ПЪРВОНАЧАЛНО ОБУЧЕНИЕ
(лекция)

## Общи положения

Целта на Закона за защита на класифицираната информация е да я защитава от нерегламентиран достъп.

Класифицирана информация по смисъла на ЗЗКИ е информацията, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация.

Основният принцип заложен в Закона за класифицирана информация е „необходимост да се знае“. Принципът „необходимост да се знае" се състои в ограничаване на достъпа само до определена класифицирана информация и само за лица чиито служебни задължения или конкретна възложена задача налагат такъв достъп.

Видовете защитата на класифицираната информация са: персонална, документална, индустриална, криптографска, физическа и на автоматизираните информационни системи или мрежи.

## Рискове за интересите на Р България в областта на защитата на класифицираната информация

**Основната 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 процес и необосновано скъп. В тези случаи ще трябва да се анализират най-важните възли от информационната инфраструктура.

Дейностите на една организация, работеща с класифицирана информация, са изложени на много рискове и анализът им включва дейности по характеризиране на организацията, идентифициране на източниците на заплаха, идентифициране на уязвимостите относно нейната сигурност и в частност тази на нейните информационни структури.

## Органи за защита на класифицираната информация

### Система от органи за защита на класифицираната информация

Системата от органи за защита на класифицираната информация обхваща:

• **Народното събрание (НС),** което приема законите в областта на защитата на класифицираната информация, техните изменения и допълнения;

• **Министерския съвет** (МС), който определя насоките на националната политика за защита на класифицираната информация;

• **Държавната комисия по сигурността на информацията** (ДКСИ), като национален орган, който осъществява политиката на Република България за защита на класифицираната информация (КИ);

• **Служби за сигурност** (СС) и **служби за обществен ред** (СОР);

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

**Държавна комисия по сигурността на информацията.**

**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.

Осъществява методическо ръководство спрямо служителите по сигурността на информацията.

**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.

**Понятие за организационна единица.**

**Права и задължения на ръководителя на организационната единица и на служителите в организационната единица**

**Организационна единица**

Съгласно §1, т.3 от Допълнителните разпоредби на ЗЗКИ „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; юридически лица; физически лица - в които се създава, обработва, съхранява или предоставя класифицирана информация.

**Задължения на организационните единици**

Организационните единици трябва: да прилагат изискванията за защита на класифицираната информация и да контролират тяхното спазване; да отговарят за защита на класифицираната информация; в случай на нерегламентиран достъп до класифицирана информация незабавно да уведомяват 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.

**Задължения на служителите в организационните единици, които имат достъп до класифицирана информация**

Служителите, получили разрешения за достъп до КИ отговарят за наличността да предадените им документи, 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.

Служителите в организационните единици, които имат достъп до класифицирана информация, са задължени:

- да спазват правила за работа с класифицирана информация;
- да защитават класифицираната информация от нерегламентиран достъп;
- да уведомяват незабавно служителя по сигурността на информацията за случаи на нерегламентиран достъп до класифицирана информация;
- да преминават периодични здравни прегледи най-малко веднъж на две години и психологически изследвания при условията и по реда на чл.42, ал.3 от ЗЗКИ;

На служителите получили разрешения за достъп до КИ е забранено:

- да разгласяват класифицирана информация в нарушение на законоустановения ред;
- да предават класифицирана информация по свързочни или комуникационни средства без съответните мерки за защита, както и да записват класифицирана информация на нерегистрирани предварително на отчет носители;
- да изнасят материали, съдържащи класифицирана информация, извън организационната единица и в нарушение на установения за това ред;
- да предават материали, съдържащи класифицирана информация, на други служби и ведомства и в нарушение на установения за това ред;
- да оставят след работно време материали, съдържащи класифицирана информация, в работното помещение (бюра, шкафове и др.), ако то не отговаря на съответните мерки за защита на информацията;
- да размножават, фотографират и унищожават материали, съдържащи класифицирана информация, в нарушение на установения за това ред;
- да записват КИ на нерегистрирани предварително на отчет магнитни носители;
- да използват материали, съдържащи класифицирана информация, за явни публикации, дипломни работи, дисертации, доклади, изказвания и др.

Служителите на службите за сигурност и за обществен ред са длъжни да уведомяват писмено ръководителите си за всяко задгранично пътуване.

**Персонална сигурност**

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

Мерките за защита на КИ в областта на персоналната сигурност гарантират достъпа до КИ във връзка с изпълнение на служебни задължения или конкретно възложени задачи след извършване на проучване на лицето за надеждност и

провеждане на обучението му в областта на защитата на класифицираната информация.

Лица, които не са служители в организационната единица, могат да се запознаят с регистрирани в нея материали само след разрешение на ръководителя на организационната единица и служителя по сигурността на информацията.

**Процедура по проучване**

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

За да стартира процедурата по проучване, трябва да има писмено съгласие на лицето, което може да бъде оттеглено на всеки от етапите на проучване. Ако лицето оттегли своето писмено съгласие, процедурата веднага се прекратява. Документите по чл. 147, ал. 1, т. 1 се връщат на лицето срещу писмена разписка, а въпросника по чл. 147, ал. 1, т. 2 и всички данни, събрани в хода на проучването, се унищожават по правилата на ППЗЗКИ.

Надеждност на лицето относно опазване на тайната е налице, когато в хода на проучването за надеждност се установява, че липсват данни относно укриване или даване на невярна информация от проучваното лице за целите на проучването, да липсват 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 на проучваното лице да работи с класифицирана информация, и не е зависимо от алкохол и наркотични вещества.

**Резултати от процедурата по проучване**

**Разрешение, отказ**

Разрешението се издава на лица, които отговарят на изискванията на чл. 40 от ЗЗКИ.

При необходимост от преиздаване на разрешение, когато срокът на валидност изтича, се започва процедура по повторно проучване, най - рано ***три месеца*** преди изтичането на валидността.

В хода на проучването може да се установи, че лицето не отговаря на изискванията по чл. 40, ал. 1 или че проучваното лице съзнателно е представило неверни или непълни данни. В такъв случай **проучващият орган издава отказ** за достъп до класифицирана информация. Отказът не се мотивира, а само се посочва правното основание и не подлежи на обжалване по съдебен ред.

**Отнемане и прекратяване**

По време на текущия контрол, който проучващият орган осъществява, може да установи, че са се появили 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.

Компетентни да издават, прекратяват, отнемат и отказват издаване на разрешение за достъп до класифицирана информация са:

- ДКСИ;
- ръководителите на службите за сигурност и службите за обществен ред;
- служителите по сигурността на информацията.

**Процедура по обжалване**

Органът, пред който лицето, на което е издаден отказ, отнемане или прекратяване, може да подаде жалба, е 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.

**Документална сигурност**

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

- „Строго секретно”
- „Секретно”
- „Поверително”
- „За служебно ползване”

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

- „Строго секретно“
- „Секретно“
- „Поверително“

Информацията, класифицирана като служебна тайна се маркира с гриф за сигурност „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 КИ, различен от посочените (втора дата). В този случай лицето посочва датата на изтичане на срока на защита на КИ в грифа за сигурност.

**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 вишестоящ ръководител.

Грифът за сигурност съдържа:

- ниво на класификация;
- дата на класифициране;
- дата на изтичане на срока на класификация, когато е различна от датата на изтичане на сроковете, определени за съответното ниво на класификация и;
- правното основание за класифициране.

Класифицирането на информацията е дейност, при която се установява:

1. Попада ли конкретната информация в списъка на категориите информация съгласно приложение № 1 към чл. 25 ЗЗКИ или в списъка по чл. 26, ал. 3 ЗЗКИ;
2. Налице ли е заплаха или опасност от увреждане или увреждане на интересите по т. 1 в съответната степен, определена съгласно чл. 28, ал. 2 и чл. 26, ал. 1 във връзка с § 1, т. 15 от допълнителните разпоредби на ЗЗКИ;
3. Дали нерегламентираният достъп до нея би създал опасност за интересите по т. 1, и
4. Налице ли са обществените интереси, подлежащи на защита съгласно чл. 25 и 26 във връзка с § 1, т. 13 и 14 от допълнителните разпоредби на ЗЗКИ.

**Информацията се класифицира според собственото ѝ съдържание**, а не според класификацията на информацията, на която се базира, или на информацията, за която се отнася.

**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.

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

Материалите (документите) носители на класифицирана информация се регистрират в регистратурите за класифицирана информация, като 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.

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

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 и служителят 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.

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.

Класифицирана информация може да се създава, обработва, съхранява или предоставя само в определените зони за сигурност (клас I и клас II).

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

Бележки или записки, съдържащи класифицирана информация, се правят на работни тетрадки или бележници, които са надлежно подвързани, с поредно номерирани листове и заведени на отчет в регистратурата; на носители, използвани в сертифицирана АИС или мрежа и заведени на отчет в регистратурата.

**Физическа сигурност**

Физическата сигурност на класифицираната информация включва система от организационни, физически и технически мерки за предотвратяване на нерегламентиран достъп до материали, документи, техника и съоръжения, класифицирани като държавна или служебна тайна.

Организационните единици прилагат система от мерки и средства за физическа сигурност на сгради, помещения и съоръжения, в които се създава, обработва и съхранява класифицирана информация.

Физическата сигурност се прилага за защита на класифицирана информация от всякаква заплаха или вреда в резултат на:

1. терористична дейност или саботаж;
2. нерегламентиран достъп или опит за нерегламентиран достъп.

За предотвратяване на нерегламентиран достъп до класифицирана информация ръководителите на организационните единици с помощта на служителите по сигурността на информацията:

1. определят зоните за сигурност;

2. определят около зоните за сигурност административни зони, в които се извършва контрол на хора и моторни превозни средства и които са с най-ниско ниво на сигурност;

3. въвеждат контролиран режим на влизане, движение и излизане от зоната за сигурност, както и задължително придружаване в тези зони на лица без право на достъп или с право на достъп до по-ниско ниво на класификация;

4. осигуряват съответен контрол над зоните за сигурност и административните зони чрез служители от звената по сигурност и охрана;

5. въвеждат специален режим за съхраняване на ключове от помещения, каси и други съоръжения, служещи за съхраняване на класифицирана информация.

За осигуряване защитата на класифицираната информация, представляваща държавна тайна, при срещи, разговори, съвещания, заседания и др., предмет на които е такава информация, се въвеждат допълнителни мерки за сигурност срещу подслушване и наблюдение.

Средствата за физическа сигурност, сертифицирани за всяко ниво на класификация за сигурност, се определят в списък, утвърден от ДКСИ.

**Сигурност на АИС/М**

Сигурността на автоматизираните информационни системи (АИС) или мрежи представлява система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежи.

Задължителните общи условия за сигурност на АИС или мрежи обхващат компютърната, комуникационната, криптографската, физическата и персоналната сигурност, сигурността на самата информация на всякакъв електронен носител, както и защитата от паразитни електромагнитни излъчвания, определени в наредба, приета от Министерския съвет по предложение на председателя на Държавна агенция "Национална сигурност".

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".

Не се допуска създаване, обработване, съхраняване и пренасяне на класифицирана информация в АИС или мрежи без наличието на издаден сертификат за тези АИС или мрежи по реда на този раздел.

Не се допуска включването на АИС или мрежи, предназначени за създаване, обработка, съхраняване и пренасяне на класифицирана информация към публични мрежи като Интернет и други подобни електронни комуникационни мрежи.

**Криптографска сигурност**

Криптографската сигурност представлява система от криптографски методи и средства, които се прилагат с цел защита на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне.

**Административнонаказателна отговорност по Закона за защитата на класифицираната информация**

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.

**Общи състави на нарушенията по ЗЗКИ**

***Съставът по чл.117 от ЗЗКИ – глоба от 2000 до 20 000 лв*.**

Нарушение на чл.17 от 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 ки;
- неосъществяване на контрол по спазването на изискванията за защита на КИ;
- неуведомяване незабавно на ДКСИ в случай на нерегламентиран достъп до КИ;
- непредприемане на мерки за ограничаване на неблагоприятните последици от нерегламентиран достъп до КИ;
- непредоставяне на информация на ДКСИ, службите за сигурност и службите за обществен ред.

Задължението по чл.11, ал.4, т.6 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 лицето, от което е поискана информацията, има качеството ОЕ, ще отговаря по чл.117 за непредоставянето ѝ. Ако няма това качество, отговорността е на базата на чл.132.

Задължението по чл.16, ал.1, т.5 – службите за обществен ред имат право да получават необходимата им във връзка с проучванията за надеждност информация от ОЕ.

***Съставът по чл.118 ЗЗКИ***

**Деяние:**

За служители в организационни единици, получили разрешение за достъп до КИ:

- да защитават КИ от нерегламентиран достъп;
- да уведомяват незабавно ССИ за случаи на нерегламентиран достъп до КИ;
- да уведомяват ССИ за всички случаи на промени на класифицираните документи и материали, при които не е налице нерегламентиран достъп;
- да преминават периодични здравни прегледи най-малко веднъж на 2 години и психологически изследвания при условията на чл.42, ал.3 ЗЗКИ;
- ако са получили разрешение за достъп до КИ с ниво на класификация „строго секретно“ 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 КИ;
- служителите на службите за сигурност и за обществен ред са длъжни да уведомяват писмено ръководителите си за всяко задгранично пътуване.

За лица, получили разрешение за достъп до КИ във връзка с изпълнението на конкретно възложена задача: длъжни са да спазват реда и условията за защита на КИ.

**Наказуемост** – Глоба от 50 до 300 лв.

***Съставът по чл.120 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”.

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, 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 или на негов вишестоящ ръководител;

• несъобщаване на получателите на информацията за промяната на нивото на класификация;

• неорганизиране на обучение от ръководителите на ОЕ на подчинените им служители за условията и реда за маркиране на информацията.

**Субект на административно наказателна отговорност:**

• лице, което има право да подписва документа, съдържащ класифицирана информация (лице по чл.31, ал.1);

• лице, което създава документ или материал, съдържащ КИ, но няма право да го подписва;

• вишестоящ ръководител на лицето по чл.31, ал.1;

• получател на информацията, чието ниво на класификация е променено;

• ръководител на ОЕ, който не организира обучение на подчинените си за маркиране на КИ;

**Наказуемост** – глоба от 100 до 500 лева.

***Съставът по чл.129 ЗЗКИ***

Който извърши или допусне извършването на нарушение по чл. 98, ал. 2 , се наказва с глоба от 500 до 1000 лв.

Когато нарушението по ал. 1 е извършено при осъществяване на дейност на юридическо лице, на същото се налага имуществена санкция в размер от 1000 до 5000 лв.

При извършване на проучването кандидатът попълва въпросник, определен с правилника за прилагане на закона.

При последващо настъпване на промени в данните, попълнени от кандидата във въпросника той се задължава незабавно да уведоми за това органа, извършил проучването.