ПЪРВОНАЧАЛНО ОБУЧЕНИЕ

ПО ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Нормативна уредба

- Закон за защита на класифицираната информация (ЗЗКИ);
- Правилник за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ).

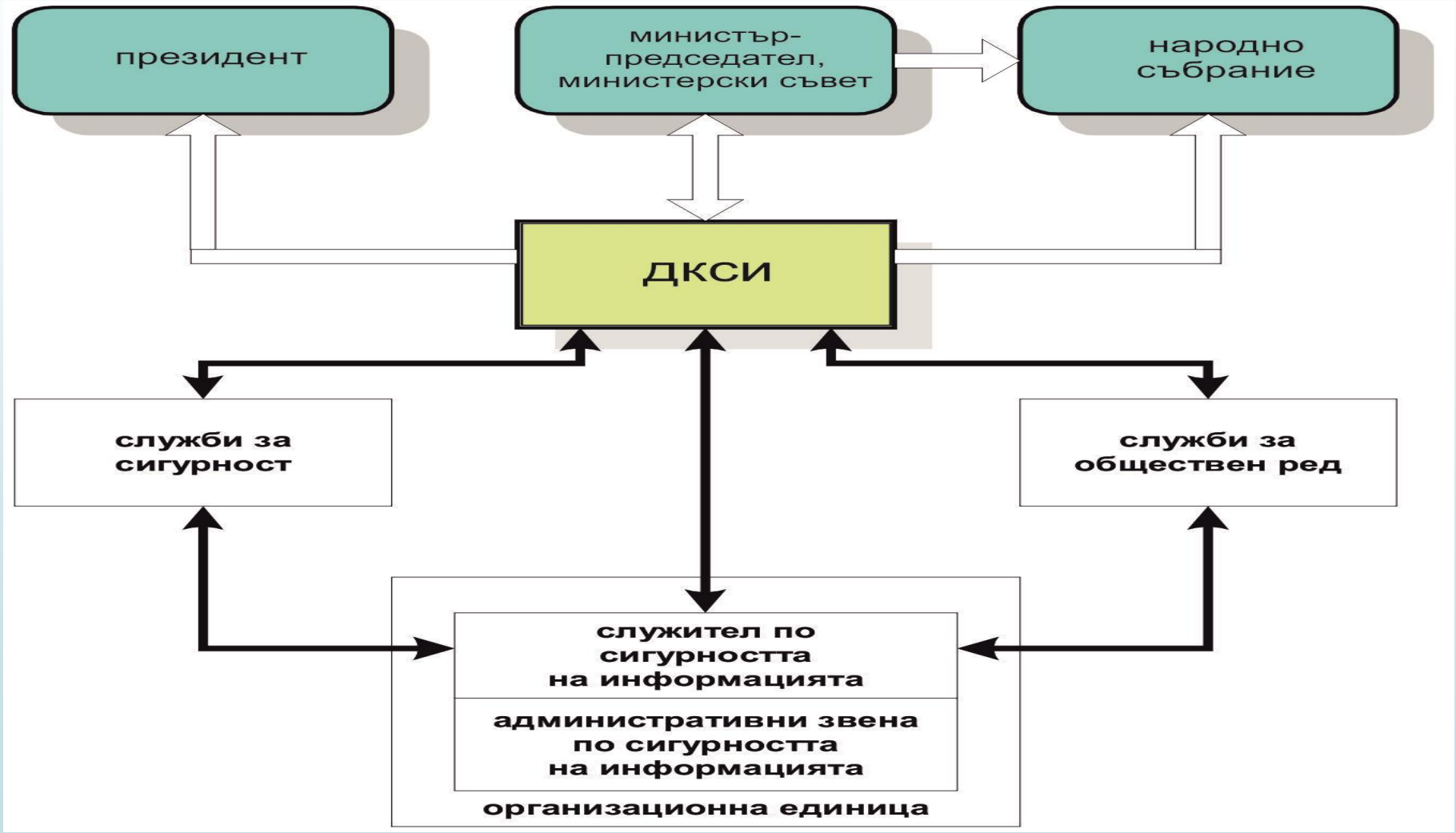
Общи положения

- Целта на Закона за защита на класифицираната информация е да защитава класифицираната информация 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.*

- Видове защита на класифицираната информация са: физическа, документална, персонална, индустриална, криптографска сигурност и сигурност комуникационните и информационните системи.

Органи за защита на класифицираната информация



Служби за сигурност

- Държавна агенция „Разузнаване“;
- Националната служба за охрана;
- Държавна агенция „Национална сигурност“;
- Главна дирекция „Борба с организираната престъпност“ и дирекция „Вътрешна сигурност“ на Министерството на вътрешните работи;
- Служба „Военно разузнаване“ на Министерството на отбраната;
- Държавна агенция „Технически операции“ и
- органите по чл. 16, ал. 2 от Закона за противодействие на корупцията и за отнемане на незаконно придобитото имущество

Служби за обществен ред

- Главна дирекция „Национална полиция“;
- Главна дирекция „Жандармерия, специални операции и борба с тероризма“,
- Главна дирекция „Гранична полиция“,
- Главна дирекция „Пожарна безопасност и защита на населението“;
- областните дирекции на МВР и
- служба „Военна полиция“ към министъра на отбраната.

Организационна единица (ОЕ)

ОЕ са органите на държавна власт и техните администрации, Министерството на отбраната и определени от министъра на отбраната структури на пряко подчинение на министъра на отбраната и формирования от Българската армия, органите на местното самоуправление и местната администрация, публичноправните субекти, създадени със закон или с акт на орган на изпълнителната власт, физическите и юридическите лица, в които се създава, обработва, съхранява или предоставя класифицирана информация.

ОЕ трябва да:

- прилагат изискванията за защита на класифицираната информация;
- контролират тяхното спазване;
- 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;
- предоставят информация по искане на ДКСИ, службите за сигурност и службите за обществен ред.

Задължения на служителите в ОЕ, които имат достъп до класифицирана информация

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

- да защитават класифицираната информация от нерегламентиран достъп;
- да уведомяват незабавно служителя по сигурността на информацията за случаи на нерегламентиран достъп до класифицираната информация;
- да уведомяват служителя по сигурността на информацията за всички случаи на промени на класифицираните материали и документи, при които не е налице нерегламентиран достъп;
- да преминават периодични здравни прегледи най-малко веднъж на две години и психологически изследвания при условията и по реда на чл. 42, ал. 3.

Задължения на служителите в ОЕ, които имат достъп до класифицирана информация

Служителите, получили разрешение за достъп до КИ:

- спазват правила за работа с класифицирана информация;
- отговарят за наличността на 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 на службите за сигурност и за обществен ред са длъжни да уведомяват писмено ръководителите си за всяко задгранично пътуване.

Задължения на служителите в ОЕ, които имат достъп до класифицирана информация

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.

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.

Документална сигурност

Документалната сигурност се състои в 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 регистратури за класифицирана информация.

Документална сигурност

Класифицирана информация:

- **Държавна тайна** е информацията, определена в списъка по приложение № 1, 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.
- **Служебна тайна** е информацията, създавана или съхранявана от държавните органи или органите на местното самоуправление, която не е държавна тайна, нерегламентираният достъп до която би се отразил неблагоприятно на интересите на държавата или би увредил друг правнозащитен интерес.
- **Чуждестранна класифицирана информация** е класифицираната информация, предоставена от друга държава или международна организация по силата на международен договор, по който Република България е страна.

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“

Информация, класифицирана като служебна тайна, се маркира с гриф за сигурност „За служебно ползване“.

Документална сигурност

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**.

Документална сигурност

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

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.

Документална сигурност

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

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.

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 временен 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.

Документална сигурност

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

Нивото на класификация на документ, включващ приложения, съответства поне на най-високото ниво на класификация на тези приложения.

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 от ЗЗКИ или в списъка по чл. 26, ал. 3 от 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.

Документална сигурност

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

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.

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.

Документална сигурност

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 или на носители, използвани в сертифицирана КИС и заведени на отчет в регистратурата.

Лица, които не са служители на организационната единица, могат да се запознават със съдържанието на регистрирани в нея документи само след разрешение на ръководителя на организационната единица или на служителя по сигурността на информацията, ако имат съответно разрешение за достъп до класифицирана информация и при спазване на принципа „Необходимост да се знае“.

Персонална сигурност

Персоналната сигурност представлява система от принципи и мерки, прилагани от компетентните органи по съответния ред 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 обучение в областта на защитата на класифицираната информация.

Индустриалната сигурност

Индустриалната сигурност представлява система от принципи и мерки, които се прилагат по отношение на кандидати - физически и юридически лица, при сключването или изпълнението на договор, свързан с достъп до класифицирана информация, с цел защитата й от нерегламентиран достъп.

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.

Сигурност на комуникационните и информационните системи (КИС)

Сигурност на комуникационните и информационните системи (КИС) представлява система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в КИС.

Целта на прилаганата система от мерки е осигуряването на трите характеристики на класифицираната информация в КИС – конфиденциалност, интегритет и достъпност на тази информация.

Административно-наказателна отговорност

Административно-наказателна отговорност носят всички лица, получили разрешение за достъп до класифицирана информация.

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.