С О Ф И Й С К И В О Е Н Е Н СЪД

ПЪРВОНАЧАЛНО ОБУЧЕНИЕ ПО ЗАЩИТА НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Тема № 1 – „Рискови фактори в областта на защита на класифицирана информация“.

Тема № 2 – „Национална система за защита на класифицираната информация“.

Тема № 3 – „Понятие за организационна единица“

Тема № 4 – „Контрол на дейността по защита на класифицираната информация. Условия и ред за извършване на проверките по прекия контрол“.

Тема № 5 – „Действия в Случай на нерегламентиран достъп до класифицирана информация“.

Тема № 6 – „Административнонаказателна отговорност.“

Тема № 7 – „Видове защита на класифицираната информация“

Тема № 1

„Рискови фактори в областта на защита на класифицирана информация“.

1. Риск, опасност, заплаха. Сравняване и разграничаване на понятията:

а) ***“Заплаха”*** е пряка, реална, непосредствена опасност. Закана да се причини някому нещо неприятно, зло. (според тълконвния речник).

б) ***„Опасност“,*** е възможност или вероятност да се слуги нещо лошо, някаква беда, нещастие.

в) ***„Риск“*** при него няма предварително определено време за настъпването му. Дори да бъде установен рано, той си остава принципно невъзможен за неутрализиране.

2. ***“Асиметрична заплаха”*** е вид заплаха, в която се съдържат неконвенционални, нетрадиционни, непознати и неочакване за противника тактики, действия или средства, срещу които противникът не може да противодейства успешно. Тя представлява мислене, организация и действие, различни от тези на противника, с цел да се увеличат собствените предимства и да се използват слабостите на противника. Асиметрията е използване на различията с цел постигане на предимство над противника.

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

а) Разлика между *заплаха* и *опасност*:

- *заплахата* е сега, тя е реален факт, проявено обстоятелство; на заплахата трябва да се противостои.

- *опасността* е свързана с възможно бъдещо развитие; опасността се крие в сферата на възможното; опасността трябва да се предвиди и да се направи необходимото за да се избегне;

б) Разлика между *заплаха* и *риск*:

- *рискът* е вероятност от възникване на заплаха вследствие определени действия на „собствената страна“; заплахата е категория, която характеризира действията на „другата страна“.
- *заплахата* е категория, която характеризира действията на „другата страна“.

4. Видове заплахи:

а) *Природни* заплахи;

б) Заплахи в резултат на *човешка дейност* (умишлена и по непредпазливост);

4.1. Заплахи в резултат на умишлена човешка дейност:

4.1.1. традиционни (общи);

4.1.2. специфични.

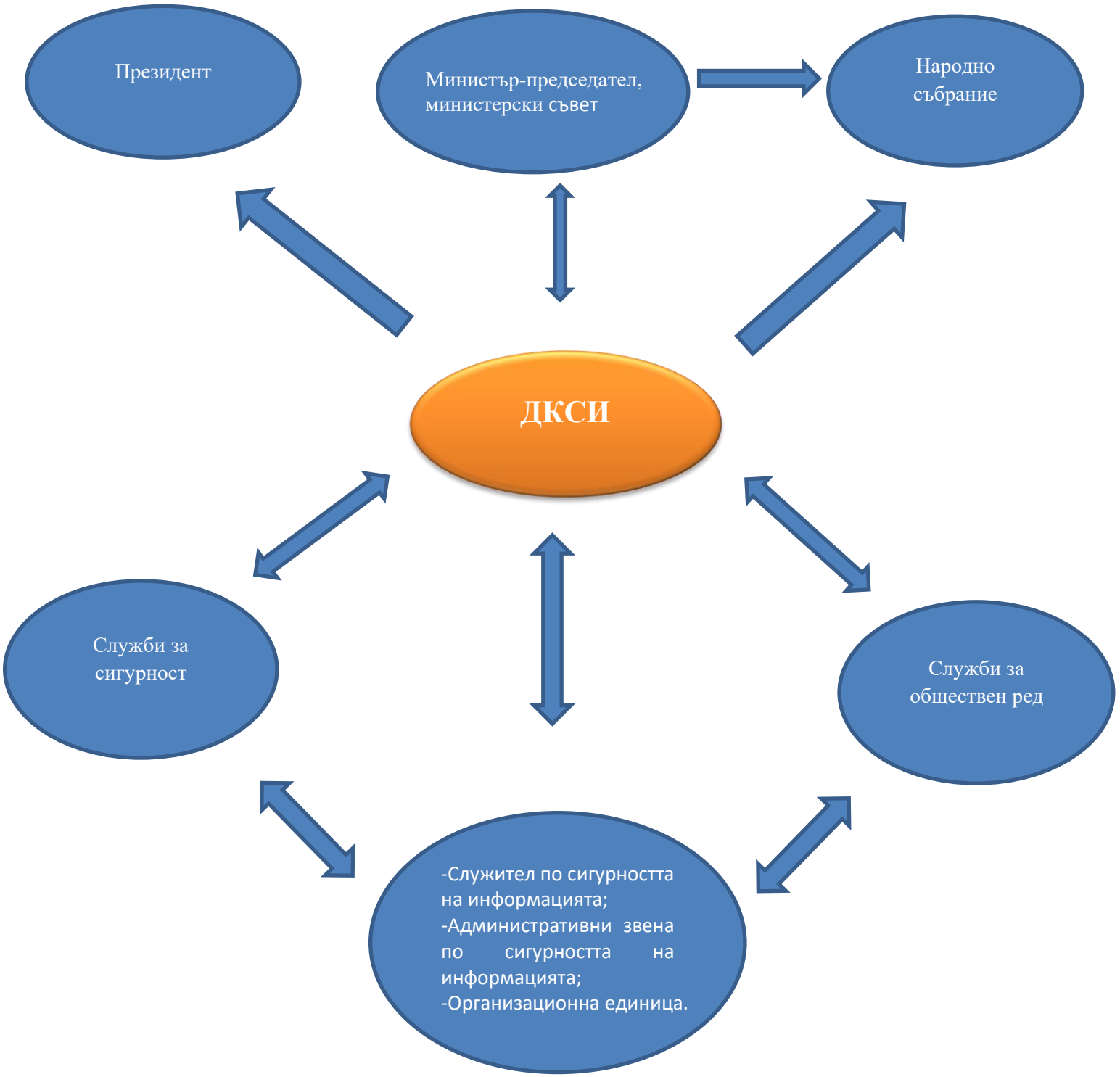
в) *Традиционни*:

- глобални;
- регионални;
- вътрешно-държавни;
- към физически лица и материални обекти.

г) *Глобални* заплахи:

- според посоката;
- според проявеността;
- от областта на действие;
- по времево действие;
- по характер.

„Винаги има опасност,
почти винаги има риск,
но не винаги има заплаха“


Президент
Министър-председател, министерски съвет
Народно събрание
ДКСИ
Служби за сигурност
Служби за обществен ред
-Служител по сигурността на информацията;
-Административни звена по сигурността на информацията;
-Организационна единица.

Фиг. № 1

Тема № 2

„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 - фиг. № 1.

1.1. 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.

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

1.3. 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).

1.4. 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:

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

1.4.2. да взема решения за пътищата и средствата за предотвратяването им;

1.4.3. 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.

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

1.6. 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.

Тема № 3

„Понятие за организационна единица“.

1. Организационна единица

а) 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.

б) 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.

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

Организационните единици трябва:

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

2.2. да отговарят за защитата на класифицираната информация;

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

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

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

3.1. 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.

3.2. 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.

3.3. 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.

Тема № 4

„Контрол на дейността по защита на класифицираната информация. Условия и ред за извършване на проверките по прекия контрол“.

1. 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.

2. 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.

3. **Същност на контрола по защитата на класифицираната информация.**

а) 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.

б) 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.

в) 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.

4. 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.

5. 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.

6. **Органи по контрола**

6.1. 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.

6.2. 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.

6.3. 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.

7. **Цел на контрола**

7.1. 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.

7.2. 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.

8. **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:

8.1. организационната единица – обект на проверката;

8.2. обхвата и продължителността на проверката;

8.3. председателя и членовете на комисията по проверката в случаите, когато има сформирана такава комисия и привлечените при необходимост експерти;

8.4. реда за докладване на резултатите от проверката;

8.5. 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.

Тема № 5

„Действия в случай на нерегламентиран достъп до класифицирана информация“.

1. 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 ѝ или до загубване на такава информация.

2. 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.

3. 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.

4. 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.

5. 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.

6. Действия на служителя по сигурността на информацията и ръководителя на организационната единица при случай на нерегламентиран достъп до класифицирана информация:

6.1. 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.

6.2. От организационната единица следва да се предприемат мерки за предотвратяване и/или ограничаване на неблагоприятните последици от реализирането на НДКИ.

6.3. Организационната единица извършва оценка на нанесените вреди и я предоставя на компетентния проверяващ орган.

1. Служителят по сигурността на информацията води на отчет случаите на НДКИ и на взетите мерки, за което информира незабавно ДКСИ.

Тема № 6

„Административно-наказателна отговорност“

1. Административно-наказателната отговорност се изразява в осъществяване на санкции, предвидени за виновно неизпълнение или лошо изпълнение на административни задължения.

2. Тя е властническо наказателна мярка, израз на държавно наказателна репресия. Тя е вид наказание, т.е. властническа наказателна мярка, израз на държавна наказателна репресия.

3. Административно-наказателна 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).

4. Не е необходимо от деянието да са настъпили определени неблагоприятни резултати – заплаха от увреждане или увреждане на определени обществени отношения.

5. 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.

6. Административно-наказателна отговорност не влече последици за съдимост и се реализира от самата администрация.

7. Същността на административно-наказателната отговорност се определя от три понятия:

7.1. административно нарушение;

7.2. административно наказание и

7.3. ред за налагате на административните наказания.

8. **Административно-наказателно отговорни лица**

8.1. Според чл. 26, ал. 1 от ЗАНН, административно-наказателно 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.

8.2. 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).

8.3. Непълнолетните, които са навършили 16 години и са могли да разбират свойството и значението на извършеното нарушение и да ръководят постъпките си, също са административно-наказателно отговорни.

8.4. 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.

8.5. ***ЗАНН установява принципа, че административно-наказателната отговорност е лична.***

Тема № 7

„Видове защита на класифицираната информация“

1. Физическа 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 е част от общите изисквания за сигурност по защита на класифицираната информация и включва общи и конкретни мерки, оценка на заплахите, както и изискванията и стандартите за физическата сигурност на класифицираната информация.

1.1. Системата от мерки има за цел:

1.1.1. да защити сградите, помещенията и съоръженията, в които се създава, обработва и съхранява класифицирана информация;

1.1.2. да създаде организация за осъществяване на ефективен контрол върху достъпа до тях.

1.2. Съгласно Закона за защита на класифицираната информация, 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.

2. Документална сигурност

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 (чл. 80, ал. 1 от ЗЗКИ). 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 (ППЗЗКИ).

3. 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 защита на класифицираната информация. Принципите и мерките по персонална сигурност включват

принципа „необходимост да се знае“, процедурата по проучване на лицата и издаването на разрешение за достъп по глава пета от ЗЗКИ, провеждането на обучение на лицата по реда на закона и правилника за неговото прилагане и осъществяването на контрол в тази област (чл. 83, ал. 1 и 2 от ЗЗКИ)

4. Криптографска сигурност

4.1. 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.

4.2. Условията и редът за използването, производството и вносът на криптографски методи и средства за защита на класифицираната информация се определят с Наредбата за криптографската сигурност на класифицираната информация (НКСКИ).

4.3. Орган по криптографската сигурност на Република България (ОКС) по смисъла на НКСКИ е Държавна агенция "Национална сигурност".

4.4. Съгласно ЗЗКИ и НКСКИ ДКСИ осъществява общото ръководство и контрол на дейностите по криптографска сигурност на класифицираната информация.

4.5. Криптографските средства и материали за защита на класифицирана информация, както и ключовите материали, се маркират, съхраняват, отчитат, архивират и унищожават по реда на Наредбата за криптографската сигурност на класифицираната информация.

4.6. При съмнения за компрометиране или при компрометиране на криптографската сигурност ОКС изготвя писмено становище, което се изпраща до ДКСИ. В случай, че компрометирането на криптографската сигурност засяга криптографски мрежи, в които се обработва информация на други държави или международни организации, те се информират в съответствие с двустранните договорености по сигурността.

5. Сигурност на комуникационни информационни системи

5.1. Сигурността 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.

5.2. Задължителните общи условия за сигурност на КИС обхващат компютърната, комуникационната, криптографската, физическата, документалната и персоналната сигурност, сигурността при свързване на КИС, контрамерките по TEMPEST, определени в наредба, приета от Министерския съвет.

5.3. Преди въвеждане в експлоатация за работа с класифицирана информация за всяка КИС се провежда процедура по акредитиране при условията и по реда, определени с наредбата по чл. 90, ал. 1 от ЗЗКИ.

5.4. Орган по акредитиране на сигурността на национални КИС, предназначени за работа с национална класифицирана информация, в които се обработва и класифицирана информация на НАТО и на ЕС, е Специализирана дирекция „Информационна сигурност“ в Държавна агенция „Национална сигурност“.

5.5. ДКСИ в качеството си на национален орган по сигурността и по прилагането и контрола по изпълнението на международните договори за взаимна защита и обмен на класифицирана информация, съгласно чл. 9, т. 6 от ЗЗКИ, извършва акредитиране на сигурността на точки на присъствие на КИС на НАТО или на ЕС и взаимната свързаност на национални КИС с тях.

5.6. За специално изтриване на 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.

6. Индустриална сигурност

6.1. 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 ѝ от нерегламентиран достъп (чл. 95, ал. 1 от ЗЗКИ).

6.2. Процедурата се инициира по два начина: от възложител или след регистриране за участие в поръчки на НАТО в базата данни на Министерството на икономиката.

6.3. Във връзка с подготовката и изпълнението на обществена поръчка, свързана с достъп до класифицирана информация, инициирането на процедурата по проучване за надеждност се извършва от възложителя. Освен изискуемите документи за проучване на служителите на кандидата за участие в обществената поръчка, възложителят е длъжен да приложи и определени документи.