МИНИСТЕРСТВО НА ОТБРАНАТА
СЛУЖБА ВОЕННА ИНФОРМАЦИЯ
София 1000, ул. “Дякон Игнатий” №3

Първоначално обучение
по защита на класифицираната информация

Общи положения

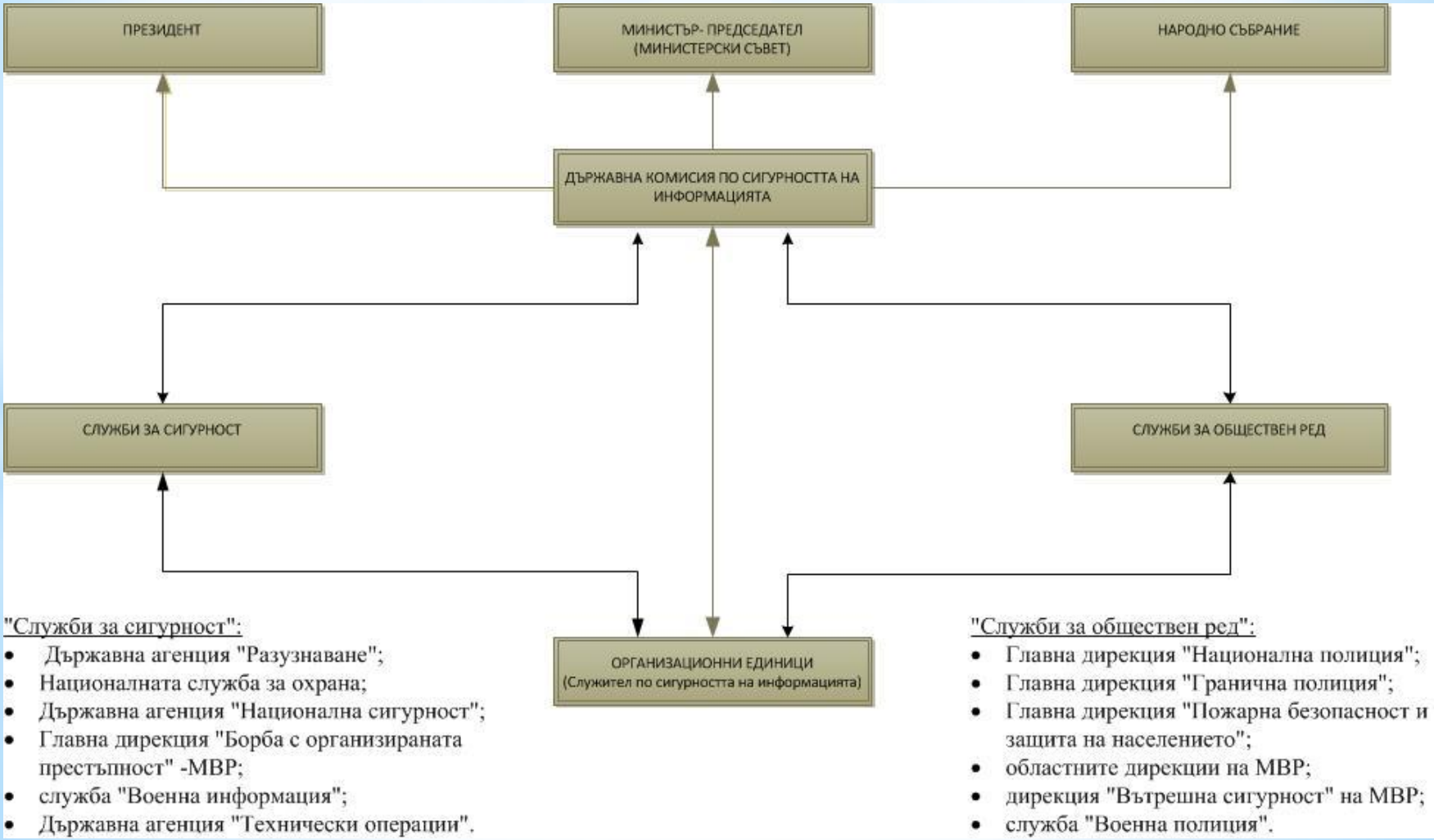
Целта на Закона за защита на класифицираната информация е да я защитава от нерегламентиран достъп.

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".

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

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



"Служби за сигурност":

- Държавна агенция "Разузнаване";
- Националната служба за охрана;
- Държавна агенция "Национална сигурност";
- Главна дирекция "Борба с организираната престъпност" -МВР;
- служба "Военна информация";
- Държавна агенция "Технически операции".

"Служби за обществен ред":

- Главна дирекция "Национална полиция";
- Главна дирекция "Гранична полиция";
- Главна дирекция "Пожарна безопасност и защита на населението";
- областните дирекции на МВР;
- дирекция "Вътрешна сигурност" на МВР;
- служба "Военна полиция".

МИНИСТЕРСТВО НА ОТБРАНАТА
СЛУЖБА ВОЕННА ИНФОРМАЦИЯ
София 1000, ул. "Дякон Игнатий" №3

Задължения на служителите в организационните единици, които имат достъп до 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 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 от ЗЗКИ;
• служителите на службите за сигурност и за обществен ред са длъжни да уведомяват писмено ръководителите си за всяко задгранично пътуване.

Служителите, получили разрешения за достъп до КИ:

- 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 КИ и да изнасят КИ извън организационната единица в нарушение със законоустановения ред;
- нямат право да записват КИ на нерегистрирани предварително на отчет магнитни носители;
- нямат право да използват материали, съдържащи КИ, за явни публикации, дипломни работи, дисертации, доклади и др.;
- нямат право да размножават и унищожават материали, съдържащи КИ, в нарушение на установения за това ред.

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

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 защита на класифицираната информация.

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.

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.

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.

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.

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.

Персонална сигурност

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.

Целта на процедурата по проучване е да се установи дали проучваното лице отговаря на законовите изисквания.

Компетентни да издават, прекратяват, отнемат и отказват издаване на разрешение за достъп до класифицирана информация са: ДКСИ, ръководителите на службите за сигурност, службите за обществен ред и служителите по сигурността на информацията.

ДОКУМЕНТАЛНА СИГУРНОСТ

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“.

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

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

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;
- 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.

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

МИНИСТЕРСТВО НА ОТБРАНАТА
СЛУЖБА ВОЕННА ИНФОРМАЦИЯ
София 1000, ул. "Дякон Игнатий" №3

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 класифициран информация се регистрират в регистратурите за класифицирана информация, като на видно място се поставя **уникален регистрационен номер.**

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

Работата с материали (документи), 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.

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.

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

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".

АДМИНИСТРАТИВНО-НАКАЗАТЕЛНА ОТГОВОРНОСТ

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

Всяко нарушение на ЗЗКИ и подзаконовите актове по прилагането му е административно нарушение и се санкционира с предвиденото в чл. 132 ЗЗКИ наказание.

Органът, издал разрешението за достъп до класифицирана информация, отнема издаденото разрешение, когато лицето е извършило системни нарушения на закона или на подзаконовите актове, свързани със защитата на класифицираната информация.

"Системни нарушения" са три или повече нарушения на закона или на нормативните актове по неговото прилагане, извършени в продължение на една година.

КРАЙ