията на информацията грифът за сигурност се заличава, като всеки елемент от грифа се зачертава с една хоризонтална, с изключение на датата на създаване, по начин, позволяващ разчитането му, без да се поставя нов гриф за сигурност.

При премахването на класификацията се отбелязват датата, правното основание за премахване, длъжността, името, фамилията и подписът на извършващия премахването.

Промяната на грифа за сигурност се отразява в съответния регистър по чл. 68, ал. 1 от ППЗЗКИ.

Лицето, установило неправилното определяне на нивото на класификация, уведомява автора на документа или неговия вишестоящ ръководител.

Организационната единица незабавно уведомява ДКСИ и всички получатели при промяна или премахване нивото на класификация на информацията, съдържаща се в съответен материал или документ. Уведомлението до ДКСИ и получателите на даден класифициран документ по чл. 50, ал. 8 от ППЗЗКИ, че нивото на класификация на документа е премахнато или променено, трябва да съдържа:

- наименование на организационната единица, в която е създаден документът;
- уникален регистрационен номер на документа;
- правното основание за промяна нивото на класификация и новият гриф за сигурност, респ. правното основание за премахване нивото;
- дата на извършване на промяната/премахването нивото на класификация.

Тук трябва да отбележим, че законодателят е дал възможност на автора на документа винаги, когато е възможно, да отбелязва върху материала разпореждания за премахване или промяна на нивото на класификация при изтичането на определен срок или при настъпване на определено събитие.

Във всички случаи получателите незабавно отбелязват промяната или премахването на грифа за сигурност върху материала и отразяват това.

За извършеното преразглеждане на създадените в организационната единица документи и материали се изготвя протокол или списък, които се подписват от всички членове на комисията и се утвърждават от ръководителя на организационната единица.

В хипотезата за удължаване срока на защита, промяна нивото на класификация на информацията или премахване на нивото на класификация по чл. 50, ал. 5, т. 3 от ППЗЗКИ, на основание чл. 50, ал. 8 от ППЗЗКИ, се изготвя протокол и следва да се уведоми ДКСИ, както и всички получатели на документите.

В хипотезата за премахване на нивото на класификация, поради изтекъл срок на защита (чл. 50, ал. 5, т. 1 и т. 2 от ППЗЗКИ), се изготвя списък, който се изпраща само до ДКСИ.

УНИЩОЖАВАНЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

"Най-добрата защита на класифицираната информация е нейното своевременно унищожаване"

(*основен принцип на служителя по сигурността на информацията*)

1. Унищожаване на класифицираната информация – същност и особености

Унищожаването на информацията е **процес, а не еднократен акт.** В зависимост от вида на носителите на информация и използваните методи, процедурата може да се раздели на унищожаване на: документи и материали; материални носители за многократен запис и информация, получена в хода на извършване на проучване за надеждност.

Задължителни предпоставки за унищожаване на класифицирана информация, която е създадена в организационната единица, са: изтичане на срока за защита (съгласно чл. 34, ал.1 от ЗЗКИ); изтичане на една година след срока на защита (съгласно чл. 33, ал. 3 от ЗЗКИ), в случай, че информацията няма историческо, практическо или справочно значение.

Държавната комисия по сигурността на информацията разрешава унищожаването на информация след предложение на комисия, съставена със заповед на ръководителя на съответната организационна единица. Комисията се състои от най-малко трима членове (чл.120, ал. 2 от ППЗЗКИ). Комисията дава заключение коя информация няма историческо, практическо или справочно значение и прави предложение за унищожаване на документи и материали.

Предложението задължително съдържа описание на предложените за унищожаване материали, както и фактическите и правните основания за унищожаването.

Решението на ДКСИ е индивидуален административен акт, който след влизане в сила се изпраща на организационната единица. Подлежи на съдебно обжалване пред съответния административен съд.

Унищожаване на първи или единствени екземпляри (оригинали) на документи и материали, носители на класифицирана информация с изтекъл срок на защита

Компетентният орган, който разрешава унищожаването на документи и материали е **ДКСИ** при спазване на следната процедура:

- **Ръководителят** на организационната единица със заповед **назначава комисия**, която се състои най-малко от трима членове, с валидни разрешения за достъп до най-високото ниво на преразглежданата информация.
- **Комисията разглежда материалите** с цел да установи дали е изтекъл законоустановеният срок за защита, предвиден за съответното ниво на класификация за сигурност и съответно дали е изминала една година от неговото изтичане.
- **Комисията извършва анализ и оценява** историческото, практическото или справочното значение на информацията с изтекли срокове.
- **Изводът на комисията** относно историческото, практическото или справочното значение на документите **не е достатъчен**. Необходимо е наличието на **становище от Държавна агенция „Архиви”** (или нейна териториална структура).
- В заключение **комисията изготвя мотивирано писмено предложение** до ДКСИ за унищожаване на първи екземпляри (оригинали) на документи-носители на класифицирана информация, с изтекъл срок на защита, които нямат историческо, практическо или справочно значение.

За да може ДКСИ да направи обективна оценка, предложението трябва да съдържа:

- пореден номер на документа (материала);
- организационна единица;
- уникален регистрационен номер на документа;
- дата на създаване на документа (материала);

- предвидена дата на изтичане на срока на защита
- дата на премахване на нивото на класификация;
- наименование на документа (материала);
- ниво на класификация;
- екз. № 1 или единствен (ако е създаден преди влизане в сила на ЗЗКИ и е маркиран като втори или следващ екземпляр, изрично да се посочи, че е оригинал и дали е приложена процедурата по § 9 от ПЗР на ЗЗКИ);
- брой на листовете;
- забележка;

Копие на становището на Държавна агенция „Архиви”.

Експертна група на ДКСИ анализира предложението и при спазени нормативни изисквания, ДКСИ разглежда по същество предложението и се произнася със съответното решение, което се изпраща до организационната единица.

След получаване на решението на ДКСИ, **комисия**, назначена от ръководителя на организационната единица **унищожава информацията**, за която е получила разрешение в присъствието на всички членове по начин, който не позволява изцяло или частично възстановяване на документа (материала) и възпроизвеждане на информацията. **Съставя се протокол** за извършеното унищожаване, като в него задължително се отразява номерът на писменото разрешение от ДКСИ.

Протоколът се подписва от членовете на комисията и се **утвърждава от ръководителя** на организационната единица.

Протоколите се оформят в сборове от документи, които не се приключват и не се предават в архив. Съгласно чл. 128 от ППЗЗКИ не се разрешава извършването на поправки и зачеркванията върху протоколите.

Унищожаване на други документи и материали, съдържащи класифицирана информация

Обект на унищожаване по тази процедура са **втори и следващи екземпляри** и копия на материали, **съдържащи класифицирана информация** по смисъла на действащата нормативна уредба.

Задължително условие тук е липсата на разпореждания от лицата по чл. 31, ал. 1 от ЗЗКИ, които забраняват тяхното унищожаване.

По тази процедура се унищожават и **лични работни тетрадки** и бележници на служителите, **които съдържат бележки и данни,** представляващи държавна или служебна тайна, както и отчетни документи по ППЗЗКИ (регистри, номенклатурен списък на видовете регистри, тетрадки за отразяване на движението на материалите в рамките на организационната единица, контролни листове за запознаването с документи, картон-заместители и др.). Унищожаването на последните е възможно, ако са унищожени или предадени в архив всички материали, заведени в тях.

При тази процедура липсва забраната за унищожаване преди изтичането на сроковете за защита и процедурата е облекчена. Причината е, че тук унищожаването на документа (втори или следващ екземпляр), в който е обективирана класифицираната информация, по принцип не води до окончателното й загубване, тъй като тя продължава да се съхранява в първия екземпляр, който е при автора.

Процедурата за унищожаване на такива документи е следната:

- **Ръководителят** на организационната единица **назначава със заповед комисия** в състав най-малко от трима членове, които имат издадено разрешение за достъп до съответното ниво на класификация на информацията;
- **Комисията разглежда документите** с цел да установи дали се касае за втори и следващи екземпляри или такива по чл. 121, ал. 1, т. 3 и т. 4 от ППЗЗКИ. При втори и следващи екземпляри трябва да се констатира има ли отбелязани върху тях разпореждания на автора на документа. При наличие на

изразена воля от страна на лицето по чл. 31, ал. 1 от ЗЗКИ, чрез съответното изрично разпореждане върху документа, същият не се унищожава.

- **Комисията преценява съдържанието** на материалите и в резултат на преценката прави предложение за унищожаването им.
- **При изпълнени законови предпоставки, комисията изготвя предложение за унищожаване до ръководителя на организационната единица**, в която се намират документите (материалите). В случая не е необходимо решение на ДКСИ, а достатъчно условие за унищожаването им е разрешението на ръководителя на организационната единица.

Процедурата по унищожаване се осъществява от комисия, която трябва да се състои **най-малко от трима членове** и да бъде назначена със заповед на ръководителя на организационната единица. Унищожаването се извършва в присъствието на всички членове на комисията по начин, непозволяващ изцяло или частично възстановяване на документите (материалите).

За извършеното унищожаване се съставя протокол. Протоколите се оформят в сборове от документи, които не се приключват и не се предават в архив. Не се разрешава извършването на поправки и зачеркванията върху протоколите.

Унищожаването на класифицирана информация, получена от друга организационна единица, маркирана като втори и следващи екземпляри, както и копия на документи е възможно да се извърши преди изтичането на срока й за защита. Документите и материалите се унищожават по предложение на комисията по чл.120 от ППЗЗКИ и след разрешение на ръководителя на организационната единица, в която се намират материалите.

Унищожаване на материални носители за многократен запис на класифицирана информация

Предпоставките за унищожаване на материални носители за многократен запис са:

- изтичане на експлоатационния срок;
- физическа повреда на носителя за многократен запис, поради което информацията не може да се изтрие.

Унищожаването на материални носители за многократен запис поради изтичане на експлоатационния срок на годност или по други причини се извършва:

– след като е осигурено копие на класифицираната информация, ако тя е необходима и не се съхранява на друг носител;

– след специално изтриване на класифицираната информация върху носителя, и

– по начин, непозволяващ използването на носителя или на части от него и извличането на остатъчна информация.

Забранява се понижаване или премахване на нивото на класификация на носител по чл. 138, ал. 1 с ниво „Строго секретно”.

Специалното изтриване е изтриване, **при което е невъзможно** или е много трудно **получаването на остатъчна информация**, като:

1. методите и средствата за специално изтриване трябва да са одобрени от службите за сигурност за съответното или по-високо ниво;

2. за информация с ниво на класификация до „Поверително“ включително, след съгласуване с Държавна агенция „Национална сигурност“, е допустимо използване на методи и средства, одобрени от ЕС и/или НАТО за съответното или по-високо ниво.

Когато унищожаването е поради физическа повреда на носителя, поради което информацията не може да се изтрие, или носителят е за

еднократен запис, **той се унищожава, без да се извършва специално изтриване.**

Специалното изтриване на информацията или унищожаването на носители се **извършва от комисия**, назначена със заповед на ръководителя на организационната единица, за което се изготвя протокол. Протоколът се подписва от всички членове на комисията, предоставя се на служителя по сигурността на информацията и се съхранява в регистратурата. **Протоколът е основание за снемане от отчет на носителите в регистратурата и като материални средства.**

Криптографските средства и материали за защита на класифицирана информация, както и ключовите материали се маркират, съхраняват, отчитат, архивират и унищожават по реда на наредбата по чл. 85 от ЗЗКИ.

Маркирането, съхраняването и отчитането на криптографските средства и материали за защита на класифицирана информация, както и ключовите материали се извършва в криптографска регистратура, която е част от регистратурата на организационната единица по чл. 51, ал. 1, или в отделна регистратура, създадена на основание чл. 51, ал. 3.

Унищожаване на класифицирана информация, получена в хода на извършване на проучване за надеждност

Процедурата е специфична, изразяваща се в изключване на общата забрана за унищожаване на класифицирана информация в срока на защита и в едногодишен срок след това.

Делата по проучване за надеждност се разглеждат като сбор от документи, в който по принцип има и явни материали. Не се допуска изваждане и унищожаване на отделни или сбор от документи, заведени в описа на делото.

Делата по проучване за надеждност на лице, **получило отказ** за издаване на разрешение за достъп до класифицирана информация, на което е отнето такова разрешение или е прекратено действието на издаденото

разрешение, **се съхраняват за срок до 5 години** от датата на влизането в сила на отказа, отнемането или прекратяването.

При откриване на нова процедура по проучване, **предшестващите дела се прилагат** и стават част от съответните нови дела по проучване.

Предпоставка за унищожаване на дела по проучване за надеждност е прекратяване на проучването, което е възможно по следните причини:

- **оттегляне** на писменото съгласие на лицето за извършване на проучване;
- **отпадане** на длъжността или на конкретната задача, свързана с достъп до класифицирана информация;
- **оттегляне** на искането за проучване от ръководителя на организационната единица.

При отпадане на необходимостта от достъп до класифицирана информация, предоставените от проучваното лице материали и документи се връщат на лицето от органа, извършващ проучването, срещу разписка.

Унищожаването на делата по проучване за надеждност се извършва по следната процедура:

- **назначаване на комисия** от проучващия орган, която да извърши унищожаването;
- **унищожаване на материалите** по начин, непозволяващ възстановяване и възпроизвеждане на информацията;
- **съставяне на протокол** за извършеното унищожаване;
- **завеждане на протокола в регистъра** на делата по проучване с номер, съответстващ на номера на унищоженото дело.

В едномесечен срок екземпляр от **протокола** за извършеното физическо унищожаване **се изпраща в ДКСИ.**

Своевременното унищожаването на класифицираната информация е основна предпоставка за изпълнение на целта на ЗЗКИ – нейната защита от нерегламентиран достъп.

ИНДУСТРИАЛНА СИГУРНОСТ

ОБЩИ ПОЛОЖЕНИЯ

Предмет

1. Предмет на настоящите насоки на работа е редът за гарантиране на индустриалната сигурност при сключване и изпълнение на договори при условията на глава VI, раздел VI от Закона за защита на класифицираната информация (ЗЗКИ), глава VII от Правилника за прилагане на ЗЗКИ (ППЗЗКИ) и Наредбата за общите изисквания за гарантиране на индустриалната сигурност (НОИГИС), както и Наредбата за условията и реда за допускане на български физически или юридически лица до участие в международни процедури на Организацията на Северноатлантическия договор (НАТО).

Цел

2. Целта на настоящите насоки на работа е защитата на класифицираната информация от нерегламентиран достъп при сключване или изпълнение на договор по чл. 95, ал. 1 от ЗЗКИ.

Принципи

3. Индустриалната сигурност се основава на принципа „необходимост да се знае“ и принципа на всеобхватност.

4. Прилагането на принципа „необходимост да се знае“ в областта на индустриалната сигурност се състои в ограничаване на достъпа само до определена класифицирана информация, свързана със сключването и изпълнението на договор по чл. 95, ал. 1 от ЗЗКИ, и само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп във връзка със сключването и изпълнението на този договор.

5. Прилагането на принципа „необходимост да се знае“ е задължително още при подготовката за сключване на договор по чл. 95, ал. 1 от ЗЗКИ. За целта организационната единица възложител следва да предприеме своевременно необходимите действия кандидатите за изпълнители по договора да бъдат проучени за надеждност и да имат издадени

удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация.

6. Прилагането на принципа на всеобхватност се състои в изпълнение както на специфичните изисквания за достъп до определена класифицирана информация на физическите и юридическите лица, кандидати, изпълнители или подизпълнители по договор по чл. 95, ал. 1 от ЗЗКИ, така и на изискванията в областта на останалите видове сигурност на информацията: персонална, документална и физическа сигурност, сигурност на комуникационни и информационни системи (КИС) и криптографска сигурност.

Приложение:

7. Изискванията за гарантиране на индустриалната сигурност се прилагат при сключване и изпълнение на договори по чл. 95, ал. 1 от ЗЗКИ.

8. Изискванията за гарантиране на индустриалната сигурност са приложими във всички случаи и спрямо договори, свързани с достъп до чуждестранна класифицирана информация по смисъла на ЗЗКИ, в случай че:

а) има сключено и влязло в сила споразумение за обмен и взаимна защита на класифицирана информация между Република България и държавата източник на чуждестранната класифицирана информация, и

б) има изрична воля за това от държавата източник на чуждестранната класифицирана.

Обвързваща сила

9. Задължението за прилагане на изискванията в областта на индустриалната сигурност е обвързващо и след изтичане на срока на конкретния договор по чл. 95, ал. 1 от ЗЗКИ.

10. След получаване на удостоверение за сигурност кандидатите за изпълнители на договори по чл. 95, ал. 1 от ЗЗКИ имат всички задължения на организационни единици и дължат изпълнение на изискванията на закона, отнасящи се за организационните единици (съгласно чл. 112 от ЗЗКИ).

Специални закони

11. Прилагането на принципите и мерките в областта на индустриалната сигурност не изключва приложимостта и на други изисквания, установени в специални закони, с оглед спецификата на конкретния договор по чл. 95, ал. 1 от ЗЗКИ.

12. Прилагането на принципите и мерките в приложното поле на специални закони, с оглед спецификата на предмета на конкретния договор по чл. 95, ал. 1 от ЗЗКИ не изключва приложимостта на принципите и мерките в областта на индустриалната сигурност.

Проучващи органи

13. Проучващите органи по чл. 95, ал. 3 от ЗЗКИ (проучващи органи по индустриална сигурност), за извършване на проучване на кандидати, изпълнители и подизпълнители по договори, свързани с достъп до класифицирана информация се определят от Министерски съвет. Те са:

а) Държавната комисия по сигурността на информацията (ДКСИ) – извършва проучване на физически и юридически лица, кандидатстващи за сключване на договор или извършващи дейност за нуждите на ДКСИ.

б) Държавна агенция „Разузнаване” (ДАР) – извършва проучване на физически и юридически лица, кандидатстващи за сключване на договор или извършващи дейност за нуждите на ДАР.

в) Служба „Военно разузнаване“ – Министерство на отбраната (СВР-МО), – извършва проучване на физически и юридически лица, кандидатстващи за сключване на договор или извършващи дейност за нуждите на СВИ-МО;

г) Държавна агенция „Технически операции“ (ДАТО) – извършва проучване на физически и юридически лица, кандидатстващи за сключване на договор или извършващи дейност за нуждите на ДАТО.

д) Държавна агенция „Национална сигурност“ (ДАНС) – извършва проучване на физически и юридически лица, кандидатстващи за сключване на договор или извършващи дейност за нуждите на ДАНС и на всички

организационни единици възложители, с изключение на тези по т. 13, „а“, „б“, „в“ и „г“ , които извършват проучване сами за себе си.

14. Проучващите органи по индустриална сигурност издават удостоверение за сигурност на българските юридически лица и съответните разрешения за достъп до класифицирана информация на българските физически и юридически лица.

15. Държавна агенция „Национална сигурност“ в качеството на проучващ орган по индустриална сигурност издава както удостоверение за сигурност и съответните разрешения за достъп до класифицирана информация, така и потвърждение за достъп до класифицирана информация на чуждестранни физически и юридически лица.

Изисквания към физическите и юридическите лица

16. Всички лица, които е необходимо да имат достъп до класифицирана информация във връзка със сключването и изпълнението на договор по чл. 95, ал. 1 от ЗЗКИ, трябва да отговарят на изискванията на глава V от ЗЗКИ и чл. 6 от НОИГИС.

17. Българските физически лица, които кандидатстват за сключване или изпълнение на договор и не са търговци, се проучват от органите по глава V на ЗЗКИ (чл. 176 от ППЗЗКИ).

18. Чуждестранни юридически лица и физически лица, граждани на чужди държави, могат да получат достъп до класифицирана информация във връзка със сключването и изпълнението на договор по чл. 95, ал. 1 от ЗЗКИ при наличието на:

а) сключен и влязъл в сила договор за обмен и взаимна защита на класифицирана информация между Република България и съответната държава.

б) получено потвърждение от съответния чуждестранен компетентен орган за наличието на разрешение или удостоверение за достъп до класифицирана информация.

19. Чуждестранните физически и юридически лица, кандидатстващи за сключване или изпълнение на договор по чл. 95, ал. 1 от ЗЗКИ, представят на възложителя на договора искане за издаване на потвърждение на чуждестранно лице. Възложителят изпраща искането в ДКСИ, която възлага на ДАНС издаване на потвърждение.

20. Чуждестранните физически и юридически лица, кандидатстващи за сключване или изпълнение на договор по чл. 95, ал. 1 от ЗЗКИ, трябва да притежават издадено от ДАНС потвърждение за достъп до класифицирана информация.

Обучение в областта на индустриалната сигурност

21. Обучение в областта на индустриалната сигурност се провежда по отношение на всички физически лица, участващи в дейностите и задачите по сключването или изпълнението на договор по чл. 95, ал. 1 от ЗЗКИ.

ПРОЦЕДУРА ПО ПРОУЧВАНЕ ПРЕЗ ВЪЗЛОЖИТЕЛ

ПОДГОТОВКА ЗА СКЛЮЧВАНЕ
НА ДОГОВОР ПО ЧЛ. 95, АЛ. 1 ОТ ЗЗКИ

Видове договори

22. Договорите по чл. 95, ал. 1 от ЗЗКИ (договори, свързани с достъп до класифицирана информация) са:

а) договори, чийто предмет съдържа класифицирана информация;

б) договори, чието изпълнение налага достъп до класифицирана информация;

в) договори, чийто предмет съдържа и чието изпълнение налага достъп до класифицирана информация.

Мотивирано становище

23. Преди започване на процедурите по водене на преговори и за определяне на изпълнител на договор по чл. 95, ал. 1 от ЗЗКИ служителят по сигурността на информацията на организационната единица възложител изготвя мотивирано становище.

24. Мотивираното становище е писмен документ, в който служителят по сигурността на информацията на организационната единица възложител описва:

а) предмета на договора по чл. 95, ал. 1 от ЗЗКИ и нивото на класификацията му;

б) основанията и условията, при които се налага достъп до класифицирана информация във връзка с договора (в изпълнение на чл. 169 от ППЗЗКИ), включително вида на договора.

в) реда за изпълнение на специфичните изисквания по чл. 10 – 13 от НОИГИС.

Схема за класификация на етапите

25. Преди започване на процедурите по водене на преговори и определяне на изпълнител, служителят по сигурността на информацията на организационната единица възложител изготвя схема за класификация на етапите за сключване и изпълнение на договора по чл. 95, ал. 1 от ЗЗКИ, съгласно изискванията на чл. 4, ал. 2 от НОИГИС.

26. Схемата за класификация на етапите съдържа:

а) конкретно и точно описание на предмета на договора по чл. 95, ал. 1 от ЗЗКИ и нивото на класификацията му;

б) подробни описания на основанията и условията, при които се налага достъп до класифицирана информация във връзка с договора (в изпълнение на чл. 169 от ППЗЗКИ), включително

в) конкретно и точно описание на вида на договора съгласно т. 20 от настоящите задължителни указания;

г) определяне на служителите по чл. 105 от ЗЗКИ и чл. 12, ал. 1 от НОИГИС;

д) подробни описания на дейностите и задачите във връзка с договора в отделно обособени етапи, като за всяка дейност и задача се посочват времето и мястото на нейното извършване, както и съдържанието и нивото на класификация на информацията, до която се налага достъп;

е) подробни описания на дейностите и задачите за изпълнение на специфичните изисквания по чл. 10 – 13 от НОИГИС.

ж) подробни описания на дейностите и задачите за изпълнение срока на задълженията по чл. 17 от НОИГИС (съгласно чл. 13 от НОИГИС).

27. Дейностите и задачите се описват в отделно обособени етапи в схемата за класификация на етапите и се подреждат хронологично, както следва:

а) Подготовка на договора – етап на дейностите и задачите по предварителния подбор и подготовката; провеждането на процедурата по набиране на кандидати; провеждането на инструктаж относно изискванията за работа с класифицирана информация; изготвянето и приемането на офертите, предварителните разговори с кандидатите за определяне на изпълнителите и подизпълнителите на договора; воденето на преговори, окончателния избор и определянето на изпълнители и подизпълнители;

б) Сключване на договора – етап на дейностите и задачите по окончателното изготвяне и подписване на договора;

в) Изпълнение на договора – етап на дейностите и задачите, извършвани в изпълнение на предмета на договора;

г) Приключване/Прекратяване на договора – етап на дейностите и задачите по приемането на изпълнението на договора и прекратяването на договорните отношения;

д) Етап след приключване/прекратяване на договора – етап на дейностите и задачите по защитата на класифицираната информация след прекратяването на договорните отношения.

28. В схемата за класификация на етапите всяка отделна дейност и всяка отделна задача се класифицира до необходимото ниво на класификация отделно от останалите, като нивото на класификация на всяка отделна дейност и всяка отделна задача може да е различно от нивото на класификация на останалите дейности и задачи. Най-високото ниво на класификация на дейностите и задачите е нивото на класификация на договора по чл. 95, ал. 1 от ЗЗКИ.

29. Схемата за класификация на етапите се съгласува с проучващия орган по чл. 95, ал. 3 от ЗЗКИ.

30. Схемата за класификация на етапите, след съгласуването ѝ с проучващия орган по чл. 95, ал. 3 от ЗЗКИ, е неразделна част от договора по чл. 95, ал. 1 от ЗЗКИ.

Съдържание на договорите

31. В съдържанието на договорите по чл. 95, ал. 1 от ЗЗКИ задължително се включват:

а) клаузи в изпълнение на разпоредбите на раздел VI от ЗЗКИ, глава VII от ППЗЗКИ и раздел II от НОИГИС.

б) изискванията за индустриална сигурност (чл. 95, ал. 4 от ЗЗКИ и чл. 10 – 13 от НОИГИС).

32. В съдържанието на договорите по чл. 95, ал. 1 от ЗЗКИ могат бъдат включени клаузи за допълнителни права и задължения с оглед спецификата на конкретния договор.

33. Неразделна част от договорите по чл. 95, ал. 1 от ЗЗКИ са:

а) Схемата за класификация на етапите след съгласуването ѝ с компетентния орган по чл. 95, ал. 3 от ЗЗКИ.

б) Списъкът с лицата, получили разрешение за достъп до класифицирана информация във връзка с договора.

ПОДГОТОВКА НА ПРОЦЕДУРАТА ПО ПРОУЧВАНЕ ЗА НАДЕЖДНОСТ ВЪВ ВРЪЗКА СЪС СКЛЮЧВАНЕ НА ДОГОВОР ПО ЧЛ. 95, АЛ. 1 ОТ ЗЗКИ

Задължения на организационната единица възложител

34. Ръководителят на организационната единица възложител организира и провежда процедурата, свързана със сключването на договора по чл. 95, ал. 1 от ЗЗКИ, в следния ред:

34.1. Възлага на служителя по сигурността на информацията на организационната единица възложител изготвянето на мотивирано становище.

34.2. Определя лице по чл. 105 от ЗЗКИ, като това лице може да бъде ССИ на организационната единица възложител.

34.3. Възлага на служителя по сигурността на информацията да изготви схема за класификация на етапите

34.4. Изпраща на компетентния проучващ орган схемата за класификация на етапите за съгласуване.

34.5. Уведомява кандидатите относно предмета на договора и нивото на класификация, като спазва принципа „необходимост да се знае“ и изискванията на ЗЗКИ и актовете по неговото прилагане.

34.6. Изисква от кандидатите за изпълнители информация относно наличието на удостоверение за сигурност, разрешения, сертификати и потвърждение за достъп до класифицирана информация.

34.7. Изпраща подписано от него писмено запитване до проучващите органи по чл. 95, ал. 3 от ЗЗКИ за наличието на издадено удостоверение за сигурност, разрешение и потвърждение за достъп до класифицирана информация (чл. 170, ал. 2 от ППЗЗКИ).

34.8. Изисква и получава от кандидатите, непритежаващи издадено удостоверение за сигурност, разрешение, сертификат и потвърждение за достъп до класифицирана информация, необходимите искания с приложени към тях документи за започване на процедурата по проучване за надеждност.

34.9. Отправя покани за водене на преговори и определяне на изпълнител, когато се изисква достъп до класифицирана информация, само към:

а) кандидатите, които имат към момента на уведомяване удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация;

б) кандидатите, спрямо които процедурата по проучване за надеждност е завършила с издаване на удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация, въз основа на изпратените от него искания и документи до проучващия орган.

34.10. Дава указания на кандидатите за изпълнители за спазване на разпоредбите на ЗЗКИ и актовете по неговото прилагане.

35. Служителят по сигурността на информацията на организационната единица възложител извършва подготовката по договора по чл. 95, ал. 1 от ЗЗКИ, както следва:

35.1. Изпълнява поставените задачи от ръководителя на организационната единица възложител във връзка със задълженията по т. 34 от настоящите указания и контролира спазването на изискванията на ЗЗКИ и актовете по неговото прилагане във връзка с договора.

35.2. Изготвя мотивираното становище съгласно т. 23 и 24 от настоящите указания във връзка със сключването и изпълнението на договора.

35.3. Изготвя схемата за класификация на етапите за сключване и изпълнение на договора по чл. 95, ал. 1 от ЗЗКИ, съгласно т. 25 – 28 от настоящите указания.

35.4. Контролира изпълнението на задълженията от лицата по чл. 105 от ЗЗКИ и чл. 12, ал. 1 от НОИГИС за спазване на ЗЗКИ и актовете по неговото прилагане във връзка с договора по чл. 95, ал. 1 от ЗЗКИ и при необходимост дава съответните указания.

36. Лицето по чл. 105 осъществява контрол по прилагането на специфичните изисквания по чл. 10 от НОИГИС, заложени в договора.

37. Лицето по чл. 105 от ЗЗКИ трябва да отговаря на следните изисквания:

а) да е служител в организационната единица възложител;

б) да притежава разрешение за достъп до информация с най-високото ниво на класификация съгласно договора;

в) да е преминало обучение по защита на класифицираната информация.

38. Лицето по чл. 105 от ЗЗКИ следи за спазването на разпоредбите на ЗЗКИ и актовете по неговото прилагане във връзка със сключването и изпълнението на договора по чл. 95, ал. 1 от ЗЗКИ и при необходимост дава указания за това на лицето по чл. 12, ал. 1 от НОИГИС.

Задължения на кандидата

39. Кандидатът:

39.1. Определя лице по чл. 12, ал. 1 от НОИГИС, което отговаря за прилагането на мерките за защита на класифицираната информация при подготовката, сключването и изпълнението на договора по чл. 95, ал. 1 от ЗЗКИ.

39.2. Лицата, които управляват и представляват кандидата за изпълнение по договор, представят на възложителя писмени искания и съгласия за започване на проучването, като попълват въпросниците по приложение № 2 към чл.47 и 48 от ЗЗКИ и съгласно приложение № 23.

39.3. Отправят писмено искане до ДКСИ, подписано от ръководителя на организационната единица изпълнител, за издаване на разрешение на служителя по сигурността на информацията на организационната единица с пълния комплект документи по персонална сигурност, които се изпращат на възложителя.

39.4. Изпълнява указанията на организационната единица възложител за спазване на разпоредбите на ЗЗКИ и актовете по неговото прилагане.

39.5. Предоставя на организационната единица възложител, необходимите документи за извършване на процедурата по проучване за надеждност съгласно изискванията на ЗЗКИ и актовете по неговото прилагане, включително предоставя списъците с лицата съгласно Приложение № 23 към чл. 173, ал. 1 от ППЗЗКИ.

39.6. При необходимост правят изменения или/и допълнения в списъка на лицата по чл. 10, ал. 2, т. 6 от НОИГИС, когато това е съгласувано с организационната единица възложител.

40. Лицето по чл. 12, ал. 1 от НОИГИС трябва да отговаря на следните изисквания:

а) да е служител в организационната единица кандидат или изпълнител по договора, свързан с достъп до класифицирана информация;

б) да притежава разрешение за достъп до класифицирана информация с най-високото ниво на класификация съгласно договора;

в) да е преминало обучение по защита на класифицираната информация.

41. Лицето по чл. 12, ал. 1 от НОИГИС следи за спазването и правилното прилагане на разпоредбите на ЗЗКИ и актовете по неговото прилагане във връзка със сключването и изпълнението на договора по чл. 95, ал. 1 от ЗЗКИ и изпълнява указанията от лицето по чл. 105 от ЗЗКИ.

Задължения на проучващите органи

42. Проучващите органи:

42.1. Съгласуват схемата за класификация на етапите.

42.2. Оказват съдействие, подпомагат и контролират възложителя и кандидатите за спазването на разпоредбите на ЗЗКИ и актовете по неговото прилагане.

42.3. Предприемат необходимите действия с оглед предотвратяване на нерегламентиран достъп до класифицирана информация и минимизиране на евентуалните вреди от неговото осъществяване във връзка със задълженията по чл. 10, ал. 2, т. 9 от НОИГИС.

ИНИЦИИРАНЕ НА ПРОЦЕДУРА ПО ПРОУЧВАНЕ И СТАРТИРАНЕ НА ДОГОВАРЯНЕ ЗА СКЛЮЧВАНЕ НА ДОГОВОР ПО ЧЛ. 95, АЛ. 1 ОТ ЗЗКИ

Изготвяне и окомплектоване на необходимите документи

43. За иницииране на процедурата по проучване за надеждност на български юридически лица кандидати, които не притежават необходимите удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация при подготовката за сключване и изпълнение на договори по чл. 95, ал. 1 от ЗЗКИ, ръководителят на организационната единица възложител изготвя подписани от него следните документи:

а) писмено искане до компетентния проучващ орган, подписано от ръководителя на организационната единица възложител, за издаване на удостоверение за сигурност на кандидата българско юридическо лице.

б) писмено искане до ДКСИ, подписано от ръководителя на организационната единица възложител, за издаване на разрешение на служителя по сигурността на информацията, определен от кандидата, във връзка с обществената поръчка или изпълнението на договора.

в) писмено искане до ДКСИ, подписано от ръководителя на организационната единица възложител, при необходимост за издаване на сертификат за достъп до класифицирана информация на НАТО на кандидата българско юридическо лице.

г) писмено искане до ДКСИ, подписано от ръководителя на организационната единица възложител, при необходимост за издаване на

сертификат за достъп до класифицирана информация на ЕС на кандидата българско юридическо лице.

д) писмено искане до ДКСИ, подписано от ръководителя на организационната единица възложител, при необходимост за издаване на потвърждение за достъп до класифицирана информация на кандидата чуждестранно лице.

44. Към искането за издаване на удостоверение за сигурност ръководителят на организационната единица възложител прилага съответните искания и документи, получени от кандидата за издаване на необходимите разрешения, сертификати и потвърждения за достъп до класифицирана информация.

45. За иницииране на процедурата по проучване за надеждност на български юридически лица кандидати за сключване и изпълнение на договори по чл. 95, ал. 1 от ЗЗКИ, ръководителят на юридическото лице кандидат изготвя подписани от него и предоставя на организационната единица възложител следните документи:

а) писмено съгласие по чл. 97 от ЗЗКИ от лицата, които управляват и представляват кандидата, за проучване на юридическото лице, съгласно приложение № 22 към чл. 171, т. 2 от ППЗЗКИ;

б) попълнен от кандидата юридическо лице въпросник – приложение № 23 към чл. 173, ал. 1 от ППЗЗКИ;

в) документите и приложенията към въпросника – приложение № 23 към чл. 173, ал. 1 от ППЗЗКИ (по б. „б“);

г) писмени декларации от лицата, които управляват и представляват кандидата юридическо лице по чл. 74, ал. 2, т. 1 от ДОПК, за предоставяне на необходимата данъчна и осигурителна информация по смисъла на чл. 72, ал. 1 от ДОПК, за целите на проучването.

д) писмено съгласие от лицата, които управляват и представляват кандидата юридическо лице, за предоставяне на данни за авоарите, операциите по сметките и влоговете за целите на проучването.

е) писмено искане до ДКСИ за издаване на разрешение за достъп до класифицирана информация на служителя по сигурността на информацията на кандидата за изпълнител, с приложени към него документи съгласно чл. 147, ал. 1 от ППЗЗКИ за извършване на проучването за надеждност;

ж) необходимите писмени искания и приложени към тях документи за служителите на кандидата, които не притежават валидни разрешения и сертификати за достъп до класифицирана информация;

з) необходимите писмени искания за издаване на потвърждения за достъп до класифицирана информация на чужди юридически и физически лица.

Задължения на организационната единица възложител

46. Служителят по сигурността на информацията на организационната единица възложител:

46.1. Проверява получените от кандидата документи във връзка със сключването на договор по чл. 95, ал. 1 от ЗЗКИ с оглед спазване на изискванията на закона, преди да бъде инициирана процедурата по проучване за надеждност и преди договарянето, при което се изисква достъп до класифицирана информация съгласно утвърдената схема за класификация на етапите.

46.2. При необходимост, предлага на ръководителя на организационната единица възложител да бъдат изпратени указания на кандидата за отстраняване на грешките и пропуските в предоставените документи.

46.3. Когато необходимите документи по проучване за надеждност на кандидата са изготвени, попълнени и окомплектовани съобразно изискванията на ЗЗКИ, предлага те да бъдат изпратени на компетентния проучващ орган.

46.4. След като получи информация, че кандидатът притежава необходимото удостоверение за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация, предлага да се

пристъпи към изпълнение на дейностите и задачите по договаряне, за които се изисква достъп до класифицирана информация съгласно утвърдената схема за класификация на етапите.

47. Ръководителят на организационната единица възложител:

47.1. Изпраща на компетентния проучващ орган необходимите искания и документи по т. 43 – 45 за иницииране на проучването за надеждност на кандидатите български граждани и юридически лица, които не притежават необходимите удостоверения за сигурност и съответните разрешения, сертификати и потвърждения за достъп до класифицирана информация.

47.2. Разпорежда изпълнението на дейностите и задачите по договарянето, за които се изисква достъп до класифицирана информация съгласно утвърдената схема за класификация на етапите, с онези кандидати, които притежават необходимите удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация.

ИЗВЪРШВАНЕ НА ПРОЦЕДУРА ПО ПРОУЧВАНЕ ВЪВ ВРЪЗКА С ДОГОВОР ПО ЧЛ. 95, АЛ. 1 ОТ ЗЗКИ

Задължения на проучващите органи

48. Проучващият орган по чл. 95, ал. 3 от ЗЗКИ започва процедурата по проучване за надеждност на кандидата юридическо лице във връзка с договора по чл. 95, ал. 1 от ЗЗКИ, след като получи необходимите искания и документи и като прилага разпоредбите на чл. 97 – 107 от ЗЗКИ и глава VII от ППЗЗКИ.

49. Проучващият орган по чл. 95, ал. 3 от ЗЗКИ уведомява организационната единица възложител за издадените удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация във връзка с договора по чл. 95, ал. 1 от ЗЗКИ и при спазване на принципа „необходимост да се знае“.

50. Във връзка с договора по чл. 95, ал. 1 от ЗЗКИ компетентният проучващ орган открива незабавно дело за проучване за надеждност (ДПН) по

начина и реда, регламентирани в чл. 110 от ЗЗКИ и чл. 152 – 157, 179 и 180 от ППЗЗКИ, на онзи кандидат, който не притежава валидно удостоверение за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация.

Обект на проучване

51. Обект на проучване по индустриална сигурност са български юридически лица и български физически лица-търговци.

52. Обект на проучване могат да бъдат и чуждестранни лица, като в този случай проучването се извършва при условията и по реда на чл. 11, ал. 2, т. 2, ал. 3, т. 3 от ЗЗКИ, глава VI, раздел V, чл. 176 – 178 от ППЗЗКИ.

53. Процедурата по проучване на кандидатите за сключване на договор по чл. 95, ал. 1 от ЗЗКИ обхваща проучване за надеждност на следните физически лица, когато същите не притежават необходимите разрешения, сертификати и потвърждения за достъп до класифицирана информация:

а) ръководителите на организационните единици и служителите по сигурността на информацията на възложителя и на кандидата;

б) лицата, които притежават, управляват и представляват юридическото лице (собствениците, ръководителите, управителите, директорите, прокуристите), членовете на управителните органи (управителни съвети, съвети на директорите и други управителни органи съобразно организацията на дейността на юридическото лице), едноличния търговец и неговите управители;

в) лицата по чл. 105 от ЗЗКИ и чл. 12, ал. 1 от НОИГИС;

г) лицата, работещи в административното звено за сигурност на кандидата;

д) лицата, които съгласно утвърдената схема за класификация на етапите изпълняват дейности и задачи, свързани с воденето на преговори за сключването на договора, когато се налага достъп до класифицирана информация;

е) лицата, които съгласно утвърдената схема за класификация на етапите изпълняват дейности и задачи във връзка с договора, налагащи достъп до класифицирана информация.

Цел на процедурата по проучване

54. Процедурата по проучване има за цел да установи дали юридическото лице отговаря на изискванията съгласно чл. 100 от ЗЗКИ.

Обхват на проучването

55. Проучващите органи събират данни за структурата и произхода на капитала на кандидата, неговите търговски партньори, финансови отношения, вещни права и други данни, необходими за преценка на надеждността, като проверяват дали лицето отговаря на изискванията съгласно чл. 101 и 102 от ЗЗКИ.

Завършване на проучването

56. В зависимост от резултатите от проучването органът по чл. 95, ал. 3 от ЗЗКИ издава удостоверение за сигурност на юридическото лице или отказ за издаване на удостоверение за сигурност (съгласно чл. 103 и сл.).

Обжалване на отказ за издаване на удостоверение за сигурност

57. При обжалване на отказ за издаване на удостоверение за сигурност се прилагат разпоредбите на чл. 62 – 65 от ЗЗКИ.

58. При подаване на жалба срещу отказ за издаване на удостоверение за сигурност проучващият орган, постановил отказа, задължително изпраща в ДКСИ делото за проучване на кандидата за сключване на договор и делата за проучване на всички физически лица по чл. 97, ал. 1 от ЗЗКИ и т. 52 от настоящите задължителни указания.

59. При разглеждане на жалбите ДКСИ може да изисква допълнителни данни и доказателства от проучващите органи по чл. 95, ал. 3 от ЗЗКИ, както и да събира нови доказателства, вкл. чрез назначаване на експертизи, провеждане на интервюта и др.

ПРИЛАГАНЕ НА МЕРКИ
В ОБЛАСТТА НА ИНДУСТРИАЛНАТА СИГУРНОСТ
СЛЕД СКЛЮЧВАНЕ НА ДОГОВОР ПО ЧЛ. 95, АЛ. 1 ОТ ЗЗКИ

60. При необходимост най-малко три месеца преди изтичането срока на валидност на издаденото удостоверение за сигурност се извършва ново проучване, ако това е необходимо за изпълнение на същия или друг договор, който изисква достъп до класифицирана информация, при условията и по реда на глава VI, раздел VI от ЗЗКИ, глава VII от ППЗЗКИ и НОИГИС, както и Наредбата за условията и реда за допускане на български физически или юридически лица до участие в международни процедури на Организацията на Северноатлантическия договор (НАТО).

61. Удостоверението за сигурност се издава за срок от три години и важи за изпълнение на всеки друг договор, свързан с достъп до класифицирана информация от същото или по-ниско ниво на класификация (чл. 106 от ЗЗКИ).

62. След сключване на договор по чл. 95, ал. 1 от ЗЗКИ между организационната единица възложител и избрания кандидат за изпълнител, издадените удостоверения за сигурност, разрешения, сертификати и потвърждения за достъп до класифицирана информация на останалите кандидати се прекратяват/обезсилват от проучващия орган, който ги е издал.

63. Проучващите органи по чл. 95, ал. 3 от ЗЗКИ, служителят по сигурността на информацията на възложителя, служителят по сигурността на информацията на изпълнителя, лицето по чл. 105 от ЗЗКИ и лицето по чл. 12, ал. 1 от НОИГИС осъществяват последващ контрол за гарантиране на индустриалната сигурност във връзка с изпълнението и след приключване на изпълнението на договор, свързан с достъп до класифицирана информация.

64. Проучващите органи по индустриална сигурност взаимодействат помежду си под общото ръководство и контрол на ДКСИ, като обменят информация във връзка с процедурата по проучване за надеждност при

подготовката, сключването и изпълнението на договори по чл. 95, ал. 1 от ЗЗКИ.

ПОДГОТОВКА НА ПРОЦЕДУРАТА ЗА УЧАСТИЕ НА БЪЛГАРСКИ ФИЗИЧЕСКИ И ЮРИДИЧЕСКИ ЛИЦА В ПРОЦЕДУРИ НА НАТО

Основания за процедурата

65. Българско юридическо лице, което е регистрирано в базата данни на Министерството на икономиката за изпълнение поръчки на НАТО, може да инициира процедура по проучване за надеждност в областта на индустриалната сигурност, като предостави пълните комплекти документи за проучване по индустриална сигурност на ДКСИ.

Задължения на кандидатите

66. Кандидатът за участие в международни процедури на НАТО събира, изготвя, попълва, комплектува и изпраща в ДКСИ следните документи:

а) мотивационно писмо, подписано от ръководителя на кандидата, в което се посочват:

– наименование и вид на дружеството или три имена на физическото лице;

– предмет на дейност;

– ръководни органи (за юридическите лица);

– адрес, изписан на кирилица и на латиница;

– данни и лица за контакт: телефонни и мобилни номера, електронна поща, факс и др.;

– основанията за исканото ниво на достъп до класифицирана информация при условията и по реда, предвидени за кандидатите за участие в международни процедури на НАТО;

б) копие на писмо от Министерството на икономиката до кандидата, че същият е регистриран в публичната база данни на кандидатите за участие в международни процедури на НАТО за календарната година;

в) писмено искане до ДКСИ, подписано от ръководителя на кандидата за участие в международни процедури на НАТО, за издаване на сертификат за достъп до класифицирана информация на НАТО на кандидата.

г) писмено искане до ДАНС, подписано от ръководителя на кандидата за участие в международни процедури на НАТО, за издаване на удостоверение за сигурност .

д) писмено искане, подписано от ръководителя на кандидата за участие в международни процедури на НАТО, за издаване на потвърждение за достъп до класифицирана информация в случаите, когато участва чуждестранно лице - изпълнител;

е) писмено съгласие по чл. 97 от ЗЗКИ от лицата, които управляват и представляват кандидата за участие в международни процедури на НАТО, съгласно приложение № 22 към чл. 171, т. 2 от ППЗЗКИ;

ж) попълнен от кандидата за участие в международни процедури на НАТО въпросник – приложение № 23 към чл. 173, ал. 1 от ППЗЗКИ;

з) документите и приложенията към въпросника – приложение № 23 към чл. 173, ал. 1 от ППЗЗКИ (б. „ж“);

и) писмени декларации от лицата, които управляват и представляват кандидата за участие в международни процедури на НАТО, за предоставяне на необходимата данъчна и осигурителна информация по смисъла на чл. 72, ал. 1 от ДОПК, за целите на проучването;

к) писмено съгласие от лицата, които управляват и представляват кандидата за участие в международни процедури на НАТО, за предоставяне на данни за авоарите, операциите по сметките и влоговете за целите на проучването.

л) писмени искания до ДКСИ за издаване на разрешение за достъп до класифицирана информация и на сертификат за достъп до класифицирана

информация на НАТО на служителя по сигурността на информацията на кандидата за участие, с приложени към тях документи за извършване на проучването за надеждност съгласно чл. 147, ал. 1 от ППЗЗКИ;

м) писмени искания и приложени към тях документи съгласно чл. 147, ал. 1 от ППЗЗКИ за издаване на необходимите разрешения, сертификати и потвърждения за достъп до класифицирана информация на ръководителя на организационната единица, завеждащия и заместник завеждащия регистратура на кандидата за участие в международни процедури на НАТО;

н) писмени искания за издаване на потвърждения за достъп до класифицирана информация на чужди юридически и физически лица, при необходимост.

о) В хода на проучването кандидатът задължително разкрива регистратура за национална класифицирана информация и при необходимост регистратура за съхраняване и обработване на класифицирана информация на НАТО – чл. 17 от Наредбата за условията и реда за допускане на български физически или юридически лица до участие в международни процедури на НАТО.

Задължения на проучващите органи

67. Държавната комисия по сигурността на информацията възлага проучването на кандидата за участие в международни процедури на НАТО на ДАНС.

68. Държавна агенция „Национална сигурност“ извършва проучването при условията и по реда на глава VI, раздел VI от ЗЗКИ, глава VII от ППЗЗКИ и НОИГИС, Наредбата за условията и реда за допускане на български физически или юридически лица до участие в международни процедури на Организацията на Северноатлантическия договор (НАТО).

69. Държавната комисия по сигурността на информацията оказва необходимото съдействие на органите и организационните единици, прилагащи мерките за гарантиране на индустриалната сигурност.

СИГУРНОСТ НА КОМУНИКАЦИОННИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ (КИС)

КИС е балансирана система от технически *(включително комуникационни средства, устройства за защита на границата, криптографски средства и среда за разпространение на сигнала в границите на системата)* и програмни средства, методи, процедури и персонал, организирани за осъществяване на една или няколко от функциите по създаване, обработване, ползване, съхраняване и обмен на класифицирана информация в електронна форма. Комуникационната и информационната система може да е изградена и на основата на една или повече отделни работни станции, несвързани в мрежа.

1. ОСНОВНИ ПОНЯТИЯ

Законът за защита на класифицираната информация (ЗЗКИ, глава VI, раздел V, чл. 89 до 94а вкл.) постановява дефинирането на задължителни общи условия за сигурност на комуникационните и информационните системи (КИС) за работа с класифицирана информация в отделна наредба - *Наредбата за сигурността на комуникационните и информационните системи (НСКИС)*.

Задължителните общи условия за сигурност на КИС, в които се създава, обработва, ползва, съхранява и обменя класифицирана информация в електронна форма, включват определянето на:

- органите по сигурността на КИС;
- условията и реда за акредитиране на КИС;
- задължителните общи изисквания за сигурност на КИС.

В чл. 89 от ЗЗКИ ***сигурността на КИС*** се определя като система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в КИС.

Задължителните общи условия за сигурност на КИС обхващат компютърната, комуникационната, криптографската, физическата, документалната и персоналната сигурност, сигурността при свързване на КИС, сигурността на самата информация на всякакъв електронен носител и контрамерките по TEMPEST за защита от компрометиращи електромагнитни излъчвания.

Целта на прилаганата система от мерки е осигуряването на трите характеристики на класифицираната информация в КИС – конфиденциалност, интегритет и достъпност.

Осигуряването на ***„Конфиденциалност на информацията“*** е защитата ѝ от разкриване от неоторизиран субект.

Осигуряването на ***„Интегритет на информацията“*** е защитата й от промяна от неоторизиран субект.

Осигуряването на ***„Достъпност на информацията“*** е осигуряване на гарантиран и своевременен достъп на оторизираните субекти до нея.

При пълна или частична загуба, на която и да е от тези характеристики на класифицираната информация в КИС, се говори за ***„Компрометиране на сигурността на КИС“***.

2. ОРГАНИ ПО СИГУРНОСТТА НА КИС

Органи по сигурността на национално ниво

Държавна комисия по сигурността на информацията

Осъществява общ контрол по защита на класифицираната информация в КИС и върху процеса на акредитирането им.

Орган по акредитиране на сигурността на КИС (ОАС)

Орган по акредитиране на сигурността е Специализирана дирекция „Информационна сигурност” на ДАНС, която изпълнява следните задачи:

- дава препоръки и указания по сигурността на КИС;
- дава препоръки за стандарти и средства, които могат да се използват в КИС за защита на класифицираната информация;
- утвърждава документите по сигурността на КИС;
- извършва комплексна оценка на сигурността на КИС;
- издава сертификати за сигурност на КИС;
- определя условията, при които следва да се извърши допълнително или ново акредитиране на КИС;
- координира и контролира дейностите по TEMPEST и определя контрамерките за защита на КИС от компрометиращи електромагнитни излъчвания;
- провежда обучение на служители по сигурността на КИС;
- води регистър на сертифицираните КИС;
- отнема и прекратява действието на сертификати за сигурност на КИС при условията, посочени в глава шеста, раздел V от ЗЗКИ;
- одобрява механизмите за защита на границата на КИС;

- определя стандарти и списъци на одобрени продукти, които могат да се използват при избор на компоненти и устройства за защита на границата;
- определя конкретните условия и етапи за акредитиране на всяка КИС.

Органи по сигурността в организационната единица

Съгласно чл. 92 от ЗЗКИ ръководителят на организационната единица, в която се използват КИС за обработка на класифицирана информация, по предложение на служителя по сигурността на информацията (ССИ) назначава или възлага на назначени служители функции по контрола за спазване на изискванията за сигурността на КИС. Тези функции се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на КИС (чл. 47 от НСКИС).

Служител по сигурността на КИС

Служителят по сигурността на КИС (ССКИС):

- създава необходимата организация и осъществява контрол на сигурността на КИС в организационната единица;
- координира изготвянето на документите по сигурността на КИС и на изработените на тяхна основа експлоатационни документи по сигурността;
- съгласува изготвените документи по сигурността на КИС и ги предоставя на служителя по сигурността на информацията;
- координира обучението по сигурността на КИС;
- при случаи или съмнения за компрометиране на сигурността на КИС:

√ незабавно уведомява отговорните длъжностни лица по сигурността в ОЕ;
√ предприема действия за ограничаване или предотвратяване на вредите;
√ координира и участва в процеса по установяването и анализирането на обстоятелства, свързани с компрометиране сигурността на КИС;
√ докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОАС.

Служителят по сигурността на информацията може да изпълнява функциите на служител по сигурността на КИС.

Орган по развитие и експлоатация (ОРЕ)

Съставът на органа по развитие и експлоатация на КИС в организационната единица се определя със заповед на нейния ръководител и изпълнява следното:

- разработва и предлага изискванията за сигурност на КИС;
- изготвя документите по сигурността за всяка КИС;
- участва в подбора и тестването на техническите и програмните средства, и механизмите за сигурност, които ще се използват в КИС;
- осигурява изпълнението на изискванията за акредитиране на КИС;
- определя мерките за сигурност и границите на отговорност при осъществяване на връзки с други КИС;
- прави предложение за възлагане функции на администратор по сигурността на всяка КИС;
- организира обучение по сигурността в КИС и провежда обучение по сигурността на служителите, на които е възложена дейността по развитието, управлението или сигурността на КИС, включително администраторите по сигурността на КИС, както и на лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС;
- организира прилагането на одобрените мерки за сигурност в КИС;
- при междусистемна връзка на КИС извършва подбор на механизми за защита на границата;
- прави преглед на свързаната със сигурността документация - периодично или при предложени промени в техническото или в програмното осигуряване, връзките с други КИС, режима за сигурност, нивото на класификация на информацията или при други дейности, които могат да повлияят на сигурността на КИС, като за резултатите информира служителя по сигурността на КИС;
- участва заедно със служителя по сигурността на КИС в установяването и анализирането на обстоятелствата, свързани с компрометиране сигурността на КИС.

Администратор по сигурността

Администраторът по сигурността на КИС (АСКИС) е от състава на ОРЕ или друго звено в организационната единица, имащо отношение към съответната КИС. Той трябва да има разрешение за достъп до най-високото ниво на класифицирана информация в КИС.

Администраторът по сигурността на КИС:

- участва в изготвянето и актуализирането на процедурите за сигурност на КИС;
- изготвя експлоатационни документи по сигурността на КИС на базата на утвърдените процедури за сигурност;
- изпълнява възложените му процедури за сигурност в КИС;
- периодично информира потребителите по въпросите за сигурността на КИС;
- предоставя на потребителите достъп до ресурсите на КИС в съответствие с определените им права;
- осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в КИС, като:

  √ следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на КИС;

  √ следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в КИС;

  √ следи за правилното функциониране на механизмите за сигурност, включително на механизмите за защита на границата;

  √ управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата;

  √ осигурява резервиране и съхраняване на одитните записи в определените срокове;
- участва заедно със служителя по сигурността на КИС и с ОРЕ в установяването и анализирането на обстоятелствата, свързани с компрометиране на сигурността на КИС;
- може да изпълнява функциите на администратор по криптографска сигурност на информацията, ако в КИС се прилагат криптографски методи и средства, одобрени и регистрирани по реда на Наредбата по криптографската сигурност на класифицираната информация;

- уведомява служителя по сигурността на КИС за случаи или съмнения за компрометиране на сигурността на КИС;
- провежда обучение по сигурността на конкретната КИС на администраторите на КИС и потребителите.

При необходимост може да се определят повече от един администратор по сигурността на КИС, отговарящи за обособени нейни части, като един от тях се определя за администратор по сигурността на цялата КИС.

Функциите и задълженията на администратора по сигурността на КИС и на администратора на КИС трябва да са ясно разграничени, като не могат да се изпълняват от едно и също лице.

В органите на държавната власт, в които са обособени повече от една организационна единица, администраторът по сигурността на КИС може да е от състава на друга организационна единица в рамките на съответния орган.

Администратор на КИС

Администратор на КИС (АКИС) е лице:

- с възложени функции и предоставени права по системно, приложно, мрежово и/или друго администриране в съответната КИС;
- което има издадено разрешение за достъп до най-високото ниво на класификация за сигурност на информацията в КИС;
- което е преминало обучение в областта на сигурността на КИС.

Администраторът на КИС изпълнява задълженията, посочени в експлоатационните документи по сигурността на КИС и указанията на администратора по сигурността на КИС, свързани със сигурността й.

Администраторът на КИС уведомява администратора по сигурността на КИС за случаи или съмнения за компрометиране на сигурността и.

Потребители в КИС

Потребители на КИС могат да бъдат лица, които имат издадено разрешение за достъп до най-високото ниво на сигурност на информацията, с която имат право да работят в КИС, които са преминали обучение в областта на сигурността на КИС и на които са предоставени права за достъп до ресурсите на системата. Потребителите са длъжни да изпълняват задълженията, посочени в експлоатационните документи по сигурността и указанията на администратора по сигурността на КИС, както и да го уведомяват за случаи или съмнения за компрометиране сигурността на КИС.

3. ОБЩИ ИЗИСКВАНИЯ ЗА СИГУРНОСТ НА КИС

Системата от мерки за сигурност на КИС включва **технически, процедурни и организационни** мерки в областта на физическата, персоналната, документалната, комуникационната, криптографската, компютърната сигурност, контрамерките по TEMPEST, както и сигурността при свързване.

Физическа сигурност

Ресурсите на КИС се разполагат в зони за сигурност клас I или клас II. Прилаганите мерки за защита на тези зони съответстват на най-високото ниво на класификация на информацията в тях и се определят в Наредбата по чл. 78 от ЗЗКИ. Допуска се КИС, предназначени за работа с класифицирана информация, представляваща служебна тайна, да се разполагат в административни зони, като това не се отнася за критичното от гледна точка на сигурността оборудване (сървъри, комуникационни устройства и др.).

За критичните от гледна точка на сигурността места се вземат допълнителни мерки за защита (система за контрол на достъпа, видеонаблюдение, недопускане присъствието само на един служител в тях).

Персонална сигурност

Потребителите на КИС трябва да имат разрешение за достъп до най-високото ниво на класифицирана информация, с която имат право да работят, а служителите, на които е възложена дейността по развитието, управлението или сигурността на КИС, както и лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС – до най-високото ниво на класифицирана информация в КИС.

Всички потребители на КИС се допускат до работа само след успешно завършено обучение по сигурността на КИС.

Документална сигурност

Всички документи, съдържащи класифицирана информация в КИС, се идентифицират, маркират и контролират по подходящ начин. Начините за тяхното идентифициране, маркиране и контролиране се определят в документите по сигурността на конкретната КИС.

Извеждането на документи, съдържащи класифицирана информация, от сертифицирани КИС се извършва в зоните за сигурност, съгласно изискванията на ППЗЗКИ.

Пренос на документи, съдържащи класифицирана информация, от една КИС към друга се извършва само ако получателят е КИС, сертифицирана за

ниво на класификация на информацията, същото или по-високо от нивото на класификация на пренасяните документи.

Материалните носители за многократен запис на класифицирана информация, използвани в КИС, се маркират и регистрират в регистратура за класифицирана информация. Съхраняването и периодичният контрол на носителите се извършват в съответствие с утвърдените процедури за сигурност на КИС.

Материалите и записаната на хартиен носител информация (пароли, пин, кодове и др.), осигуряващи достъп до КИС или ресурси на КИС, се класифицират с ниво на класификация за сигурност на информацията, съответстващо на най-високото ниво на класификация на информацията, за която дават достъп в КИС, и се унищожават по ред, определен в документите по сигурността на конкретната КИС, а не по реда на ППЗЗКИ.

Преносими компютърни устройства, предназначени за класифицирана информация, се маркират като носители на такава информация и се разглеждат като КИС или част от КИС. Пренасянето им извън зоните за сигурност се извършва по реда на ППЗЗКИ.

Комуникационна и криптографска сигурност, контрамерки по TEMPEST

Комуникационната сигурност представлява система от мерки за сигурност, прилагани с цел защита на класифицираната информация от нерегламентиран достъп при нейното пренасяне по комуникационни системи и включва защита с криптографски методи и средства, контрамерки по TEMPEST и защита при пренасяне на информацията в рамките на зоните за сигурност.

Комуникационните средства, организирани за пренос на класифицирана информация, включително при междусистемна връзка, трябва да осигуряват механизми за:

- надеждна и защитена идентификация и автентификация на изпращача и на получателя на информацията, които да се извършват преди началото на преноса на информацията;
- осигуряване на конфиденциалност, интегритет и достъпност на пренасяната информация;
- потвърждаване получаването на информацията.

В КИС не се допуска безжичен пренос на класифицирана информация, освен в случаите, когато е защитена с одобрени по реда на Наредбата за криптографската сигурност на класифицираната информация криптографски средства.

За защита на класифицирана информация в КИС се прилагат само криптографски средства, одобрени по реда на Наредбата за криптографската сигурност на класифицираната информация.

Форма на информация, получена чрез обработка на класифицирана информация с одобрени криптографски средства, не представлява класифицирана информация по смисъла на ЗЗКИ.

Комуникационните и информационните системи, предназначени за класифицирана информация с ниво „Поверително“ и по-високо, трябва да са осигурени с контрамерки по TEMPEST, които съответстват на най-високото ниво на класификация на информацията в КИС.

Контрамерките по TEMPEST включват:

- определяне на защитеността на работните помещения и съоръжения, в които ще се разполага техническо оборудване на КИС, по отношение на затихването на електромагнитните вълни;
- изпълнение на изискванията към техническото оборудване на КИС по отношение на максимално допустимите нива на компрометиращи електромагнитни излъчвания;
- изпълнение на изискванията при разполагане, инсталиране и захранване на КИС;
- допълнителни мерки съобразно спецификата на конкретната КИС.

Във всяка организационна единица, в която се експлоатират или се предвижда да се въвеждат в експлоатация криптографски средства за защита на класифицираната информация, с писмена заповед на нейния ръководител се определят служители, изпълняващи функции по криптографската сигурност: **служител по криптографската сигурност, администратор по криптографската сигурност и потребители на криптографски средства**.

Служителят по сигурността на информацията може да изпълнява функциите на служител по криптографската сигурност в организационната единица.

Редът за използване на криптографски методи и средства за защита на класифицираната информация се регламентира в Наредбата за криптографската сигурност на класифицираната информация.

В тази наредба като органи за криптографска сигурност на национално ниво се определят:

- ДКСИ – осъществява общо ръководство и контрол на дейностите по криптографска сигурност.

- ДАНС – орган по криптографската сигурност (ОКС) на Република България.

Минимални изисквания за компютърна сигурност

- еднозначна идентификация и автентификация на потребителя, които трябва да предхождат всички останали негови действия в КИС;
- контрол на достъпа по преценка - предоставяне на права за достъп до обектите на КИС на базата на идентификацията на потребителя или неговата принадлежност към потребителска група; правата за достъп се предоставят само от администратора по сигурността на конкретната КИС или от упълномощени потребители; механизмите за контрол трябва да осигуряват възможност за разделяне на потребителите и за достъп до информацията според принципа „необходимост да се знае“;
- непрекъснат и синхронизиран по време запис на събития, свързани със сигурността на конкретната КИС (одитни записи); записват се действия, свързани с контрола на достъпа (включително неуспешни опити за достъп), действия по отношение на обекти и действия на оторизирани субекти, влияещи върху сигурността; информацията в одитните записи трябва да осигурява възможност за установяване на действия на отделните субекти, свързани със сигурността на КИС;
- защита на одитните записи, свързани със сигурността, срещу неоторизиран преглед, промяна и изтриване;
- обработка на обекти на конкретната КИС, така че при следващото им разпределяне към субект той да не може да установи предишното им съдържание или да получи права за достъп на използвалите ги преди това субекти;
- актуална защита от вредни програмни средства.

За осигуряване на минималните изисквания за сигурност се реализират програмни и технически механизми, спрямо които трябва да се осъществява конфигурационен контрол и които трябва да са защитени от нерегламентиран достъп.

4. АКРЕДИТИРАНЕ НА КИС

Съгласно чл. 91, ал. 2 от ЗЗКИ не се допуска създаване, обработване, съхраняване и пренасяне на класифицирана информация в КИС, на които не е издаден сертификат за сигурност.

Този сертификат се издава от Органа по акредитиране на сигурността на КИС (ОАС) при успешно завършена процедура по акредитиране и гарантира, че съответната КИС е одобрена да функционира в конкретната среда на експлоатация и при приемливо ниво на риска, въз основа на приложен одобрен комплекс от мерки за сигурност.

Процедура по акредитиране на КИС

Процедурата по акредитиране на КИС започва от етапа на нейното проектиране и протича при тясно взаимодействие между ОРЕ в организационната единица и ОАС за уточняване на изискванията за сигурност към изгражданата КИС. Тя е описана в хронологичен ред в НСКИС.

Процесът на акредитиране завършва с комплексна оценка от комисия, която включва:

- проверка на документите по сигурността;
- проверка на изпълнението на предвидените мерки за сигурност

При необходимост от използване на криптографски средства, процедурата по тяхното въвеждане в експлоатация трябва да предхожда процедурата по акредитиране на КИС.

В Глава VII от НСКИС е регламентиран редът за отнемане и прекратяване на сертификати за сигурност на КИС.

Документи по сигурността на КИС

Документите по сигурността, необходими за извършване на акредитирането на всяка КИС, са:

- специфични изисквания за сигурност (СИС);
- процедури за сигурност, изготвени на основата на СИС.

При случай на издаване на сертификат за сигурност за обособена част от КИС, ОАС може да изисква допълнителни СИС и/или процедури за сигурност за нея.

Документите по сигурността се класифицират по реда на ЗЗКИ и ППЗЗКИ.

Специфични изисквания за сигурност (СИС)

Задължителните специфични изисквания и процедури за сигурност на КИС във всяка организационна единица се определят от ръководителя на организационната единица по предложение на служителя по сигурността на

информацията. Тези изисквания и процедури подлежат на утвърждаване от Органа по акредитиране на сигурността на КИС.

Специфичните изисквания за сигурност се основават на резултатите от анализа на риска, който се документира в тях. Формулирането им започва в етапа на проектиране на КИС, като се детайлизират в процеса на разработване и изграждане.

В етапа на експлоатация те определят границите на отговорност на ОРЕ и на останалия състав, действащ в локалната и глобалната среда за сигурност.

При прекратяване на експлоатацията се ползват за определяне на действията, които трябва да се предприемат с цел запазване сигурността на информацията.

В своя завършен вид СИС определят как се постига, управлява и контролира сигурността на КИС и служат за основа при формулирането на процедурите за сигурност.

Процедури за сигурност (ПС)

Процедурите за сигурност представляват подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на мерките за сигурност от СИС.

Всяка процедура трябва да съдържа следните елементи:

- лице, което изпълнява процедурата;
- описание на последователността на действията за изпълнение на процедурата;
- период на изпълнение на процедурата;
- лице, отговорно за контрола по изпълнението на процедурата.

Процедурите за сигурност се оформят като документ, състоящ се от раздели, съдържащи мерки по всички видове сигурност, действия при критични ситуации, управление на конфигурацията и отговорности и задължения на потребителите.

Сигурност при свързване на КИС

Чл. 94 от ЗЗКИ допуска реализирането на междусистемна връзка на КИС, предназначени за класифицирана информация до ниво „Секретно“ включително, с други КИС за класифицирана информация със същото или различно ниво на класификация, както и към информационни системи от затворен тип при условията, посочени в Наредбата за сигурността на КИС. В същия член са посочени и случаите, в които такава връзка не се допуска.

В чл. 94а от ЗЗКИ е посочено кога се разрешава осъществяването на междусистемна връзка на КИС.

В Глава шеста от НСКИС са регламентирани както следва:

- общите изисквания при свързване на КИС;
- минималните изисквания към механизмите за защита на границата;
- планирането, одобряването и въвеждането в експлоатация на механизми за защита на границата при междусистемна връзка;
- изискванията за сигурност при осъществяване на междусистемна връзка към информационни системи от затворен тип и към системи с публичен достъп

5. ЗАКЛЮЧЕНИЕ

Масовото използване на КИС за работа и пренос на класифицирана информация и съсредоточаването на големи масиви от данни и документи в тях ги прави прицелна точка на непрекъснато нарастващ брой заплахи.

Осигуряването на адекватни мерки за защита на класифицираната информация в КИС е задача с приоритетно значение за всяка организационна единица, в която се експлоатират.

За решаването на тази задача са необходими както добро познаване на нормативните изисквания и точно прилагане на мерките за сигурност, така и ангажираност и обединени усилия от страна на ръководния и изпълнителския персонал.

КОНТРОЛ НА ДЕЙНОСТТА ПО ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Нерегламентирано разкриване или разгласяване на информация, документ или материал, които носят гриф за сигурност, би могло да увреди в различна степен интересите на държавата и нейната сигурност. Затова контролната дейност е изключително важна за осигуряване на законосъобразно и устойчиво функциониране на Националната система за защита на класифицираната информация.

За да бъде последователно провеждана държавната политика в областта на защитата на класифицираната информация трябва непрестанно да се отчита как се прилагат нормативните разпоредби и указанията на компетентните органи по отношение дейността на органите и прилаганите мерки за защита. Контролът е най-сигурното средство непрестанно да се следи актуалното състояние на установената в закона система за защита на класифицираната информация, да се неутрализират заплахите, рисковете и вредите за националната сигурност и обществените интереси.

Същност на контрола по защитата на класифицираната информация

Контролът е процес, в който определени в закона органи и длъжностни лица установяват в каква степен създадените материални условия и организацията на дейността в организационните единици, както и поведението на лицата с разрешение за достъп до класифицирана информация съответстват на нормативните разпоредби и указанията на компетентните органи.

Проверките за осъществяване на пряк контрол се извършват само от определените в закона длъжностни лица, на които са възложени контролни функции в областта на защитата на класифицираната информация. За целта те разполагат с компетентност – оправомощени са да преценяват наличие или липса на необходимите условия за защита на класифицираната информация и да съставят актове за установяване на нарушения. Контролиращите органи осъществяват своята дейност с правно регламентирани средства, с помощта на които се констатира и/или предотвратява нерегламентиран достъп до класифицирана информация и се гарантира нейната защита.

Проверките се изразяват в съвкупност от констатации, въз основа на които се дават препоръки и/или конкретни предписания за усъвършенстване и ефективно функциониране на изградените в организационните единици системи за защита на класифицираната информация.

Основното предназначение на контрола е превенцията за недопускане на нерегламентиран достъп до класифицирана информация. Посредством контрола се установяват пропуски, недостатъци и нарушения в работата на организационните единици и се посочват начините за осигуряване на надеждна защита на класифицираната информация. За целта контролиращите органи проверяват доколко ефективно ръководителите на организационните единици, служителите по сигурността на информацията и завеждащите регистратури създават условия за опазване на класифицираната информация и законосъобразно ли боравят с нея всички лица, които имат разрешение за достъп.

Същевременно чрез контрола се оказва методическа помощ на организационните единици, длъжностните лица по сигурността на информацията и другите лица с достъп до класифицирана информация. Проверките по прекия контрол дават възможност за анализ и компетентна оценка относно законосъобразността и ефективността в работата с класифицирана информация и нейната защита, организирането и провеждането на превантивна дейност за недопускане на нерегламентиран достъп.

Технологията на проверката е деликатен процес, който изисква време за свързване с проверяваната организационна единица и изясняване на осъществяваната в нея дейност по защитата на класифицираната информация. При осъществяване на проверка по прекия контрол се установява:

– съществуват или отсъстват факти на нерегламентиран достъп до класифицирана информация в проверяваната организационна единица;

– дали установената фактическа обстановка компрометира превантивната дейност и дава възможност за евентуален нерегламентиран достъп до класифицирана информация в тази организационна единица;

– длъжностните лица по защита на класифицираната информация и всички останали служители с разрешение за достъп изпълняват ли изискванията на Закона за защита на класифицираната информация и на актовете по неговото прилагане относно отделните видове защита на класифицираната информация.

В резултат на констатациите се дават препоръки и конкретни предписания за отстраняване на допуснатите пропуски и недостатъци. При установени нарушения контролиращият орган изпраща писмено предупреждение, подканващо писмо и след това може да пристъпи към търсене на административнонаказателна отговорност (или да сезира компетентните правораздавателни органи за търсене на наказателна отговорност в случай, че има данни за извършено престъпление). Следва да се отбележи, че налагането

на наказания не е самоцел и масова практика на контролиращите органи, а крайна мярка.

Нормативна уредба

Нормативната уредба на контрола се съдържа на първо място в чл.12 от Закона за защита на класифицираната информация (ЗЗКИ), обн. ДВ, бр.45 от 30 април 2002 г. с последно изм./доп. ДВ, бр.17 от 26 февруари 2019 г. и в редица разпоредби на Правилника за прилагане на ЗЗКИ (ППЗЗКИ), приет с ПМС № 276/02.12.2002 г. с последно изм./доп. ДВ, бр. 17 от 26 февруари 2019 г.

Наредбата за реда за извършване на проверките и осъществяване на пряк контрол за защита на класифицираната информация (НРИПОПКЗКИ), приета с ПМС № 44 от 21 февруари 2003 г. с последно изм./доп. ДВ, бр. 44 от 09 май 2008 г., определя реда за извършване на проверките по чл.12 от ЗЗКИ (проверките по прекия контрол).

Подзаконовите нормативни актове по отделните видове защита на класифицираната информация установяват системата от мерки, способи и средства, които организационните единици са задължени да прилагат за защита на създаваната, обработваната, предаваната, приеманата и съхраняваната в тях класифицирана информация.

Пряко отношение към контрола върху дейността по защита на класифицираната информация има и Законът за Държавна агенция „Национална сигурност” (ЗДАНС), който урежда устройството и дейността на Държавната агенция „Национална сигурност” (ДАНС), статута на нейните служители и правомощията на органите й. Сред дейностите, извършвани от ДАНС законът поставя и защитата на националната сигурност от посегателства, свързани с нарушаване функционирането на Националната система за защита на класифицираната информация.

Органи по контрола

ЗЗКИ възлага на Държавната комисия по сигурността на информацията (ДКСИ) не само да организира, осъществява и координира дейността по защита на класифицираната информация, но и да контролира тази дейност. ДКСИ е орган по общия контрол.

Пряк контрол по защита на класифицираната информация и по спазването на законовите разпоредби в тази област се осъществяват от служители на ДАНС, на които законът предоставя определени права.

Текущият контрол в организационната единица се извършва всекидневно от служителя по сигурността на информацията – основното длъжностно лице по спазването на изискванията на ЗЗКИ във връзка със защитата на класифицираната информация.

ДКСИ и ДАНС са отговорните органи в областта на контрола върху защитата на класифицираната информация в национален мащаб. Между тях има определено от законът разделение на функциите, но същевременно и взаимодействие.

В качеството си на национален орган, който осъществява политиката на Република България по защитата на класифицираната информация, ДКСИ притежава обща компетентност по защитата на националната класифицирана информация. При изпълнението на възложените й от закона дейности ДКСИ издава задължителни указания до задължените по закона субекти, осъществява методическо ръководство спрямо служителите по сигурността на информацията и осигурява еднаква защита на класифицираната информация.

ДКСИ е отговорният орган по организирането и контролирането на изпълнението на задълженията за защита на класифицираната информация, съдържаща се в международните договори, по които Република България е страна и осъществява редица функции в тази област.

На ДКСИ е възложена и функцията да осъществява също така общ контрол по защитата на класифицираната информация, която се създава, съхранява, обработва и предава в комуникационни и информационни системи.

В изпълнение на разпоредби на ЗЗКИ и ЗДАНС, като специализиран орган към Министерския съвет за изпълнение на политиката по защита на националната сигурност и в качеството си на основен компетентен орган в областта на прекия контрол, ДАНС извършва проверки с цел недопускане на вреди в резултат на компрометиране на класифицираната информация и възпрепятстване на нейната ефективна защита. ДАНС контролира и дейността по защита от паразитни електромагнитни излъчвания на техническите средства, обработващи, съхраняващи и пренасящи класифицирана информация.

Контролиращите органи, които извършват проверките по прекия контрол върху защитата на класифицираната информация и по спазването на законовите разпоредби в тази област, са служители на ДАНС, определени с писмена заповед на председателя на ДАНС, снабдени със служебни карти по образец. Редът, по който те извършват проверките, е определен в посочената по-горе Наредба за реда за извършване на проверките и осъществяване на пряк контрол за защита на класифицираната информация.

Цел на контрола

Основната цел на контрола е установяване на актуалното състояние на системата за защита на класифицираната информация, която е изградена и действа в организационната единица – обект на контрол.

Първостепенно място в дейността на контролиращите органи по време на проверката заема установяването на недостатъци по отношение на мерките за сигурност. Особено внимание се обръща на превенцията на нарушенията, които биха могли да предизвикат отслабване на защитата, изгубване или дори нерегламентиран достъп до класифицирана информация.

За да се констатира спазват ли се разпоредбите на ЗЗКИ, ППЗЗКИ и другите подзаконови нормативни актове в тази област, при проверката трябва да се установи познава ли се материята по защита на класифицираната информация, служителите с разрешение за достъп до такава информация подготвени ли са своевременно и ефективно да отстраняват всички рискове и опасности, чието проявление би довело до нерегламентиран достъп. Следва да се установи също така дали се изпълняват нормативните изисквания по отделните видове сигурност и, в крайна сметка, създадени ли са всички необходими условия да не се допусне възникването на заплахи за сигурността на класифицираната информация в проверяваната организационна единица.

Обект и обхват на контрола

Обект на проверките по прекия контрол са организационните единици и всички техни поделения, подразделения, структурни звена и обособени части. На контрол подлежат и всички лица от проверяваната организационна единица (или от друга организационна единица, свързана с проверяваната), отговорни за планирането, организирането, ръководството, контрола и спазването на мерките за защита на класифицираната информация. Разбира се, проверките не могат да не обхванат средствата, способите и средата, които се използват за създаване, обработка, съхраняване, предаване и защита на класифицираната информация.

Проверките по прекия контрол обхващат всички организационни единици, включително структурите на въоръжените сили и организационните единици, които създават, обработват и съхраняват класифицирана информация или пренасят документи и/или материали, съдържащи класифицирана информация, която засяга въоръжените сили, по отношение защитата на тази информация.

На контрол подлежат всички видове защита (сигурност) на класифицираната информация – физическа, документална, персонална, криптографска, на КИС, индустриална. Оценяват се от гледна точка на законосъобразност и ефективност съществуващите към момента на проверката материални и организационни условия за защита на класифицираната информация, както и действащата в организационната единица практика по видовете защита.

При извършване на проверките по прекия контрол за контролиращите органи е важно да установят задоволително ли е състоянието на мерките за защита на класифицираната информация в проверяваната организационна единица. Съществено значение има констатацията дали се познават и прилагат разпоредбите на ЗЗКИ, ППЗЗКИ и другите подзаконови нормативни актове по отношение на работата с класифицирана информация и нейната защита. Непознаването на материята се отразява особено неблагоприятно в резултатите от проверката.

Неспазване на нормативните изисквания най-често се констатира в организационните единици, в които не се провежда обучение и лицата с достъп имат ниско ниво на подготовка за работа с класифицираната информация и нейната защита. Някои служители по сигурността на информацията не провеждат редовно първоначални и текущи обучения по защита на класифицираната информация, а други провеждат обучението формално и това не дава необходимия ефект.

Значително по-високо е равнището на подготовка на работещите с класифицирана информация или отговорни за нейната защита длъжностни лица в организационните единици, които се възползват от организираните и провежданите от ДКСИ в нейния Учебен център в град Банкя, както и „на място“ в организационните единици, курсове за първоначално, текущо и тематично обучение. Практиката показва, че включването и на ръководителите на организационни единици в курсове за обучение дава положителен ефект, но за съжаление това не се случва често. Посредством провежданото от нея обучение ДКСИ изпълнява и възложеното й от закона задължение да осигурява еднаквата защита на класифицираната информация.

За контролиращите органи е важно ръководителят на проверяваната организационна единица определил ли е вътрешни правила при спазване на законовите изисквания за правилното определяне на нивото на класификация, както и за неговата промяна или премахване. Тези правила следва да отчитат спецификата съобразно сферата на дейност на организационната единица и нейните структурни звена, ако има такива, и да спомагат за предотвратяване

настъпването на вреди от нерегламентиран достъп до създаваната и съхранявана в организационната единица класифицирана информация.

Съдържание на проверките по прекия контрол

Контролиращите органи извършват дейността по прекия контрол, като строго се придържат към изискванията на закона. Но проверките не могат да бъдат формални, тъй като състоянието на всяка организационна единица е различно. Важни са практическите решения, а не прилагането на схема. Подходът на контролиращите органи е конкретен за всяка проверявана организационна единица. В ДАНС е създадена система от критерии за осъществяване на проверките по прекия контрол. Организационните единици се степенуват по важност от гледна точка на обема създавана и получавана класифицирана информация, нейната важност за националната сигурност и възможностите за нерегламентиран достъп.

Проверките по прекия контрол се изразяват в съвкупност от действия, мерки и препоръки, предназначени да осигурят ефективното функциониране и усъвършенстване на системите за защита на класифицираната информация. Анализират се рисковете, опасностите и заплахите за сигурността на класифицираната информация в организационната единица – обект на контрол. Установява се не само наличие или липса на нерегламентиран достъп до класифицирана информация, но и съществуването на опасности, рискове и заплахи за нерегламентиран достъп.

При констатирани нарушения контролиращите органи дават препоръки и/или конкретни задължителни предписания, които трябва да се изпълнят от длъжностните лица в указания срок. При неизпълнение на задължителните предписания и неспазване на указаните срокове или в случай на съществени нарушения, контролиращите органи могат да налагат санкции. Изпраща се писмено предупреждение, подканващо писмо и едва тогава – при условията и по реда на закона – се пристъпва към търсене на административнонаказателна или наказателна отговорност, в зависимост от конкретния случай.

Всички тези мерки са насочени към постигане на законосъобразно и ефективно функциониране на организационната единица чрез поддържане на такива условия и ред на работа при създаването, обработката, предаването, приемането, съхраняването и унищожаването на класифицираната информация, които осигуряват предоставяне само на регламентиран достъп до такава информация и спазване на принципа „Необходимост да се знае“.

Права на контролиращите органи и ограничения при проверките

За да могат контролиращите органи успешно да изпълняват възложените им задачи по прекия контрол, законът им предоставя определени права.

Служителите, определени с писмена заповед на председателя на ДАНС като контролиращи органи, които осъществяват пряк контрол по защитата на класифицираната информация и спазването на законовите разпоредби в тази област, на първо място имат право на достъп до обектите и помещенията в проверяваната организационна единица, като могат да извършват оглед на тези обекти и помещения. Контролиращите органи имат право на достъп до документите за организацията по защитата на класифицираната информация, както и до комуникационните и информационните системи на организационната единица и свързаните с тях информационни системи. Целта е да се установи надеждността на защитата.

Контролиращите имат право при необходимост да изискват писмени или устни обяснения от ръководителите и служителите в проверяваната организационна единица. При отказ на ръководителя и/или служителите да дадат исканите обяснения, контролиращите органи съставят протокол.

При необходимост контролиращите органи имат право да получават информация от други организационни единици във връзка с организационната единица – обект на контрол, както и да изискват обяснения от техните ръководители и служители за дейността по създаването, обработването, съхраняването и предоставянето на класифицираната информация във връзка с извършваната проверка.

В зависимост от направлението на проверката, контролиращите органи могат да получат информация от други организационни единици. При необходимост могат да изискват обяснения и от техни ръководители и служители относно дейността по създаването, обработването, съхраняването и предоставянето на класифицирана информация във връзка с извършваната проверка в организационната единица, която е обект на контрол.

Когато се окаже, че са необходими специални знания за изясняване на обстоятелства във връзка с извършваната проверка, контролиращите органи могат да привличат експерти.

Контролиращите органи могат да дават конкретни предписания във връзка със защитата на класифицираната информация.

Какво може да се установява и каква информация представлява интерес при проверките по прекия контрол? В хода на проверката се събира информация за създадената в контролираната организационна единица система

за защита на класифицираната информация. Тази информация може да се използва за:

– анализ и оценка за актуалното състояние на системата за защита на класифицираната информация и заплахите към нея;

– идентифициране, отстраняване и предотвратяване на рисковите фактори, които биха довели до нерегламентиран достъп до класифицирана информация;

– изготвяне на предписания до организационната единица – обект на контрол за предприемане на необходимите организационно-технически мерки за подобряване на функционалността и сигурността на системата за защита на класифицираната информация;

– реализиране на административнонаказателна или наказателна отговорност.

Информацията, която е събрана по време на проверките по прекия контрол може да бъде използвана и предоставяна само за целите на защитата на класифицираната информация.

Видове проверки

Проверките по прекия контрол се различават по обхват и по планиране.

Според обхвата проверките са общи – когато се проверяват всички видове защита на класифицираната информация, или тематични – когато проверките се ограничават до отделни видове защита на класифицираната информация. По преценка на контролиращия орган може да се премине от тематична към обща проверка, като постфактум се представя съответно коригирана заповед.

Многобройни (около 2150) разнообразни структури в страната са регистрирани и съществуват като организационни единици при условията и по реда на ЗЗКИ. Това са централни органи на държавната власт, органи на изпълнителната власт и нейната местна администрация, органи на съдебната власт, органи на местното самоуправление, определени търговски дружества. Видно е, че проверките по прекия контрол не биха могли да се провеждат без предварително планиране в зависимост от анализа на средата в организационните единици и заплахите за класифицираната информация.

Плановите проверки могат да бъдат с предварително уведомяване на организационната единица – обект на контрол (преди извършването на проверката се изпраща уведомително писмо до ръководителя на организационната единица), или без предварително уведомяване. Плановите общи и тематични проверки се провеждат в рамките на работното време на проверяваната организационна единица.

Инцидентни (непланови) проверки се провеждат при необходимост – по решение на контролиращия орган или когато той е уведомен от дадената организационна единица за опасност от възникване или в случай на вече възникнал нерегламентиран достъп до класифицирана информация. Основание за такава проверка може да бъде и получен от контролиращия орган сигнал от друг достоверен източник за опасност от възникване или за вече осъществен нерегламентиран достъп до класифицирана информация.

След започване на инцидентна проверка на това основание контролиращите органи незабавно уведомяват писмено председателя на ДАНС за започналата проверка, като посочват основанието за нея и могат да предложат допълнителни мерки за защита на класифицираната информация, която е обект на нерегламентиран достъп. Председателят на ДАНС или определено от него длъжностно лице се произнася по предприетите действия и може да даде допълнителни указания.

Ред за извършване на проверките по прекия контрол

Проверките по прекия контрол се извършват по реда на Наредбата за реда за извършване на проверките и осъществяване на пряк контрол за защита на класифицираната информация, в съответствие с изискванията на ЗЗКИ.

За да започне проверка по прекия контрол, председателят на ДАНС или определено от него длъжностно лице (обикновено заместник председател на ДАНС) със своя писмена заповед определя:

1. организационната единица – обект на проверката;
2. обхвата и продължителността на проверката;
3. председателя и членовете на комисията по проверката в случаите, когато има сформирана такава комисия и привлечените при необходимост експерти;
4. реда за докладване на резултатите от проверката;
5. материално-техническото и финансовото осигуряване на проверката.

След издаването на тази заповед, ръководителят на проверката изготвя план, който се утвърждава от председателя на ДАНС или определено от него длъжностно лице. Освен съдържащите се в писмената заповед идентифициращи елементи и материално-техническите условия на проверката, планът съдържа още:

– подлежащите на проверка видове защита на класифицираната информация (в случай на тематична проверка);

– проблемите, които изискват специално внимание;

– способите и средствата за извършване на проверката;

– направленията, по които ще действат експертите;

– реда, по който ще се докладват резултатите от проверката.

При извършването на проверка контролиращите органи се легитимират със своята служебна карта по образец, издадена от председателя на ДАНС. След това ръководителят на организационната единица – обект на контрол е длъжен да предприеме действия за даване на възможност на контролиращите органи да осъществят проверката.

Задължения на организационната единица при проверка

Нормативните разпоредби установяват съответствие между правата на контролиращите органи и задълженията на ръководителя на проверяваната организационна единица.

Какви са задълженията на ръководителя на организационната единица и другите длъжностни лица по защитата на класифицираната информация при извършването на проверка по прекия контрол?

На първо място ръководителят на проверяваната организационна единица е длъжен да осигури на контролиращите органи достъп до всички обекти, помещения, документи и материали, свързани с организацията по защита на класифицираната информация, както и до КИС за създаване, съхраняване, обработка и пренос на такава информация. Ръководителят трябва да осигури присъствието на всички лица от организационната единица, които контролиращите посочат.

Както вече беше посочено по-горе, ръководителят и служителите в проверяваната организационна единица или от други организационни единици във връзка с извършваната проверка са длъжни да дадат писмени или устни обяснения при изискване от контролиращите. При отказ да се дадат изисканите обяснения, контролиращите съставят протокол, който заедно с доклада и другите събрани в хода на проверката материали и експертни мнения формира сбор от документи за резултатите от проверката.

Резултати от проверката

Всяка проверка завършва с определени резултати, които могат да се оценят като положителни (позитивни) или отрицателни (негативни).

Положителни са резултатите, когато в хода на проверката се установи съответствие на актуалното състояние на проверяваната организационна единица с изискванията на закона и не се констатира нерегламентиран достъп до класифицирана информация.

При установяване на пропуски или нарушения, обосноваващи отрицателни резултати от проверката, се дават препоръки и/или задължителни предписания за отстраняване на конкретни недостатъци. Неспазването на определените срокове за изпълнение на препоръките или задължителните предписания, както и констатирането на нерегламентиран достъп до класифицирана информация, са основания за налагане на предвидени в закона санкции.

Проверката приключва с изготвянето на доклад, чието съдържание отразява в хронологичен ред всички действия на контролиращите органи. Посочват се техните заключения относно резултатите от проверката, събраните в хода на проверката документи и материали, както и номерата на констативните протоколи или административните актове в случай, че такива са съставени. Докладът, събраните материали и експертни мнения формират сбор от документи. Въз основа на сбора от документи контролиращите органи изготвят и изпращат до проверената организационна единица уведомително писмо за резултатите от проверката.

В резултат на констатациите при проверката контролиращите органи дават препоръки и/или предписания за отстраняване на пропуските и недостатъците във връзка със сигурността на информацията. При установени нарушения се изготвят и изпращат до проверената организационна единица предписания във връзка със сигурността. По преценка на контролиращите се предприемат мерки за търсене на административнонаказателна или наказателна отговорност. Изпраща се писмено предупреждение, подканващо писмо и едва след това, по преценка на контролиращия орган, се пристъпва към процедурата за налагане на административно наказание.

Важно задължение на контролиращите органи след приключване на проверката е изготвянето и изпращането на доклад до ДКСИ. Въз основа на тези доклади във всеки момент може да се състави цялостна картина за състоянието на Националната система за защита на класифицираната информация. За откритите проблеми, които налагат изменения в общата

политика за сигурност на класифицираната информация, контролиращите изготвят информация, която изпращат до ДКСИ и до службите за сигурност.

Контрол върху регистратурите

Разпоредбите на чл.129 и сл. от ППЗЗКИ възлагат на ръководителят на организационната единица, на служителят по сигурността на информацията и на контролиращите органи на ДАНС да осъществяват текущ и периодичен контрол върху цялостната дейност и състоянието на регистратурите.

Текущият контрол на регистратурите се организира от ръководителя на организационната единица и служителя по сигурността на информацията. Той включва планови и извънпланови, годишни, частични и цялостни проверки.

Периодичният пряк контрол на регистратурите се осъществява от контролиращите органи на ДАНС по реда на Наредбата за реда за извършване на проверките и осъществяване на пряк контрол за защита на класифицираната информация.

Ръководителят на организационната единица всяка година със заповед назначава комисия за извършване на годишна проверка на регистратурата. При нея фактическата наличност на материалите се сверява по отчетните документи, а също така и с актовете за унищожаване на материали за текущата година и с описите за получаване и изпращане на материали. За резултатите от тази проверка комисията изготвя протокол, който се предоставя както на служителя по сигурността на информацията, така и на ДАНС.

Следва да се има предвид, че цялостна проверка на регистратурата задължително се извършва в два случая:

– при смяна на завеждащия регистратурата, или

– при констатиране на нерегламентиран достъп до заведен в същата регистратура материал-носител на класифицирана информация.

При смяна на завеждащия регистратурата всички съдържащи класифицирана информация материали се предават/приемат с комисия, назначена със заповед на ръководителя на организационната единица.

Служителят по сигурността на информацията, който е длъжен да следи за спазването на изискванията на закона във връзка със защитата на класифицираната информация в организационната единица, извършва периодични проверки на отчетността и движението на материалите и документите, съдържащи класифицирана информация.

Извън горепосочените случаи, съгласно изричната разпоредба на чл.132, ал.1 от ППЗЗКИ, завеждащият регистратура извършва ежемесечни вътрешни проверки на регистратурата, като проверява:

– наличността на изработените и получените материали, съдържащи класифицирана информация;

– наличността на материали с класифицирана информация, които се намират в служителите в организационната единица с разрешение за достъп;

– воденето на отчетните документи;

– състоянието на регистратурата.

За резултатите от всяка такава проверка завеждащият регистратура изготвя протокол, който предоставя на служителя по сигурността на информацията. Не са установени изисквания за формата на този протокол, но той би следвало да отразява резултатите от проверката съгласно посочения по-горе неин обхват. Правната норма не оставя съмнение, че ежемесечна проверка се извършва и за нея се съставя протокол, независимо дали през изминалия месец в регистратурата има или няма постъпили, изпратени или получени документи и материали с класифицирана информация. Тази разпоредба на ППЗЗКИ е императивна, т.е. задължителна за изпълнение от завеждащия регистратура и нейното неспазване е предпоставка за налагане на санкции. При проверка по прекия контрол служителят по сигурността на информацията трябва да представи на контролиращия орган протоколите за ежемесечните проверки на завеждащия регистратурата.

Контрол за надеждност на лицата с достъп до класифицирана информация

Контролът за надеждност на лицата, получили достъп до класифицирана информация, се осъществява от компетентните органи (ДАНС и другите служби за сигурност) чрез използване на предвидените в ЗЗКИ методи и средства.

Контролът в тази област се осъществява чрез системата от принципи и мерки, която компетентните органи прилагат спрямо лицата с достъп до класифицирана информация с цел гарантиране на тяхната надеждност с оглед защитата на класифицираната информация. На първо място тук се отчита спазването на принципа „необходимост да се знае“, т.е. гарантирането на достъп до съответната класифицирана информация само на лицата, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

В изпълнение на задачите си по контрола, като си взаимодействат помежду си, ДАНС и другите служби за сигурност имат право да прилагат и използват разузнавателни способи при условията и ред, определени със закон. Те могат, също така, да използват данни от своите информационни масиви за физически и юридически лица – обект на проучване, както и да съхраняват

данните, получени в процеса на проучване на физически лица и на кандидати – физически и юридически лица, при сключване и изпълнение на договор, свързан с достъп до класифицирана информация. Съгласно действащите закони службите за сигурност имат право да съхраняват и данни за случаи на нерегламентиран достъп до класифицирана информация. Съгласно разпоредба на ЗЗКИ те могат да получават необходимата информация от държавните органи, органите на местното самоуправление, физически и юридически лица.

Важно е да се знае, че контролът за надеждност на лицата, получили достъп до класифицирана информация, се осъществява от компетентните органи от момента на започване на процедурата по проучване на лицето и продължава, докато това е необходимо, съгласно сроковете за защита на класифицираната информация.

Контрол по изпълнението на задълженията за опазване на класифицираната информация по международни договори, по които Република България е страна

ЗЗКИ възлага на ДКСИ организацията, контрола и отговорността по изпълнението на задълженията за защита на класифицираната информация, която се съдържа в международните договори, по които Република България страна.

Под ръководството на ДКСИ организацията и контролът на дейностите по защита на чуждестранната класифицирана информация гарантират изпълнението на задълженията на Република България, които произтичат от нейното членство в НАТО и Европейския съюз и сключените международни договори. Освен по многостранните международни договори за присъединяване към НАТО и Европейския съюз, Република България е страна и по 50 двустранни споразумения за обмен и защита на класифицирана информация. Всяко от тези споразумения определя ДКСИ като компетентен национален орган по сигурността, който следи и носи отговорност за спазване на клаузите по защита на чуждестранната класифицирана информация, предоставена на Република България. В ДКСИ функционира централна регистратура в областта на международните отношения.

Под ръководството на ДКСИ се организират регистратури в областта на международните отношения в организационните единици, в които се съхранява и обменя чуждестранна класифицирана информация. Дейността на тези регистратури се организира в съответствие със сключения международен договор и правилата за защита на класифицираната информация на съответната международна организация или на държавата, от която изхожда

класифицираната информация. ДКСИ констатира съответствието на прилаганите марки със съответните директиви и решения в регистратури и контролни пунктове за класифицирана информация на НАТО и класифицирана информация на Европейския съюз.

Компетентните органи по сигурността на НАТО и на Европейския съюз провеждат инспекции в регистратурите, които работят с тяхна класифицирана информация за установяване в какво състояние е системата за защита съобразно действащите директиви. В резултат на инспекциите се правят констатации относно ефективността на прилаганите в Република България мерки за защита съобразно действащите директиви за сигурността на класифицираната информация на НАТО и класифицираната информация на Европейския съюз. При необходимост от коригиращи действия в организацията на системата за защита се дават препоръки до компетентните органи на Република България с цел да се гарантира спазването на изискваните минимални стандарти.

Проведените досега инспекции и направените в резултат на тях констатации дават основание да се направи заключение, че като член на НАТО и на Европейския съюз Република България е надежден партньор в областта на защитата на тяхната класифицирана информация.

НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Лекцията включва: определение на нерегламентиран достъп до класифицирана информация (НДКИ), прояви на НДКИ – по видовете сигурност, действия на служителя по сигурността на информацията (ССИ) и ръководителя на организационната единица при случаи на НДКИ, действия на органа по прекия контрол ДАНС при случаи на нерегламентиран достъп до национална класифицирана информация, действия на ДКСИ при случаи на нерегламентиран достъп до чуждестранна класифицирана информация, резултати от действията на ДАНС и ДКСИ, както и превенция на НДКИ.

Съгласно § 1, т. 6 от допълнителните разпоредби на ЗЗКИ нерегламентиран достъп до класифицирана информация е разгласяване, злоупотреба, промяна, увреждане, предоставяне, унищожаване на класифицирана информация, както и всякакви други действия, водещи до нарушаване на защитата й или до загубване на такава информация.

За нерегламентиран достъп се счита и всеки пропуск да се класифицира информация с поставяне на съответен гриф за сигурност или неправилното му определяне, както и всяко действие или бездействие, довело до узнаване от лице, което няма съответното разрешение или потвърждение за това.

Съгласно изискванията § 1, т. 4 от допълнителните разпоредби на ЗЗКИ, ръководителя на организационната единица ръководи, организира и контролира дейността по защитата на класифицираната информация. Той е отговорен за планирането, организирането, прилагането и спазването на мерките за защита на класифицираната информация в организационната единица.

Служител по сигурността на информацията е физическо лице, назначено от ръководителя на организационната единица за осъществяване на дейността по защита на класифицираната информация в организационната единица. ССИ следи за спазването на изискванията на ЗЗКИ и на международните договори във връзка със защитата на класифицираната информация. ССИ прилага правилата относно видовете защита на класифицираната информация в организационната единица.

В резултат на нерегламентирания достъп до класифицирана информация може да настъпи вреда в областта на националната сигурност, отбраната, външната политика или защитата на конституционно установения ред. Съгласно § 1, т. 15 от допълнителните разпоредби на ЗЗКИ вреда е заплаха или увреждане на интересите на Република България или на тези интереси, които тя се е задължила да защитава, вредните последици от чието увреждане не могат да бъдат елиминирани, или вредни последици, които могат да бъдат смекчени само с последващи мерки.

В зависимост от значимостта на интересите и сериозността на причинените вредни последици вредите са непоправими или изключително големи, трудно поправими или големи и ограничени.

През последните години в страната са установени случаи на нерегламентиран достъп до класифицирана информация, вследствие на следните най-често срещани нарушения:

- нарушения на изискванията, свързани с отчетността, движението и класификацията на документи;
- загуба на документи, съдържащи класифицирана информация с ниво „Поверително“ и „Секретно“, както и загуба на част от документ с ниво „Поверително“;
- единични целенасочени действия на лица, чиито деяния осъществяват състави на престъпления по смисъла на Наказателния кодекс;
- неправилно определяне или неактуализиране на периметъра на зоните за сигурност и на административната зона;
- „съхраняване, обработване и обмен на класифицирана информация извън определените зони за сигурност;
- не се актуализират основните организационни документи, свързани с физическата сигурност;
- разкриване на класифицирана информация по непредпазливост;
- неспазване на изискванията на чл. 46 и чл. 47 от ППЗЗКИ при поставяне или пропускане поставянето на гриф за сигурност;
- неизпълнение на заповед, ограничаваща достъпа на конкретен служител;
- в регистратура за класифицирана информация до ниво „Поверително“ са приети документи, представляващи държавна тайна с ниво „Секретно“;
- унищожаване на оригинали на документи, маркирани с гриф за сигурност, за които не е изготвено предложение до ДКСИ и не е получено разрешение за тяхното унищожаване;
- неспазване на сроковете по чл. 55, ал. 2 от ЗЗКИ за ново проучване за надеждност;
- липса на обучение на служители по защита на класифицираната информация или формалното му провеждане;
- не всички служители, включени в списъците по чл. 37 от ЗЗКИ, имат издадени разрешения за достъп до класифицирана информация;
- неприлагане в пълнота принципите и мерките в областта на индустриалната сигурност;
- използване на нерегистрирани и дори лични материални носители за многократен запис за работа с класифицирана информация;
- създаване на документи и обработка на класифицирана информация на несертифицирани КИС или на КИС, които са свързани с интернет, в нарушение на чл. 93 от ЗЗКИ;
- загуба на флаш-памети с ниво „Поверително“, съдържащи криптографско средство и криптографски ключове;
- използване на криптографски мрежи, които не са въведени в експлоатация по реда, посочен в НКСКИ;
- пропуски при разпространение, съхранение и унищожаване на криптографски ключове и материали.

ДЕЙСТВИЯ НА СЛУЖИТЕЛЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА И РЪКОВОДИТЕЛЯ НА ОРГАНИЗАЦИОННАТА ЕДИНИЦА ПРИ СЛУЧАЙ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Организационната единица незабавно уведомява в писмена форма ДКСИ и ДАНС за всеки констатиран случай на НДКИ. Уведомлението се изготвя съгласно Приложение към т. III.1 от Задължителните указания на ДКСИ относно действия в случай на нерегламентиран достъп до класифицирана информация.

От организационната единица следва да се предприемат мерки за предотвратяване и/или ограничаване на неблагоприятните последици от реализирането на НДКИ.

Организационната единица извършва оценка на нанесените вреди и я предоставя на компетентния проверяващ орган.

Служителят по сигурността на информацията води на отчет случаите на НДКИ и на взетите мерки, за което информира незабавно ДКСИ.

ДЕЙСТВИЯ НА ДАНС ПРИ РЕАЛИЗИРАНЕ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

ДАНС извършва инцидентна проверка в организационната единица по чл. 12 от ЗЗКИ и по реда и условията на НРИПОПКЗЗКИ с цел изясняване на обстоятелствата и отстраняване на всички рискове и заплахи, чието проявление би довело или е довело до НДКИ.

Проверката представлява съвкупност от действия, мерки и препоръки, предназначени да осигурят ефективното функциониране и усъвършенстване на системите за защита на класифицираната информация в организационната единица.

В проверката се извършва констатиране на моментното актуално състояние на системата за защита на класифицираната информация в организационната единица. Изясняват се предпоставките/причините, довели до НДКИ, както и хронологията на действията на служителите на организационната единица. Установяват се лицата, които с действието/бездействието си са допринесли за реализирането на НДКИ.

В хода на проверката се оценяват всички рискове и заплахи за защитата на класифицираната информация, чието проявление би довело до нерегламентиран достъп. Извършва се анализ на събраните данни относно заплахите за националната сигурност и оценка на актуалното състояние на системата за защита на класифицираната информация в организационната единица. Идентифицират се и се отстраняват или се предотвратяват рисковите

фактори, които биха довели или са довели до НДКИ. В отделни случаи на груби или системни нарушения по преценка на комисията, извършваща проверката, се стига до реализиране на административнонаказателна или наказателна отговорност.

В резултат на констатираните нарушения на организационната единица се дават предписания за предприемане на необходимите организационно-технически действия по ограничаване на вредните последици, както и за подобряване на функционалността и усъвършенстване на системата за защита на класифицираната информация в организационната единица.

След проверката се изготвя и изпраща доклад до ДКСИ за констатираните нарушения и проблеми, налагащи изменения на общата политика за сигурност на класифицираната информация.

ДЕЙСТВИЯ НА ДКСИ ПРИ РЕАЛИЗИРАНЕ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

В случай на нерегламентиран достъп до чуждестранна класифицирана информация ДКСИ предприема действия по реда и условията на съответния международен договор или правилата на международната организация, съгласно чл. 9, т. 6 от ЗЗКИ. ДКСИ извършва необходимите действия в координация с компетентната служба за сигурност.

ДАНС извършва проверка за изясняване на обстоятелствата по реда и условията на НРИПОПКЗЗКИ. ДАНС предприема необходимите действия в координация с ДКСИ. За резултатите от проверката ДАНС изготвя доклад и своевременно го изпраща на ДКСИ.

При нерегламентиран достъп до чуждестранна класифицирана информация ДКСИ предприема действия за уведомяване на съответните органи съгласно ЗЗКИ, конкретния международен договор или правилата на съответната международна организация.

В случай на нерегламентиран достъп до класифицирана информация с ниво на класификация „Строго секретно“, съгласно чл. 9, т. 13 от ЗЗКИ ДКСИ уведомява незабавно министър-председателя на Р България.

Във връзка с констатираните нарушения и проблеми относно защитата на националната и чуждестранната класифицирана информация, при необходимост се предлагат/приемат налагащи изменения на общата политика за сигурност на класифицираната информация.

РЕЗУЛТАТИ ОТ ДЕЙСТВИЯТА НА ДАНС И ДКСИ ПРИ ОСЪЩЕСТВЯВАНЕ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

При констатиран нерегламентиран достъп до класифицирана информация се изясняват фактите и причините, довели до него. Извършва се анализ и оценка на ефективността на прилаганите мерки за защитата на

класифицираната информация в конкретната организационна единица и структура. Оценяват се наличието на рисковете и вредите, относимостта им към заплаха или увреждане на интересите на Р България.

При невъзможност материалният носител на класифицирана информация да бъде възстановен или не може да бъде намерен, той се обявява за безвъзвратно загубен материал.

За резултатите от проверката се уведомява организационната единица и се дават указания за прилагане на превантивни мерки с цел свеждане до минимум на рисковете от бъдещо настъпване на НДКИ.

Информацията от проверката се използва за реализиране на административнонаказателна или наказателна отговорност. При данни за извършено престъпление се уведомява съответната прокуратура.

Осъществяват се специфични информационни, аналитични и контролни дейности – правят се оценки и прогнози за качеството на защита на класифицираната информация на територията на страната и в чужбина. На базата на констатираните нарушения и проблеми в организационната единица се набелязват инициативи за изменения на общата политика за сигурност на класифицираната информация, касаеща Националната система за защита на класифицираната информация.

ПРЕВЕНЦИЯ НА НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ И ПРЕДОТВРАТЯВАНЕ НА ЗАПЛАХИТЕ ЗА СИГУРНОСТТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ В ОРГАНИЗАЦИОННИТЕ ЕДИНИЦИ

Превенцията на НДКИ включва стриктно спазване изискванията на ЗЗКИ и подзаконовите нормативни актове, както и директивите на НАТО и решенията на ЕС. Необходимо е ефективно прилагане на организационни, физически и технически мерки за предотвратяване на НДКИ, прилагане на общи и конкретни мерки за осигуряване защитата на класифицираната информация, както и специфични мерки за сигурност.

Необходимо е да се извършва оценка на заплахите за сигурността на класифицираната информация, да се прилагат ефективни методи за противодействие на заплахите за сигурността на класифицираната информация.

За предотвратяване на заплахите за сигурността на класифицираната информация в организационната единица е необходимо да се актуализира и надгражда системата за сигурност. Своевременно да се идентифицират негативните процеси, свързани със заплахата за класифицираната информация, да се прогнозира тяхното развитие. Нужно е да се оцени степента на ефективност на осъществяваните мероприятия за защита на класифицираната информация. Предпоставки за предотвратяване на вредните процеси са познаването и изпълнението на задълженията от длъжностни лица, които следва да организират, ръководят и контролират защитата на класифицираната информация, както и изграждането на съзнание за сигурност.

Нужно е да се осъществява предварителен и текущ контрол от ССИ спрямо организацията, способите и средствата за сигурност, както и да се провеждат обучения и брифинги на служителите с достъп до класифицирана информация.

Провеждането на проверки по прекия контрол, осъществяването на общ контрол и методическо ръководство от ДКСИ също спомагат за превенция на рисковете за сигурността на класифицираната информация. Не на последно място по важност фактор е взаимодействието между органите по общия и прекия контрол, позволяващо отстраняване на нарушенията и минимизиране на негативните последици при проява на рискове за националната сигурност.

АДМИНИСТРАТИВНОНАКАЗАТЕЛНА ОТГОВОРНОСТ ПО ЗАКОНА ЗА ЗАЩИТАТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

СЪЩНОСТ И ПРИНЦИПИ НА АДМИНИСТРАТИВНОНАКАЗАТЕЛНАТА ОТГОВОРНОСТ

Административнонаказателната отговорност се изразява в осъществяване на санкции, предвидени за виновно неизпълнение или лошо изпълнение на административни задължения.

Тя е властническо наказателна мярка, израз на държавно наказателна репресия. Тя е вид наказание, т.е. властническа наказателна мярка, израз на държавна наказателна репресия.

Административнонаказателна отговорност се налага за неизпълнение на задължения, установени във връзка с нормалното функциониране на дейността по държавното управление. Тя не влече последици за съдимост и се реализира от самата администрация (административен орган, на които са вменени тези задължения със закон).

Не е необходимо от деянието да са настъпили определени неблагоприятни резултати – заплаха от увреждане или увреждане на определени обществени отношения.

Отговорността се носи за самото неизпълнение на установените задължения, поради което и съставите на нарушения в преобладаващата си част са формални – деяния на просто извършване.

Административнонаказателна отговорност не влече последици за съдимост и се реализира от самата администрация.

Същността на административнонаказателната отговорност се определя от три понятия:

- административно нарушение,
- административно наказание и
- ред за налагане на административните наказания.

В най-обобщен вид тя е изразена в принципите, на които е изграден институтът на административнонаказателната отговорност:

- ***Принцип на законоустановеност на съставите на административните нарушения и на наказанията*** – само предвидените в закона деяния представляват административни нарушения и за тях се носи определената в закона отговорност;

- ***Принцип на вината*** – наказанието се налага за проявена лична вина при извършването на наказуемо деяние.
- ***Справедливост на административните наказания*** – постига се чрез правилата за индивидуализация на наказанието;
- ***Недопустимост за налагане на повторно наказание за едно и също нарушение (non bis in idem);***
- ***Принцип на зачитане на личността и моралната сфера на нарушителя;***
- ***Принцип на бързина и ефективност*** на административнонаказателната отговорност - кратки процесуални и преклузивни срокове за извършване на отделни производствени действия.

КУМУЛИРАНЕ

Административната отговорност не може да се кумулира само с наказателната отговорност, тъй като разликата между административните нарушения и престъпленията е в степента на обществената опасност.

Наказателната отговорност поглъща административно-наказателната. (чл. 33 от ЗАНН) С всички останали юридически отговорности административната отговорност може да се кумулира (дисциплинарна, имуществена).

АДМИНИСТРАТИВНО НАРУШЕНИЕ

Определение за това какво представлява административно нарушение се съдържа в чл. 6 от Закона за административните нарушения и наказания (ЗАНН) ***„Административно нарушение е това деяние (действие или бездействие), което нарушава установения ред на държавно управление, извършено е виновно и е обявено за наказуемо с административно наказание, налагано по административен ред”.***

Административните нарушения се определят чрез признаците, установени от ЗАНН, които могат да се обособят като признаци от обективна страна и признаци от субективна страна. За характеризиране на конкретните състави на нарушения по ЗЗКИ е необходимо да се посочват и субектите на нарушението с оглед на спецификата, че в преобладаващия брой случаи те представляват специални субекти.

Признаци от обективна страна

Деянието – представлява определено действие или бездействие. Чрез него се посочва начинът, по който може да бъде извършен конкретният състав на административно нарушение;

Противоправност и насоченост на административните нарушения – противоречие с предвидения от правото ред, което съдържа в себе си определена степен на обществена опасност. Административните нарушения са специфични нарушения, извършени в сферата на държавно управление.

Самият факт на неизпълнение на публичноправните задължения, т.е. всяко отклонение от установения административен ред представлява реална опасност за управленческата дейност;

Наказуемост – за деянието е предвидено административно наказание. Характерно за всички състави на нарушения по ЗЗКИ е, че предвидените санкции имат имуществен характер – глоба за физически лица и имуществена санкция за юридическите лица;

Особен административен ред, по който се преследва – съставите на нарушения по ЗЗКИ не съдържат тази особеност на административните нарушения. Тя е посочена общо за всички състави с разпоредбата на чл. 134, ал. 2 от ЗЗКИ, който препраща към реда, предвиден в ЗАНН.

Признаци от субективна страна

Вината – особено отношение на дееца към извършеното от него деяние и последиците от това деяние.

Има две форми на вината – **умисъл и непредпазливост**.

За налагане на административнонаказателна отговорност са релевантни и двете форми на вината.

Според чл. 7, ал. 2 от ЗАНН непредпазливите деяния не се наказват само в изрично предвидените случаи.

Съставите на административни нарушения по ЗЗКИ не съдържат изисквания за формата на вината, при която извършеното деяние може да се квалифицира като административно нарушение. Липсата на изрично правило води до приложението на общите правила за административните нарушения, предвидени в ЗАНН. Това означава, че за съставомерността на предвидените по ЗЗКИ деяния формата на вината е без значение.

Мотиви и цели на извършителя – съставите по ЗЗКИ не предвиждат мотивите или целите на извършителя като елемент от съставите на административни нарушения.

АДМИНИСТРАТИВНОНАКАЗАТЕЛНО ОТГОВОРНИ ЛИЦА

Според чл. 26, ал. 1 от ЗАНН административнонаказателно отговорни са пълнолетните лица, навършили 18 години, които са извършили административни нарушения в състояние на вменяемост. **Вменяемостта е способност и състояние, които дават възможност на едно лице да съзнава, ръководи и контролира постъпките си.** Вменяемостта е обусловена от физически и психически предпоставки, които дават възможност да се разкрие дължимото от закона поведение. Извежда се от аргумент на противното от чл. 33, ал. 1 от НК.

В българското право вменяемостта се свързва с навършването на определена възраст – 18 години. Ако лицето е навършило 18 години и не е поставено под запрещение, то се счита за вменяемо. Лица навършили 18 години стават административно наказателно отговорни (чл.26 от ЗАНН).

Непълнолетните, които са навършили 16 години и са могли да разбират свойството и значението на извършеното нарушение и да ръководят постъпките си, също са административнонаказателно отговорни.

За административни нарушения, извършени от малолетни, непълнолетни на възраст от 14 до 16 години и поставени под пълно запрещение, отговарят съответно родителите, попечителите или настойниците, които съзнателно са допуснали извършването им.

ЗАНН установява принципа, че административно-наказателната отговорност е лична.

В съответствие с него и с принципа на вината е правилото на чл. 24, ал. 2 от ЗАНН, според което за административни нарушения, извършени при осъществяване на дейността на предприятия, учреждения и организации, отговарят работниците и служителите, които са ги извършили, както и ръководителите, които са наредили или допуснали да бъдат извършени. С това правило се изключва възможността юридическо лице да носи административнонаказателна отговорност. Юридическото лице не може да има укоримо поведение, обусловено от годност, вменяемост за извършване на неправомерно поведение. Юридическите лица като такива могат да извършват само правомерни действия.

Въпреки разпоредбата на чл. 24, ал. 2 от ЗАНН, институтът на административнонаказателната отговорност допуска хипотезата на юридически лица да се налагат санкции за неизпълнение на задължения към държавата или общината при осъществяване на тяхната дейност (чл. 83, ал. 1 от ЗАНН). Санкцията може да има само имуществен характер и по същество не представлява глоба, макар да се налага по един и същи ред. Това означава, че

като изключение, за неизпълнение на задължения към държавата или общината, могат да бъдат санкционирани юридически лица и еднолични търговци. Налице е обективна отговорност. В административнонаказателните разпоредби на ЗЗКИ налагането на имуществена санкция на юридически лица има характер на правило.

✓ ***Административнонаказателно отговорни са и чужденците, които на територията на Република България извършат административно нарушение съгласно националното право.***

✓ ***Административнонаказателните разпоредби на закона се прилагат и спрямо български граждани, които извършат административни нарушения в чужбина, наказуеми по българските закони, ако засягат интересите на нашата държава.***

ОБЩА ХАРАКТЕРИСТИКА НА СЪСТАВИТЕ НА АДМИНИСТРАТИВНИТЕ НАРУШЕНИЯ ПО ЗЗКИ

Специални субекти

Административнонаказателно лица в ЗЗКИ имат една съществена отлика – много често е предвиден специален субект.

Това означава, че към установените от ЗАНН критерии кои лица са административнонаказателно отговорни, се добавят и допълнителни критерии.

Например субекти по някои от административните състави по ЗЗКИ могат да бъдат само лица, които представляват организационна единица:

- лица, които са получили разрешения за достъп до класифицирана информация;
- лица, които са служители по сигурността на информацията;
- длъжностни лица от службите за сигурност и службите за обществен ред и т.н.

В съставите на административни нарушения по ЗЗКИ преобладават специалните субекти във връзка с особените обществени отношения, които законът регулира.

Начин на формулиране на съставите на административни нарушения

Характерна особеност на съставите на административни нарушения по ЗЗКИ е начинът на тяхното формулиране – законодателният подход е очертаването им с препращащи норми. Съставите на административни нарушения се определят чрез посочването на точно определена разпоредба от закона, за неспазването на която се налага предвидената санкция. Извън тези

състави е предвидено, че всяко неспазване на закона или нормативните актове по неговото прилагане представлява административно нарушение.

Единственото изключение от формулирането на съставите с препращащи норми е разпоредбата на чл. 131 от ЗЗКИ, при която деянието, което представлява административно нарушение, е конкретно посочено („Ръководител на организационна единица, който не предостави информация на компетентните органи, поискана при условията и по реда на закона, се наказва с глоба от 500 лева").

Начинът на изграждане на правната уредба на защитата на класифицираната информация не позволява възприемането на подхода в ЗЗКИ за формулиране на съставите на административни нарушения.

ЗЗКИ не съдържа изчерпателна уредба на обществените отношения, свързани със създаването, обработването, съхраняването, реда за достъп и предоставянето на класифицирана информация. Правната уредба е доразвита с ППЗЗКИ, издадени са редица наредби по отделните видове сигурност на информацията, които я детайлизират. Да се предвиждат състави на нарушения за точно определени разпоредби на закона, чието конкретно съдържание е установено с подзаконовите актове по прилагането му, не е издържано от правна гледна точка.

СИСТЕМА НА НАРУШЕНИЯТА

Общи състави и състави на конкретни нарушения по ЗЗКИ

Установените в ЗЗКИ състави на административни нарушения условно могат да се поделят в две групи:

- общи състави, формулиране на съставите в приложното поле на които се включват нарушения на множество (групи) задължения във връзка със защитата на класифицираната информация;
- конкретни състави, при които не се изпълняват точно определени задължения във връзка със защитата на класифицираната информация.

Практическото значение от разграничаването на съставите на нарушения на общ и конкретен състав на нарушение е във връзка със случаите, когато едно и също деяние може да бъде подведено в хипотезата на два състава. Принципът за недопустимост на повторна санкция за едно и също деяние изключва възможността да се реализира отговорност и по двата състава. Поради това деянието трябва да бъде подведено в хипотезата на специалния състав, когато такъв е установен. В този смисъл само ако деянието не попада в съставите на конкретни нарушения, трябва да бъде наказано по общите състави.

Всички състави на нарушения на ЗЗКИ могат да се определят като формални нарушения.

Неизпълнението на предвидените задължения е основание за налагане на отговорност, като не е необходимо да са настъпили определени последици от това. Вредоносният резултат от деянието (застрашаването или увреждането на обществените отношения, които ЗЗКИ цели да защити) не е елемент от състава на нарушението, но той не е и правно ирелевантен. Значението на вредоносните последици от деянието обаче рефлектира в друга плоскост – според чл. 59, ал. 1, т. 2 от ЗЗКИ нарушението на закона или подзаконовите актове по прилагането му, което е създало опасност от възникване или е довело до значителни вреди за интересите на държавата, организациите или лицата в областта на защитата на класифицираната информация, е основание за отнемане на издаденото разрешение за достъп до класифицирана информация.

Административни наказания по ЗЗКИ

От предвидените по ЗАНН административни наказания (глоба, имуществена санкция за юридически лица, обществено порицание, временно лишаване от право да се упражнява определена професия или дейност) ЗЗКИ предвижда налагането само на глоба за физически лица и имуществена санкция за юридически лица.

Основание за налагане на административни наказания по ЗЗКИ е както извършването на нарушения, така и допускането на тяхното извършване.

В значителен брой от съставите на нарушения по ЗЗКИ е предвидена отговорност за ръководителя на организационната единица и за служителя по сигурността на информацията, ако са допуснали извършването на нарушения от други лица, за действията на които е трябвало да осъществяват контрол.

ПОВТОРНОСТ И СИСТЕМНОСТ НА НАРУШЕНИЯТА ПО ЗЗКИ

По-тежко наказуеми нарушения

За понятията „повторни” и „системни нарушения” са предвидени легални дефиниции в § 1, т. 16 и 17 от Допълнителните разпоредби на ЗЗКИ.

Повторно е нарушението на закона или на нормативните актове по неговото прилагане, извършено в едногодишен срок от влизането в сила на наказателното постановление, с което е наложено наказание за същия вид нарушение. Значението на повторността при извършване на

административно нарушение по ЗЗКИ е посочено в чл. 133 от ЗЗКИ – за повторно нарушение са налага глоба или имуществена санкция в двоен размер на първоначално посочената.

Административнонаказващият орган е лишен от възможността да индивидуализира наказанието по правилата на чл. 27 от ЗАНН. При повторно извършено нарушение в условията на обвързана компетентност той налага двойния размер на санкцията, наложена за първото нарушение.

Като системни се определят три или повече нарушения на закона или на нормативните актове по неговото прилагане, извършени в продължение на една година – са основание за отнемане на издадено РДКИ.

За разлика от повторността, за определянето на нарушението като системно, е без значение неговият вид. Количественият белег е определящ за системността. Системните нарушения на закона или подзаконовите актове по прилагането му са основание за отнемане на издаденото разрешение за достъп до класифицирана информация на основание чл. 59, ал. 1, т. 3 от ЗЗКИ.

РЕД НА НАЛАГАНЕ НА АДМИНИСТРАТИВНОНАКАЗАТЕЛНАТА ОТГОВОРНОСТ

Установяване на административни нарушения

Административнонаказателното производство се образува със съставянето на акт за административно нарушение. Актове за установяване на нарушения по ЗЗКИ според чл. 134 от ЗЗКИ могат да съставят само **длъжностни лица, упълномощени от:**

- Председателя на ДКСИ;
- Председателя на ДАНС

ДКСИ има правомощия да организира, осъществява, координира и контролира дейността по защитата на класифицираната информация (чл. 8, т. 1 от ЗЗКИ). В съответствие с това правомощие е установеното в чл. 134 от ЗЗКИ правило актовете за установяване на административни нарушения да се съставят от упълномощени от председателя на ДКСИ длъжностни лица.

Председателят на ДАНС също може да упълномощи длъжностни лица с функцията да съставят актове за установяване на административни нарушения. Основанието на това правомощие е във връзка с прекия контрол по защитата на класифицираната информация.

Задължително условие за законосъобразността на акта е в заповедта за проверката да бъдат посочени конкретните упълномощени служители. Не може да се извършва проверка по устна заповед.

Разграничаване на производството по установяване на административни нарушения и дейността по осъществяване на пряк контрол по защитата на класифицираната информация

Производството по установяване на административните нарушения по ЗЗКИ трябва да се разграничава от дейността по прекия контрол, предвиден в чл. 12 от ЗЗКИ и развит в Наредбата за реда за извършване на проверките за осъществяване на пряк контрол по защитата на класифицираната информация (Наредбата). Те се осъществяват на базата на различни нормативни актове (т.е. имат различно основание), преследват точно определени цели и имат различни последици.

Реализирането на административнонаказателната отговорност се осъществява по правилата на ЗАНН.

Целите, които се преследват с административно-наказателната отговорност, са тези, които ЗАНН посочва като цели на наказанието – да се предупреди и превъзпита нарушителят към спазване на установения правен ред и да се въздейства възпитателно и предупредително върху останалите граждани. Проверките за осъществяване на пряк контрол по защита на класифицираната информация имат за цел спазването на нормативните актове в областта на защитата на класифицираната информация и отстраняването на всички рискове и заплахи, чието проявление би довело до нерегламентиран достъп (чл. 2 от Наредбата). Основната цел на дейността на контролиращите органи по време на проверката в организационните единици – обект на контрол, е установяване на актуалното състояние на системата за защита на класифицираната информация (чл. 7 от Наредбата). Обстоятелството, че председателят на ДАНС със заповед е определил служители, които извършват проверките за осъществяване на пряк контрол, не е достатъчно за съставяне на акт за установяване на административни нарушения по ЗЗКИ. Според чл. 3, ал. 3 от Наредбата в заповедта трябва да се определят изрично служителите, имащи правомощия да съставят такива актове съгласно чл. 134, ал. 1 от ЗЗКИ.

Последица от установяване на административно нарушение е единствено реализиране на административнонаказателна отговорност чрез издаване на наказателно постановление и изпълнение на наложеното с него административно наказание.

В случаите на констатирани нарушения при извършена проверка по реда на прекия контрол предприемането на мерки за търсене на административнонаказателна отговорност е само една от възможните последици. Освен нея при всички положения трябва да се изпълнят и другите изисквания на чл. 23, ал. 2 от Наредбата:

- да се изготвят и изпратят до организационната единица – обект на контрол, предписания във връзка със сигурността;
- да се изготви и изпрати доклад до ДКСИ;
- да се изготви и изпрати до ДКСИ и до службите за сигурност информация за откритите проблеми, които налагат изменения в общата политика за сигурност на класифицираната информация.

Актът за установяване на административното нарушение се съставя в присъствието на нарушителя и свидетелите, които са присъствали при извършването (свидетели на нарушението) или установяването (свидетели на установяване на нарушението) на нарушението.

Възможно е актът за установяване на административно нарушение да се състави в отсъствие на нарушителя, когато същият е известен, но не може да се намери или не се яви след покана. Ако няма свидетели, присъствали при извършването или установяването на нарушението, или ако е невъзможно той да се състави в тяхно присъствие, той се съставя в присъствието на двама други свидетели (свидетели на акта), като това се отбелязва изрично в акта.

Актът за установяване на административно нарушение трябва да съдържа реквизитите, посочени в чл. 42 от ЗАНН. Той се подписва от актосъставителя и поне един от свидетелите, посочени в него и се предявява на нарушителя да се запознае със съдържанието му и да го подпише със задължение да уведоми наказващия орган при промяна на адреса си.

При подписване на акта на нарушителя се връчва препис от него срещу разписка, а в акта се отбелязва датата на неговото подписване. Ако нарушителят откаже да подпише акта, това се удостоверява с подписа на един свидетел (свидетел на отказа), името и точния адрес, който се отбелязва в акта.

Освен възраженията при съставяне на акта, нарушителят има право да възразява писмено в тридневен срок от подписването му. Когато във възраженията си нарушителят посочи писмени или веществени доказателства, според чл. 44, ал. 2 от ЗАНН те трябва да бъдат събрани служебно, доколкото това е възможно. След връчване на акта на нарушителя цялата административнонаказателна преписка се изпраща на административнонаказващия орган.

Актът за установяване на административно нарушение трябва да бъде съставен в сравнително кратки срокове: най-късно в тримесечен срок

от откриването на нарушителя и в едногодишен срок от извършване на нарушението. След изтичането на тези срокове според чл. 34, ал. 1 от ЗАНН не се образува наказателно производство поради изтекла давност.

Налагане на административни наказания

Според чл. 134, ал. 1 от ЗЗКИ наказателните постановления се издават от председателя на ДКСИ или от председателя на ДАНС.

Наказващият орган е длъжен да се произнесе в едномесечен срок след получаването на административнонаказателната преписка. Ако се установи, че актът не е връчен на нарушителя, наказващият орган го връща на актосъставителя. Установяването на това обстоятелство се улеснява от задължението на актосъставителя да връчи при подписването препис от акта срещу разписка на нарушителя.

Оспорване на адм. наказателното производство – 7 дни

Преди да се произнесе по преписката наказващият орган проверява акта с оглед на неговата законосъобразност и преценява възраженията и събраните доказателства, а когато е необходимо, има право да извършва разследване на спорните обстоятелства.

Когато се установи, че нарушителят е извършил деянието виновно и същото не представлява малозначителен случай, наказващият орган издава наказателно постановление, с което налага административно наказание в установените от закона предели. Препис от наказателното постановление се връчва срещу подпис на нарушителя, а когато той не се намери на посочения адрес това се отбелязва върху наказателното постановление и то се счита за връчено от деня на отбелязването.

Маловажен случай на административното нарушение е този, при който извършеното нарушение, с оглед на липсата или незначителността на вредните последици, или с оглед на други обстоятелства, представлява по-ниска степен на обществена опасност в сравнение с обикновените случаи на административни нарушения от съответния вид.

ОБЩИ СЪСТАВИ НА НАРУШЕНИЯТА ПО ЗЗКИ

Съставът по чл. 117 от ЗЗКИ

Нарушение на чл. 17 ЗЗКИ – чл. 17 ЗЗКИ установява задълженията на организационните единици.

Съставът на нарушението по чл. 117 от ЗЗКИ може да се определи като общ състав с оглед на многобройните форми на деянията, чрез които той може да бъде осъществен.

Деянието:

- неприлагане на изискванията за защита на класифицираната информация;
- неосъществяване на контрол по спазването на изискванията за защита на класифицираната информация;
- неуведомяване незабавно на ДКСИ в случай на нерегламентиран достъп до класифицирана информация;
- непредприемане на мерки за ограничаване на неблагоприятните последици от нерегламентиран достъп до класифицирана информация;
- непредоставяне на информация на ДКСИ, службите за сигурност и службите за обществен ред.

Административната отговорност е предвидена за неизпълнение на задължението на организационната единица по чл. 10, ал. 1, т. 2 от ЗЗКИ. На това основание ДКСИ получава незабавно и безплатно необходимата във връзка с упражняването на правомощията по чл. 9 информация от **държавни органи и органи на местното самоуправление**. На основание т. 3 се получава информация от физически и юридически лица, които могат да откажат да я предоставят, ако не е свързана с проучване за надеждност, за което са дали съгласие или са били уведомени по съответния ред. Ако организационната единица, която е отказала предоставянето на информация, не е държавен орган или орган на местното самоуправление, отговорността по този състав не може да се реализира. В този случай може да се приложи разпоредбата на чл. 132 от ЗЗКИ.

Задължението по чл. 11, ал. 4, т. 6 от ЗЗКИ – във връзка с извършването на проучванията за надеждност, издаването на потвържденията и осъществяването на пряк контрол, службите за сигурност имат право да получават необходимата информация от държавни органи, органите на местното самоуправление, физически и юридически лица**.** Ако дадена организационна единица, е отказала предоставяне на информация, то тя ще отговаря по чл. 117 от ЗЗКИ за непредоставянето й.

Задължението по чл. 16, ал. 1, т. 5 от ЗЗКИ – службите за обществен ред имат право да получават необходимата им във връзка с проучванията за надеждност информация от организационната единица.

Наказуемост – глоба от 2000 до 20 000лв.

Съставът по чл. 118 от ЗЗКИ

Деяние:

<u>За служители в организационни единици, получили разрешение за достъп до класифицирана информация съгласно чл. 18, ал. 1 от ЗЗКИ са длъжни да:</u>

- Да защитават класифицираната информация от нерегламентиран достъп;
- Да уведомяват незабавно ССИ за случаи на нерегламентиран достъп до класифицирана информация – чл. 18, ал. 1, т. 2;
- Да уведомяват ССИ за всички случаи на промени на класифицираните документи и материали, при които не е налице нерегламентиран достъп – чл. 18, ал. 1, т. 3 от ЗЗКИ;
- Да преминават периодични здравни прегледи най-малко веднъж на 2 години и психологически изследвания при условията на чл. 42, ал. 3 от ЗЗКИ;
- Ако са получили разрешение за достъп до КИ с ниво на класификация „Строго секретно", с изключение на лицата по чл. 39, ал. 1 от ЗЗКИ, трябва да информират писмено ССИ за всяко частно задгранично пътуване преди датата на заминаването, освен ако пътуването е в държави, с които Република България има сключени споразумения за защита на класифицираната информация;
- Служителите на службите за сигурност и за обществен ред са длъжни да уведомяват писмено ръководителите си за всяко задгранично пътуване – чл. 18, ал. 4 от ЗЗКИ;

Лицата получили разрешение за достъп до класифицирана информация във връзка с изпълнението на конкретно възложена задача са длъжни да спазват реда и условията за защита на класифицирана информация.

Наказуемост – Глоба от 50 до 300 лв.

Съставът по чл. 120 от ЗЗКИ

Който извърши нарушение, свързано с определянето на нивото на класификация и маркирането на информацията с гриф за сигурност, както и промяната или заличаването на грифа за сигурност се наказва с глоба от 100 до 500 лв. В тази връзка се предвиждат конкретни задължения, неизпълнението на които представлява състав на административно нарушение. Конкретните деяния, с които може да се осъществи съставът на нарушение по чл. 120 от ЗЗКИ, са:

✓ Определяне на нивото на класификация, респ. определяне на гриф за сигурност не от лицето, което има право да подпише документ, съдържащ

класифицирана информация или удостоверяващ наличието на класифицирана информация в материал. В тази категория нарушения е и неопределянето на временен гриф за сигурност от лицето, което е създало документ или материал, съдържащ класифицирана информация, когато е различно от лицето, което има право да го подпише;

✓ Маркиране с гриф за сигурност, който не съответства на нивото на класификация;

✓ Поставяне, промяна и заличаване на грифа за сигурност не в рамките на предоставения на лицето достъп;

✓ Неоснователна промяна на нивото на класификация на информацията;

✓ Промяна или заличаване на нивото на класификация без съгласието на лицето по чл. 31, ал. 1 от ЗЗКИ или на негов висшестоящ ръководител;

✓ Несъобщаване на получателите на информацията за промяната на нивото на класификация;

✓ Неорганизиране на обучение от ръководителите на организационните единици на подчинените им служители за условията и реда за маркиране на информацията.

Субект на административнонаказателна отговорност

- Лице, което има право да подписва документа, съдържащ класифицирана информация (лице по чл. 31, ал. 1 от ЗЗКИ);
- Лице, което създава документ или материал, съдържащ класифицирана информация, но няма право да го подписва;
- Висшестоящ ръководител на лицето по чл. 31, ал. 1 от ЗЗКИ;
- Получател на информацията, чието ниво на класификация е променено;
- Ръководител на организационна единица, който не организира обучение на подчинените си за маркиране на КИ;
- Всяко друго лице.

Наказуемост – глоба от 100 до 500 лева.

Съставът по чл. 121 от ЗЗКИ

Лицата, имащи право да подписват документи, са длъжни най-малко веднъж на 2 години, да преразглеждат периодично всеки документ или материал, маркиран с гриф за сигурност, за наличието на правни основания за промяна или премахване на нивото на класификация. Неизпълнението на това задължение представлява състав на нарушение по силата на чл. 121 от ЗЗКИ.

Наказуемост – глоба от 100 до 1000 лева.

Съставът по чл. 123 от ЗЗКИ

Ръководител на организационна единица или служител по сигурността на информацията, който извърши или допусне извършването на нарушение, свързано с неприлагане на система от мерки и средства за физическа сигурност на сгради, помещения и съоръжения, в които се създава, обработва и съхранява класифицирана информация се наказва с глоба от 50 до 400 лв.

Субект на административнонаказателна отговорност – определени са в чл. 123 от ЗЗКИ:

- ръководител на организационна единица;
- служител по сигурността на информацията.

Основание за налагане на административнонаказателна отговорност по този състав е както неприлагането на изискванията за физическа сигурност, така и допускането на това неизпълнение.

Наказуемост – глоба от 50 до 400 лева.

Съставът по чл. 125 от ЗЗКИ

Задължителните специфични изисквания за сигурност на АИС или мрежи във всяка организационна единица се определят от ръководителя на организационната единица по предложение на служителя по сигурността на информацията. Тези изисквания подлежат на утвърждаване от Държавна агенция "Национална сигурност".

Деяние – По предложение на служителя по сигурността на иформацията ръководителят на ОЕ определя задължителните специфични изисквания за сигурност на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация. Тези изисквания трябва да бъдат утвърдени от Специализирана дирекция “Технически операции” - ДАНС (СДТО). Като административно нарушение е обособено неизпълнението на изискването за утвърждаване на задължителните специфични изисквания за сигурност на АИС или мрежи, определени от ръководителя на организационната единица.

Като законодателен пропуск може да се определи обстоятелството, че не е установен състав на административно нарушение за неизпълнение на задължението по чл. 90, ал. 5 от ЗЗКИ – всички последващи промени в задължителните спацифични изисквания се утвърждават също от СДТО.

Наказуемост – глоба от 300 до 2000 лева.

Съставът по чл. 126 от ЗЗКИ

Деяние – В организационните единици, в които се използват АИС или мрежи за обработка на класифицирана информация, трябва да има служители, които осъществяват функции по контрол за спазване на изискванията за сигурност на тези системи или мрежи. Тези служители може да се назначат специално за тази цел или да са служители от административното звено по сигурността, на които са възложени такива функции. Назначаването на тези служители, респ. възлагането на функции по контрола на вече назначени служители от административното звено по сигурността, се извършва от ръководителя на организационната единица по предложение на служителя по сигурността на информацията. Ако такива служители не бъдат назначени/определени, се носи административна отговорност по правилата на чл. 126 от ЗЗКИ.

Наказуемост – глоба от 500 до 1000 лева.

Съставът по чл. 131 от ЗЗКИ

„Ръководител на организационна единица, който не предостави информация на компетентните органи, поискана при условията и по реда на закона, се наказва с глоба от 500 лв.”

ПРЕСТЪПЛЕНИЯ ПРОТИВ ИНФОРМАЦИЯТА, ПРЕДСТАВЛЯВАЩА ДЪРЖАВНА ТАЙНА, ПРЕДВИДЕНИ В НАКАЗАТЕЛНИЯ КОДЕКС

Отделно от административнонаказателната отговорност, при висока степен на обществена опасност, законодателят в Наказателния кодекс е предвидил носене на наказателна отговорност за престъпления против информацията, представляваща държавна тайна, а именно:

- Който разгласи информация, представляваща държавна тайна, която му е била поверена или станала известна по служба или работа, както и този, който разгласи такава информация, като съзнава, че от това може да последват вреди за интересите на Република България, ако не подлежи на по-тежко наказание, се наказва с лишаване от свобода от две до осем години.

- Който загуби документи, издания или материали, съдържащи информация, представляваща държавна тайна, или чуждестранна класифицирана информация, получена по международен договор, по който

Република България е страна, се наказва с лишаване от свобода до две години или с пробация.

- Който стане причина да бъде разкрита информация, представляваща държавна тайна, или чуждестранна класифицирана информация, получена по международен договор, по който Република България е страна, по непредпазливост, се наказва с лишаване от свобода до две години или с пробация.

УСЛОВИЯ И РЕД ЗА ПРЕНАСЯНЕ НА КЛАСИФИЦИРАНИ ДОКУМЕНТИ И/ИЛИ МАТЕРИАЛИ ЧРЕЗ КУРИЕРИ - СЛУЖИТЕЛИ В ОРГАНИЗАЦИОННИ ЕДИНИЦИ

Нормативни изисквания при приемане, пренасяне и предаване на класифицирана информация

В изпълнение на изискванията за защита на класифицираната информация от нерегламентиран достъп по отношение на своевременното приемане, пренасяне и предаване на класифицираната информация е необходимо служителите в организационните единици, които изпълняват функции на куриери да бъдат запознати с изискванията на глава V, раздел V от ППЗЗКИ, както и със Задължителните указания на ДКСИ въз основа на Решение на ДКСИ № 202-II/02.11.2004 г. , Решение № 68 – I/25.10.2011 г. и Решение № 35–I/15.05.2018 г. за пренасяне на документи и/или материали, съдържащи класифицирана информация чрез куриери - служители в организационни единици и Задължителните указания въз основа на Решение на ДКСИ № 55 I/28.07.2016 г., изм. с Решение на ДКСИ № 83 II/19.10.2017 г. за разкриване, функциониране и закриване на регистратура за класифицирана информация.

Пренасянето на материали, съдържащи класифицирана информация, съгласно регламента на чл. 81, ал. 1 от ППЗЗКИ, може да се извършва:

- чрез специална куриерска служба (СКС);
- чрез куриер от организационната единица;
- чрез комуникационни информационни системи (КИС) или мрежи;
- по пощата;
- чрез военна пощенска свръзка при обявено военно положение или положение на война.

Всеки куриер, пренасящ материали, съдържащи класифицирана информация, на територията на страната, се придружава най-малко от още един служител, който е охрана.

Материали, съдържащи класифицирана информация с ниво на класификация „Строго секретно”, се пренасят само чрез специалната куриерска служба, с изключение на Въоръжените сили, Министерството на вътрешните работи, Държавна агенция „Национална сигурност”, Държавна агенция „Разузнаване” и Националната служба за охрана, които могат да пренасят тези материали и със свои куриери (чл. 82, ал. 1 от ППЗЗКИ).

Служител (куриер) от организационната единица може да пренася пакети с материали, съдържащи класифицирана информация, с изключение на материалите с ниво на класификация „Строго секретно”, освен в случаите по

чл. 82, ал. 1, след провеждане на обучение и изпит, резултатите от които се отразяват в протокол (чл. 89 от ППЗЗКИ). На служителите (куриери), успешно преминали обучение, ДКСИ издава специална (служебна) карта, с която те се легитимират при изпълнение при изпълнение на служебните си задължения.

Служителите от службите за сигурност могат да пренасят пакети с материали, съдържащи класифицирана информация, след провеждането на обучение и изпит, като се легитимират със служебна карта /чл. 89, ал. 3 от ППЗЗКИ/.

Носене на оръжие при изпълнение на служебните задължения от куриерите:

За осигуряване защитата на класифицираната информация от нерегламентиран достъп по отношение на пренасяне на пакети с материали, съдържащи класифицирана информация при изпълнение на функциите на куриери, служителите на организационни единици носят оръжие, съгласно чл. 81, ал. 3 от ППЗЗКИ. Носенето на оръжие от куриерите и охраната не е задължително при пренасянето на материали, съдържащи класифицирана информация, между регистратури, намиращи се в една и съща охранявана сграда (чл. 81, ал. 4 от ППЗЗКИ).

При изпълнение функциите на куриер, служителят в организационната единица е длъжен:

- своевременно да приема, пренася и предава пакетите с материали, съдържащи класифицирана информация;
- да осигури защитата на пакетите с материали, съдържащи класифицирана информация от всякаква заплаха или вреда, в резултат на природни бедствия, аварии, терористична дейност или саботаж;
- да осигури защитата на пакетите с материали, съдържащи класифицирана информация от всякаква заплаха или вреда, в резултат на нерегламентиран достъп или опит за нерегламентиран достъп;
- в случаите на нерегламентиран достъп, да информира незабавно служителя по сигурността на информацията.

При приемане, пренасяне и предаване на пакети с материали, съдържащи класифицирана информация:

- да знае точните адреси на регистратурите на организационните единици, до които ще се извършва пренасянето;
- да носи със себе си служебно оръжие и специална служебна карта на куриер, издадена от ДКСИ, съгласно чл. 89 от ППЗЗКИ;

- да не оставя без охрана и наблюдение материалите, съдържащи класифицирана информация;
- след предаване на материалите, съдържащи класифицирана информация да върне опис (Приложение №7, от ППЗЗКИ) в регистратурата, която го е изпратила;
- да уведоми служителя по сигурността на информацията за изпълнение на задачата по пренасянето.

На куриера е забранено:

- да нанася поправки върху пакетите с материали, съдържащи класифицирана информация или описите;
- да нарушава целостта на опаковката на материалите, съдържащи класифицирана информация;
- да се запознава със съдържанието на материалите, съдържащи класифицирана информация при нарушаване на целостта на опаковката им;
- да предава пакети с материали, съдържащи класифицирана информация извън зоната за сигурност на съответната организационна единица, както и в тъмни, неосветени помещения.

Нормативни изисквания за физическа сигурност и цялост при опаковане на пакети с материали съдържащи, класифицирана информация

Материалите, съдържащи класифицирана информация, представляваща държавна тайна се пренасят в пликове или опаковани в пакети, съгласно чл. 85 от ППЗЗКИ:

- пакетите представляват две здрави, непрозрачни, поставени една в друга опаковки или пликове, надеждно запечатани и облепени по начин, непозволяващ изваждане на материалите от опаковките, без да се повредят съдържанието или печатите на тези опаковки;
- пликовете и пакетите в които се поставят материали, съдържащи класифицирана информация се опаковат със здрава и непрозрачна хартия (Приложение № 9 от ППЗЗКИ);
- върху външната опаковка на пакета се изписват без съкращения:

  - в горната лява част – подателят и неговия точен адрес;
  - в долната дясна част - получателят и неговия точен адрес;
  - в горната дясна част – номерът на експедиционното писмо, който се счита за номер на пакета;
  - в долната лява част се изписва - „Само чрез куриер”.

- върху вътрешната опаковка се изписват без съкращения:

- в горната лява част – подателят

- в долната дясна част – получателят

- в горната и долната част – подходящо ниво на класификация, но не по-ниско от най-високото ниво на документите, които се съдържат в пакета;

- при необходимост върху вътрешната опаковка се изписва „Да се отвори от …”, като се посочват името и длъжността на лицето, до което е адресиран материалът;

- на обратната страна на плика се поставят пет, а на пакет или руло с превързана опаковка - не по-малко от пет марки-лепенки, подпечатани с печата на регистратурата;

- куриерска чанта, кутия или куфар с шифрово запечатващо устройство се счита за външна опаковка;

- пренасянето на пакетите по куриер се извършва в подходящи чанти(куфари), гарантиращи тяхната сигурност и цялост, съгласно чл. 86 от ППЗЗКИ;

- пакети, които не могат да бъдат поставени в чанти или куфари, се пренасят опаковани и закрити така, че да се гарантира целостта им;

- материали, съдържащи класифицирана информация, които поради своето естество и размери, тегло и форма не могат да бъдат поставени в пакети, чанти или куфари се пренасят опаковани и закрити така, че да се гарантира защитата им от нерегламентиран достъп, съгласно чл. 87 от ППЗЗКИ.

Куриерите пренасят пакети с материали, съдържащи класифицирана информация, в страната, пътувайки със служебни автомобили или в отделно купе в пощенски вагон или във вагон на БДЖ, които не подлежат на проверка, или с въздухоплавателни средства.

Съгласно чл. 99 от ППЗЗКИ не се разрешава, освен в случаите предвидени в правилника, предаването и приемането на:

- материали, съдържащи класифицирана информация извън зоната за сигурност на съответната организационна единица, в тъмни и неосветени помещения;

- пакети с оръжие, режещи предмети, взривни и лесно запалими вещества, както и други опасни вещества и предмети;

- пликове (пакети) с неправилни и неясни адреси на подателя и на получателя;

- пликове (пакети) с некачествена или повредена опаковка или печати;

- пликове (пакети), подпечатани с печати, които не са от регистратурата на подателя.

Ред за приемане, пренасяне и предаване на материали, съдържащи класифицирана информация

Съгласно чл. 93 от ППЗКИ на куриерите се осигурява достъп до регистратурата или място в зоната за сигурност в организационните единици, където се извършва приемане и предаване на пакети с материали, съдържащи класифицирана информация.

- пакетите с материали, съдържащи класифицирана информация, се приемат от определен служител от регистратурата на организационната единица съгл. чл. 98, ал.1 от ППЗЗКИ;
- по изключение в извънработно време, материалите, съдържащи класифицирана информация, се предават на дежурния на организационната единица, съгласно чл. 98, ал. 2 от ППЗЗКИ;
- при приемане на пакети с материали, съдържащи класифицирана информация, куриерът е длъжен да провери:
  - правилното оформяне на пакетите (пликовете);
  - съответствието на печатите върху марките-лепенки с тези на регистратурата;
  - съответствието на номерата на пакетите (пликовете) и адреса с посочените в описа.

При неизпълнение на изискванията за оформяне на пакетите (пликовете), несъответствията се отстраняват на място или пакетите не се приемат. Неприетите пакети се зачеркват в описа по начин, позволяващ прочитане на зачертаното, след което описът се заверява с подписа и печата на подателя, като се поставя и дата. Куриерът се подписва само за фактически приетото количество.

- Куриерът-служител в организационна единица приема пакетите с материали, съдържащи класифицирана информация, от регистратурата, по опис приложение № 7 от ППЗЗКИ, изготвен в 3 (три) екземпляра, съгласно чл. 96 от ППЗЗКИ;
  - екземпляр № 3 с подписа на куриера остава в регистратурата на организационната единица;
  - екземпляри № 1 и № 2 се подписват от служителя на регистратурата, която предава пакетите, като екземпляр № 1 се подпечатва с печата на организационната единица;
  - екземпляри № 1 и № 2 се предават на куриера;

- след предаването на пакетите служителят, който ги е приел се подписва в екземпляр № 2 на описа, поставя печат, дата и час на получаване и го връща на куриера;
- екземпляр № 1 остава на съхранение в регистратурата на адресата;
- екземпляр № 3 се унищожава, след като куриерът върне екземпляр № 2 в регистратурата, изпратила пакетите.

Съгласно изменението с Решение на ДКСИ № 83-II/19.10.2017 г. на Задължителни указания за разкриване, функциониране и закриване на регистратура за класифицирана информация, издадени въз основа на Решение на ДКСИ № 55- I/28.07.2016 г.:

„*6. Служителят по сигурността на информацията поддържа актуален списък на служителите в организационната единица, определени да приемат пакети с документи и материали, съдържащи класифицирана информация. Списъкът съдържа информация за валидните разрешения за достъп до класифицирана информация и сертификати за достъп до класифицирана информация на ЕС и НАТО на служителите.*

7. На куриерите се осигурява достъп до списъка по т. 6 от настоящите Задължителни указания. ***Списъкът се поставя на видно място в регистратурата за класифицирана информация и/или в зоната за сигурност на организационната единица****.“*