ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
1505 СОФИЯ, ул.”Черковна” № 90
тел.: +3592 9333 600; факс: +3592 9873 750; e-mail: dksi@government.bg

МЕТОДИКА ЗА ИЗГРАЖДАНЕ И ОЦЕНКА НА СРЕДСТВАТА И СИСТЕМИТЕ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

(приета на заседание на ДКСИ с Протокол № 165-I/30.06.2004г., изм. с Решение № 2-I/08.01.2009 г., Решение №26-I/10.04.2012г., Решение № 55-I/21.07.2015 г.)

София
2015 г.

АНОТАЦИЯ

“Методика за изграждане и оценка на средствата и системите за физическа сигурност на класифицирана информация” представлява документ, създаден в резултат на работата на сформираната по инициатива на ДКСИ постоянна работна група по физическа сигурност, като са използвани становищата на специализираните подгрупи “Архитектурно – строителна част”, “Електроника – системи за сигурност (СОТ), контрол на достъпа в зоните за сигурност и системи за видеонаблюдение”, “Пожароизвестителни и пожарогасителни системи”, “Метални каси и шкафове и заключващи механизми” и “Защита от подслушване”, както и чешкия опит в тази област.

СЪДЪРЖАНИЕ:

ВЪВЕДЕНИЕ	**4**
1. МЕТАЛНИ КАСИ И ШКАФОВЕ И ЗАКЛЮЧВАЩИ МЕХАНИЗМИ	**5**
2. ЗОНИ НА СИГУРНОСТ И ЗАКЛЮЧВАЩИ СИСТЕМИ	**9**
3. ГРАНИЦА НА ОБЕКТА	**15**
4. КОНТРОЛ НА ФИЗИЧЕСКИЯ ДОСТЪП В ЗОНАТА ЗА СИГУРНОСТ ИЛИ ОБЕКТА, ПРОИЗВОЛЕН КОНТРОЛ И РЕЖИМ НА ВЛИЗАНЕТО	**17**
5. ОХРАНА И АЛАРМЕНИ СИСТЕМИ ПРОТИВ ПРОНИКВАНЕ /АСПП/, КОНТРОЛ НА ДОСТЪПА И ВИДЕОНАБЛЮДЕНИЕ	**20**
6. ЗАЩИТА НА ПЕРИМЕТЪРА	**27**
7. ПОЖАРОИЗВЕСТИТЕЛНИ И ПОЖАРОГАСИТЕЛНИ СИСТЕМИ	**29**
8. ДЕТЕКТОРИ НА СУБСТАНЦИИ ИЛИ СРЕДСТВА, ИЗПОЛЗВАНИ ГЛАВНО ЗА ОТКРИВАНЕ НА МЕТАЛИ	**30**
9.РЕЗАЧКИ ЗА УНИЩОЖАВАНЕ НА ИНФОРМАЦИОННИ НОСИТЕЛИ	**30**
10.ИЗИСКВАНИЯ ЗА ЗАЩИТА СРЕЩУ НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ И ИЗИСКВАНИЯ ЗА ЗАЩИТА НА ОБОСОБЕНИ ТЕХНИЧЕСКИ ОСИГУРЕНИ ЗОНИ	**33**
11. УСЛОВИЯ ЗА ИЗПОЛЗВАНЕ НА СЕРТИФИЦИРАНИТЕ ТЕХНИЧЕСКИ СРЕДСТВА ОТ ОТДЕЛНИТЕ КАТЕГОРИИ	**34**
12. ОЦЕНКА НА ЕЛЕМЕНТИТЕ НА ФИЗИЧЕСКАТА СИГУРНОСТ	**37**
13. МИНИМАЛНИ ИЗИСКВАНИ ПОКАЗАТЕЛИ ЗА ОЦЕНКА НИВОТО НА ФИЗИЧЕСКАТА СИГУРНОСТ	**41**

ВЪВЕДЕНИЕ:

Методиката за изграждане и оценка на средствата и ситемите за физическа сигурност на класифицираната информация представлява разпоредби, които допълват НАРЕДБАТА за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

Тези разпоредби относно прилагането на средствата за физическа сигурност за целите на защита на класифицираната информация изграждат относителен комплекс от взаимносвързани правила. Необходимо е да се вземе предвид качеството на използваните технически средства, начина на тяхното прилагане и не на последно място, взаимодействието на дадено техническо средство със съблюдаването на охраната и подходящите за района мерки. За да може да се реализира взаимодействието на тези комбинации от мерки за сигурност и да се установят унифицирани правила за минимално възможното ниво на гарантиране на класифицираната информация, е необходимо да се използва математически метод, който представя мерките за сигурност чрез определени числени обозначения, сумата от които се оценява по съответния начин. На основата на оценката е възможно да се определи дали мерките за сигурност спрямо определено ниво на класифицирана информация и определана степен на риск, са достатъчни и ако това не е така, да се намери оптималният начин за завишаване до исканото ниво. Преимуществото на този метод (наистина малко по-сложен от обикновеното изреждане на необходимите мерки за сигурност) се състои в това, че за определено ниво на сигурност може да се избере комбинация от средства за сигурност, така че да се намери най-добро решение, което да отговаря на определението нужди и да съответства на финанасовите и технически възможности на обекта.

Методиката е структурирана по следния начин: в главите от 1 до 10 са описани основните мерки за сигурност, които включват технически средства, физическа сигурност и режимни мерки. Описанието се спира детайлно на качеството на тези мерки и в повечето случаи то се оценява в точки. В глава 11 са описани правила за използване на сертифицирани технически средства. В глава 12 във формата на прости математически формули са определени отношенията между стойностите на мерките за сигурност. Глава 13 се състои от таблици с минималните стойности на оценката (точките), които са необходими за даденото ниво на класифицирана информация в отговор на определена степен на риск.

1. МЕТАЛНИ КАСИ И ШКАФОВЕ И ЗАКЛЮЧВАЩИ МЕХАНИЗМИ

Защитената каса може да се категоризира според устойчивостта й срещу насилствено и скрито проникване. В случай, че рискът от неосезаемо проникване е по-висок от риска от проникване с взлом, е целесъобразно да се предложи използването на каса от по-нисък тип (напр. тип2) заедно с ключалка от по-горен тип (напр. тип 4)

1.1. КАСА (контейнер, сейф, шкаф)

1.1.1. Каса – тип 4	SS1= 4 точки

Каса тип 4 може да се използва за съхраняване на класифицирана информация от всички нива на защита, намираща се в зоната на сигурност – клас I или II (вж. Втора глава)

Изисквания:

Касата е огнеупорна, бронирана, с две заключващи устройства.

Изисквания според БДС и стандартите на Европейския съюз **:**

Каса тип 4 отговаря на изискванията за сигурност за клас 4 или по-висок според стандарт БДС EN 1143-1.

Съгласно стандарт БДС EN 1143-1, каса тип 4 трябва да бъде оборудвана с ключалка минимум клас В според стандарт EN 1300.

Изисквания на НАТО:

Каса тип 4 е определен за съхранение на класифицирана информация от степен СВЕТОВНО СТРОГО СЕКРЕТНО (козмик топ сикрет) или по-ниска при условие, че се намира в зона на сигурност от клас I и II.

В случай, че в каса от тип 4 се съхранява криптографска класифицирана информация, то тогава тя трябва да бъде оборудвана с шифрова ключалка, поне (най-малкото) тридискова.

1.1.2. Каса – тип 3	SS1 = 3 точки

Каса тип 3 може де се използва за съхранение на класифицирана информация от всички степени на класификация, при условие, че тя се намира в зоната на сигурност (вж. Глава втора)

Изисквания:

Каса тип 3 е огнеупорна, с едно заключващо устройство.

Изисквания според БДС и стандартите на Европейския съюз **:**

Каса тип 3 отговаря на изискванията за сигурност за клас III или по-висок според стандарт БДС EN 1143-1.

Съгласно стандарт БДС EN 1143-1, каса тип 3 да бъде оборудвана с ключалка минимум клас B според стандарт EN 1300.

Изисквания на НАТО:

Каса тип 3 е определена за съхранение на класифицирана информация с ниво НАТО СЕКРЕТНО и НАТО ПОВЕРИТЕЛНО или по-ниски нива. За съхранение на класифицирана информация СВЕТОВНО СТРОГО СЕКРЕТНО тази каса трябва де се използва само в случай, че е оборудвана с ключалка от категория C, съгласно европейския стандарт EN 1300 (ключалка тип 4, вж.1.2.2). И двата варианта са валидни при условие, че касата се намира в зона на сигурност клас I и II.

В случай, че в каса тип 3 се съхранява криптографска класифицирана информация, то тогава тя трябва да е оборудвана с шифрова ключалка, поне (най-малкото) тридискова.

1.1.3. Каса – тип 2	SS1 = 2 точки

Каса тип 2 не може да се използва за съхранение на класифицирана информация от степен СТРОГО СЕКРЕТНО и СЕКРЕТНО. Класифицирана информация от по-ниска степен може да се съхранява, ако касата се намира в зона за сигурност (вж. Глава втора).

Изисквания:

Каса тип 2 представлява метален шкаф с едно заключващо устройство.

Изисквания според БДС и стандартите на Европейския съюз:

Каса тип 2 отговаря на изискванията за сигурност на клас 0, I и II според БДС EN 1143-1.

Съгласно БДС EN 1143-1 каса тип 2 трябва да бъде оборудвана ключалка минимум клас A според EN 1300 (ключалка тип 2, вж.1.2.3)

Изисквания на НАТО:

Каса тип 2 може да се използва само за съхранение на класифицирана информация с ниво НАТО ОГРАНИЧЕНО при условие, че тя се намира в зона на сигурност клас I и II.

1.1.4. Каса – тип 1	SS1 = 1 точка

Каса тип 1 може да се затваря и заключва. Каса тип 1 може да се използва за съхранение на класифицирана информация с ниво ПОВЕРИТЕЛНО при условие, че се намира в зона за сигурност (вж. Втора глава) или ЗА СЛУЖЕБНО ПОЛЗВАНЕ.

Изисквания:

Каса тип 1 представлява метален канцеларски шкаф с едно заключващо устройство.

Изисквания на НАТО:

Каса тип 1 може да се използва само за съхранение на информация с ниво НАТО ОГРАНИЧЕНО.

1.2. ЗАКЛЮЧВАЩИ МЕХАНИЗМИ (заключващи устройства, ключалки)

Инструкции за работа с ключовете на касите/сейфовете

Боравенето с ключовете на касите се урежда съгласно чл. 23 от Наредбата за системата от мерки, способи и средства за физическа сигурност на класифицираната информация и за условията и реда за тяхното използване.

Определената комбинация за заключване на ключалката трябва да се научи наизуст от лицата, които ползват касата. Защитените каси имат по два ключа. Шифровите комбинации на защитените каси се определят от служителя, на когото е зачислена съответната каса. Резервни ключове и записана комбинация от цифри (код) за отваряне в случай на непредвидени обстоятелства, трябва да се съхраняват в запечатана непрозрачна опаковка в дежурната част, съответно при ръководителя на звеното за сигурност или охраната в организационната единица. Резервните ключове и шифровите комбинации се използват само при извънредни случаи. Ключовете, които се използват постоянно и резервните ключове се съхраняват в отделни каси. Записът на всяка шифрова комбинация се съхранява в отделни пликове. Всички ключове, писмени шифрови комбинации и пликове се поставят под защита не по-ниска от защитата на класифицираната информация, към която те осигуряват достъп. Служителят, на когото е зачислена защитената каса, е длъжен да възпроизвежда единствено по памет шифровата комбинация. Забранява се писменото възпроизвеждане на шифровата комбинация, освен в случаите на чл.23, ал.5 от Наредбата.

Шифровите комбинации се променят в следните случаи:

- при сервизното обслужване на касата;
- при смяна на някои от лицата, които знаят комбинацията;
- когато се установи нерегламентиран достъп или опит за нерегламентиран достъп до класифицирана информация;
- през период не по-дълъг от 12 месеца.

1.2.1 Заключващо устройство – тип 4	SS2 = 4 точки

Заключващо устройство тип 4 осигурява висока степен на устойчивост срещу професионално проникване, при което се използват изключително високи технологии и инструменти, недостъпни в търговската мрежа.

Изисквания:

Заключващо устройство тип 4 представлява секретен патрон, защитен срещу разпробиване и чупене, и допълнителна секретна или касова брава.

Изисквания според БДС и стандартите на Европейския съюз:

Заключващо устройство тип 4 отговаря на изискванията за сигурност клас В или по-висок според БДС EN 1300 и EN 1300.

1.2.2. Заключващо устройство – тип 3	SS2 = 3 точки

Заключващо устройство тип 3 осигурява степен на устойчивост срещу професионално проникване, при което се използват технологии и инструменти, които са пазарно достъпни за професионалния ключар .

Изисквания:

Заключващо устройство тип 3 представлява секретен патрон, защитен срещу разпробиване и чупене

Изисквания съгласно БДС и стандартите на Европейския съюз:

Заключващо устройство тип 3 отговаря на изискванията на категория за сигурност клас В или по-висок според БДС EN 1300 и EN 1300.

1.2.3. Заключващо устройство – тип 2	SS2 = 2 точки

Заключващо устройство тип 2 осигурява степен на устойчивост срещу проникване с употреба на минимални средства

Изисквания:

Заключващо устройство тип 2 представлява секретен патрон, защитен срещу разпробиване и чупене.

Изисквания според БДС и стандартите на Европейския съюз:

Заключващо устройство тип 2 отговаря на изискванията за сигурност клас А според БДС EN 1300 и EN 1300.

1.2.4. Заключващо устройство – тип 1	SS2 = 1 точка

Заключващо устройство тип 1 осигурява устойчивост срещу неразрешено отваряне от страна на случаен нарушител.

Изисквания:

Заключващо устройство тип 1 представлява секретен патрон

Изисквания според БДС и стандартите на Европейския съюз:

Заключващо устройство тип 1 отговаря на изискванията за сигурност клас А според БДС EN 1300 и EN 1300.

2. ЗОНИ ЗА СИГУРНОСТ И ЗАКЛЮЧВАЩИ СИСТЕМИ

За типа на зоната за сигурност решаваща е тази част от границата на зоната, която има най-ниска степен на устойчивост.

Когато зоната за сигурност се състои от едно помещение, долните условия са валидни за цялата й граница. Когато зоната за сигурност се състои от повече помещения, следващите условия са валидни само за границата на защитения район.
Когато зоната за сигурност се състои от трезор, входът за него не трябва да бъде в тази част на границата на зоната за сигурност, която същевременно е граница на обекта. В този случай отметката S 2 е 0.

Механична защита означава защита на отвори, които позволяват преминаването на шаблон със следните размери:

Отвор	Размер
Продълговат	400 мм х 250 мм
Елипсовиден	400 мм х 300 мм
Кръгъл	Диаметър 350 мм

2.1. ЗОНА ЗА СИГУРНОСТ

Ръководителите на организационните единици с помощта на служителите по сигурността на информацията определят със заповед зоните за сигурност в зависимост от нивото на класификация и начина на създаване, обработване, съхраняване и предоставяне на информацията. Видовете зони за сигурност, в които се създава, обработва, съхранява или предоставя класифицирана информация, са Зона за сигурност клас I и Зона за сигурност клас II.

ЗОНА ЗА СИГУРНОСТ КЛАС I :

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.

Изисквания:

1. Ясно определен охраняван периметър, към който всички входове и изходи се контролират;
2. Система за контрол на физическия достъп, позволяваща влизането само на лица, притежаващи разрешение за достъп до съответното ниво на класификация на информацията, и при спазване на принципа "необходимост да се знае";
3. Определяне нивото на класификация и категорията информация, която обикновено се съхранява в зоната и до която има пряк физически достъп.

ЗОНА ЗА СИГУРНОСТ КЛАС II :

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.

Изисквания:

1. Ясно определен охраняван периметър, към който всички входове и изходи се контролират;

2. Система за контрол на физическия достъп, позволяваща влизането без придружител само на лица, притежаващи разрешение за достъп до съответното ниво на класификация на информацията, и при спазване на принципа "необходимост да се знае";

3. Осигуряване на придружител за всички останали лица с цел предотвратяване на нерегламентиран достъп до класифицирана информация и неконтролирано влизане в зони, които са обект на мерки за техническа сигурност.

2.1.1.Зона за сигурност (Клас I или клас II) – тип 4	SS3 = 4 точки

Зона на сигурност тип 4 може да бъде от клас I или клас II, в която се съхранява информация с ниво на класификация **"Строго секретно".**

В зависимост от мястото на съхраняване се прилагат следните мерки за сигурност:

1. Сертифициран за това ниво на класификация за сигурност контейнер (каса) при наличието на следните допълнителни мерки за защита:

а) непрекъсната охрана от служители;

б) проверка на контейнера по т. 1 през интервал не по-голям от 2 часа, осъществяван чрез визуално наблюдение от служителите от охраната;

в) наличие на сертифицирана АСПП (Алармена система против проникване) и сили за реагиране, които след постъпване на сигнала за нарушение пристигат на мястото на нерегламентирания достъп за време по-малко от необходимото за отваряне на касата (шкафа, сейфа);

2. Оборудване с АСПП - в открита зона за създаване, обработване, съхраняване или предоставяне на класифицирана информация и осигуряване със сили за реагиране, които след постъпване на сигнала за нарушение пристигат на мястото на нерегламентирания достъп за време по-малко от необходимото за проникване в зоната;

3. Оборудване с АСПП - в подземно помещение и осигуряване със сили за реагиране, които след постъпване на сигнала за нарушение пристигат на мястото на нерегламентирания достъп за време по-малко от необходимото за проникване в помещението.

Изисквания:

Планировка на помещението на регистратурата спрямо общия обем на сградата - регистратурата се разполага във възможно най-защитената част на сградата.

1. Хоризонтална - помещенията, които обслужват зоната да не бъдат преходни по отношение на други помещения извън зоната.

2. Вертикална - препоръчително среден етаж, без първи и последен, като се избягват ъглови помещения и такива, до които има достъп от съседни сгради, както и да не се разполага над котелни помещения.

3. Конструктивна част – монолитна, стоманобетонна, плочо-гредова конструкция, с ограждащи стени от бетон, стоманобетон или тухлена зидария с дебелина 25 сантиметра или от еквивалентен материал по отношение на физическа издържливост.

Изисквания за помещенията:

1. Сградите трябва бъдат от първа, втора или трета степен на пожароустойчивост.

2. Под - негорим, с граница на огнеустойчивост 60 минути.

3. Таванска конструкция – негорима, с граница на огнеустойчивост 60 минути.

4. Стени – негорими, с граница на огнеустойчивост 60 минути.

5. Дограма.

5. 1. Външни прозорци - няма изисквания по отношение на пожароустойчивост, задължително с решетки - вътрешни или външни.

Външни решетки - от профилна стомана, с размери над 15х15мм плътно, или 25х25х3 кух профил, или ф 16 плътно, или ф 18х2 тръба; плътна метална конструкция в затворен контур; метална рамка от профилна стомана с минимална дебелина 4 мм; усилена плътна конструкция в областта на заключващия механизъм при наличие на такъв; светлият размер на отворите да не надвишава 250х250мм. Монолитно закрепени към стените в не по-малко от четири точки.

Вътрешни решетки – от профилна стомана, с размери над 8х8мм плътно, 15х15х1.5 кух профил, ф 10 плътно, ф 12х2 тръба; плътна метална конструкция в затворен контур, закрепени към стените в не по-малко в четири точки. При отваряеми решетки, същите се осигуряват със заключващ механизъм.

5. 2. Врати - метална врата с граница на огнеустойчивост 45 минути.

6. Защита на отвори - всички отвори, от които има възможност за достъп, трябва да имат стоманени решетки, съгласно изискванията за прозорците.

Общо инсталационно оборудване.

1. Отопление - препоръчително централно отопление, без отоплителни уреди с пламъчно горене.

2. Електрооборудване – клас “Н” / Нормална пожарна опасност/. Проходните отвори за кабелите да бъдат огнезащитени.

3. Вентилация и климатизация - без директно преминаване на въздухопроводи през помещенията на регистратурата. Наличните отвори да са защитени с огнепреградни клапи с граница на огнеустойчивост минимум 45 минути.

4. В и К – не се допуска преминаване на инсталационни щрангове през помещенията.

2.1.2. Зона за сигурност (Клас I или клас II) – тип 3	SS3 = 3 точки

Зона за сигурност тип 3 може да бъде от клас I или клас II, в която се съхранява информация с ниво на класификация **"Секретно".**

За информация с ниво на класификация "Секретно" се прилага една от мерките за сигурност, предвидени за съхраняване на информация с ниво на класификация "Строго секретно" или една от следните мерки:

- съхраняване в сертифицирана за това ниво на класификация за сигурност каса (шкаф, сейф) - без допълнителни мерки за защита;

- в открити помещения за създаване, обработване, съхраняване или предоставяне на класифицирана информация - при наличие на следните допълнителни мерки за сигурност:

а) непрекъсната охрана на помещението, в което се намира касата, от служители на звеното за сигурност и охрана при съответната организационна единица или дежурната част;

б) задължителни периодични проверки на помещението от служителите на звеното за сигурност и охрана или дежурната част;

в) снабдяване на откритото помещение с АСПП и осигуряване със сили за реагиране, които след постъпване на сигнала за нарушение пристигат на мястото на нерегламентирания достъп за време по-малко от необходимото за проникване в помещението.

Изисквания:

Планировка на помещението на регистратурата спрямо общия обем на сградата - регистратурата се разполага във възможно най-защитената част на сградата.

1. Хоризонтална - помещенията, които обслужват зоната да не бъдат преходни по отношение на други помещения извън зоната.

2. Вертикална - препоръчително среден етаж, без първи и последен, като се избягват ъглови помещения и такива, до които има достъп от съседни сгради, както и да не се разполага над котелни помещения.

3. Конструктивна част – монолитна, стоманобетонна, плочо-гредова конструкция, с ограждащи стени от бетон, стоманобетон или тухлена зидария с дебелина 25 сантиметра или от еквивалентен материал по отношение на физическа издържливост.

Изисквания за помещенията:

1. Сградите трябва бъдат от първа, втора или трета степен на пожароустойчивост.

2. Под - негорим, с граница на огнеустойчивост 60 минути.

3. Таванска конструкция – негорима, с граница на огнеустойчивост 60 минути.

4. Стени – негорими, с граница на огнеустойчивост 60 минути.

5. Дограма

5. 1. Външни прозорци - няма изисквания по отношение на пожароустойчивост, задължително с решетки - външни или вътрешни.

Външни решетки - от профилна стомана, с размери над 15х15мм плътно, или 25х25х3 кух профил, или ф 16 плътно, или ф 18х2 тръба; плътна метална конструкция в затворен контур; метална рамка от профилна стомана с минимална дебелина 4 мм; усилена плътна конструкция в областта на заключващия механизъм при наличие на такъв; светлият размер на отворите да не надвишава 250х250мм. Монолитно закрепени към стените в не по-малко от четири точки.

Вътрешни решетки – от профилна стомана, с размери над 8х8мм плътно, 15х15х1.5 кух профил, ф 10 плътно, ф 12х2 тръба; плътна метална конструкция в затворен контур, закрепени към стените в не по-малко в четири точки. При отваряеми решетки, същите се осигуряват със заключващ механизъм.

5. 2. Врати - метална врата с граница на огнеустойчивост 45 минути.

6. Защита на отвори - всички отвори, от които има възможност за достъп, трябва да имат стоманени решетки, съгласно изискванията за прозорците.

Общо инсталационно оборудване.

1. Отопление - препоръчително централно отопление, без отоплителни уреди с пламъчно горене.

2. Електрооборудване – клас “Н” / Нормална пожарна опасност/. Проходните отвори за кабелите да бъдат огнезащитени.

3. Вентилация и климатизация - без директно преминаване на въздухопроводи през помещенията на регистратурата. Наличните отвори да са защитени с огнепреградни клапи с граница на огнеустойчивост минимум 45 минути.

4. В и К – не се допуска преминаване на инсталационни шрангове през помещенията.

2.1.3. Зона за сигурност (Клас I или клас II) – тип 2	SS3 = 2 точки

Зона на сигурност тип 2 може да бъде от клас I или клас II, в която се съхранява информация с ниво на класификация **"Поверително".**

За информация с ниво на класификация "Поверително" се прилага обемът мерки за сигурност, предвидени за защита на информация с ниво на класификация "Строго секретно" и "Секретно", с изключение на допълнителните защитни мерки.

Изисквания:

Планировка на помещението на регистратурата спрямо общия обем на сградата – регистратурата се разполага се във възможно най-защитената част на сградата.

1. Хоризонтална - помещенията, които обслужват зоната да не бъдат преходни по отношение на други помещения извън зоната.

2. Вертикална - препоръчително среден етаж, без първи и последен, с изглед към вътрешен двор или части на сградата, като се избягват ъглови помещения и такива, до които има достъп от съседни сгради, както и да не се разполага над котелни помещения.

3. Конструктивна част - препоръчително е външните стени да бъдат стоманобетонни, тухлени с дебелина 25 сантиметра или от еквивалентен материал по отношение на физическа издържливост.

Изисквания за помещенията:

1. Сградите трябва да бъдат от първа, втора или трета степен на пожароустойчивост.

2. Под, стени и таван – в помещенията за съхранение на информация с ниво на класификация “Поверително” облицовките да са негорими.

3. Дограма:

3.1. Външни прозорци - няма изисквания по отношение на пожароустойчивост; задължително с метални решетки със стъпка на вертикалните елементи не повече от 150 мм /Наредба № 7 за системите за физическа защита на строежите /.

3.2. Врати - няма изисквания по отношение на пожароустойчивост; задължително с метална решетка със стъпка на вертикалните елементи не повече от 150 мм или метална врата.

4. Защита на отвори - всички отвори, от които има възможност за достъп, трябва да имат решетки, съгласно изискванията за прозорците.

Общо инсталационно оборудване.

1. Отопление - без отоплителни уреди на твърдо гориво и уреди с открито пламъчно горене.

2. Електро оборудване - без ограничения.

3. Вентилация и климатизация - без директно преминаване на въздухопроводи през помещенията. Наличните отвори да са защитени с огнепреградни клапи с граница на устойчивост 15 минути.

4. В и К - без ограничения.

2.1.4. Зона за сигурност – тип 1	SS3 = 1 точка

Зона на сигурност тип 1 може да бъде от клас I или клас II, както и административната зона съгласно чл. 14, ал. 1, т. 1 от Наредбата. В зона на сигурност тип 1 се съхранява информация с ниво на класификация **"За служебно ползване"**.

Изисквания:

Планировка на помещението на регистратурата спрямо общия обем на сградата – регистратурата се разполага се във възможно най-защитената част на сградата.

1. Хоризонтална - помещенията, които обслужват зоната да не бъдат преходни по отношение на други помещения извън зоната.

2. Вертикална - препоръчително среден етаж, без първи и последен, с изглед към вътрешен двор или части на сградата, като се избягват ъглови помещения и такива, до които има достъп от съседни сгради, както и да не се разполага над котелни помещения.

3. Конструктивна част - препоръчително е външните стени да бъдат стоманобетонни, тухлени с дебелина 25 сантиметра или от еквивалентен материал по отношение на физическа издържливост.

Изисквания за помещенията:

1. Сградите трябва бъдат от първа, втора или трета степен на пожароустойчивост;

2. Под, стени и таван –няма изисквания.

3. Дограма:

3.1. Външни прозорци - няма изисквания по отношение пожароустойчивост; задължително с метални решетки със стъпка на вертикалните елементи не повече от 150 мм /Наредба № 7 за системите за физическа защита на строежите /.

3. 2. Врати - няма изисквания по отношение пожароустойчивост; задължително с метална решетка със стъпка на вертикалните елементи не повече от 150 мм или метална врата.

4. Защита на отвори - всички отвори, от които има възможност за достъп, трябва да имат решетки, съгласно изискванията за прозорците.

Общо инсталационно оборудване.

1. Отопление - без отоплителни уреди на твърдо гориво и уреди с открито пламъчно горене.

2. Електро оборудване - без ограничения.

3. Вентилация и климатизация - без директно преминаване на въздухопроводи през помещенията. Наличните отвори да са защитени с огнепреградни клапи с граница на устойчивост 15 минути.

4. В и К - без ограничения.

2.2. ЗАКЛЮЧВАЩИ СИСТЕМИ (заключващи устройства, ключалки), ОПРЕДЕЛЕНИ ЗА ЗАКЛЮЧВАНЕ НА ЗОНИТЕ НА СИГУРНОСТ

2.2.1. Заключваща система – тип 4	SS4 = 4 точки

Заключваща система тип 4 осигурява висока степен на устойчивост срещу професионално проникване, при което могат да се използват особено развити технологии и инструменти, които са недостъпни в търговската мрежа.

Изисквания :

1. Секретен патрон, защитен срещу разпробиване и чупене и допълнителна секретна брава
2. Заключващата система е клас В, съгласно изискванията на стандарт EN 1300

2.2.2. Заключваща система – тип 3	SS4 = 3 точки

Заключваща система тип 3 осигурява висока степен на устойчивост срещу професионално проникване, при което може да се използват технологии и инструменти, които са пазарно достъпни за професионалния ключар.

Изисквания:

1. Секретен патрон, защитен срещу разпробиване и чупене.
2. Заключващата система е клас В, съгласно изискванията на стандарт EN 1300.

2.2.3. Заключваща система – тип 2	SS4 = 2 точки

Заключваща система тип 2 осигурява устойчивост срещу разбивач, който притежава ограничен обхват на инструменти.

Изисквания:

1. Секретен патрон, защитен срещу разпробиване и чупене.
2. Заключващата система е клас А, съгласно изискванията на стандарт EN 1300.

2.2.4. Заключваща система – тип 1	SS4 = 1 точка

Ключалка тип 1 осигурява устойчивост срещу упражняване на физическа сила и скрито проникване.

Изисквания:

Секретен патрон клас А, съгласно изискванията на стандарт EN 1300

3. ГРАНИЦА НА ОБЕКТ

Обект – сграда или друга конструкция или по друг начин маркиран район, в който се намират зоните на сигурност.

Граница на обекта – повърхността (“обвивката”) на сградата, огради или други подобни ограничители.

Решаваща за определяне вида на обекта е тази част от границата му, която има най-ниска устойчивост.

Когато границата на обекта или сградата по цялото си протежение е една и съща като границата на зоната на сигурност, оценката S3/C3 е 0.

Специален случай е когато границата на обекта се ограничава с границата на периметъра (ограда и др.) В този случай тя се оценява като граница на обекта. Ако в

периметъра има контрол на изхода, е възможно неговата оценка да се вземе за определяне нивото на сигурността на обекта.

Периметърът представлява обозначената външна граница на зоните за сигурност, която изисква защита.

По периметъра се изграждат физически бариери, които могат да бъдат оборудвани и с технически средства, възпрепятстващи нерегламентирания достъп. Степента на прилаганите средства за физическа и техническа охрана на защитавания обект зависи от нивото и обема на класифицираната информация, която се съхранява в тази зона за сигурност.

Защитното осветление в зоните за сигурност трябва да осигурява възможност за ефективно наблюдение от страна на звеното за сигурност и охрана и техническите средства за защита.

За повишаване нивото на защита на периметъра в зоните за сигурност се използват алармени системи против проникване (АСПП).

Алармените системи против проникване сигнализират при опит за нерегламентиран достъп или осъществен такъв достъп и осигуряват необходимото време за реакция на силите за реагиране. Алармените системи против проникване се използват съгласно плана за физическа сигурност на обекта.

3.1. Обект – тип 4	S3 = 5 точки

Обект тип 4 има масивна конструкция, която осигурява висока степен на устойчивост срещу насилствено проникване.

Изисквания:

Стени, подове и тавани трябва да се направени от конструкции с повишена устойчивост. Обект тип 4 има минимален брой врати, прозорци и други отвори. Ако има такива, тези врати, прозорци и отвори трябва да бъдат осигурени с механично възпиращи средства, които осигуряват същата степен на устойчивост срещу разбиване, както другите гранични части на обекта от тип 4.

3.2. Обект тип 3	S3 = 3 точки

Обект тип 3 осигурява известна степен на устойчивост срещу насилствено проникване.

Изисквания:

Стените , подовете и таваните трябва да са изградени от устойчиви конструкции – тухли или блокове, може да се използва модерна строителна технология - готови сглобяеми елементи, стоманени и стъклопакети и др. Вратите, прозорците и други отвори трябва да бъдат защитени с механични възпиращи средства, които осигуряват същата степен на устойчивост срещу разбиване като другите гранични части на обекта от тип 3. Това условие не е валидно, когато долната част на прозореца или отвора отговаря на следните изисквания:

Намира се най-малко на 5,5 метра над земята.

В него не може да се проникне от покрива, чрез използването на гръмоотводи, водосточни тръби, парапети или други елементи на конструкцията, земни неравности, дървета или други сгради.

Отговаря на изискванията за сигурност на сградата.

3.3. Обект тип 2	S3 = 2 точки

Обект тип 2 осигурява степен на устойчивост срещу насилствено проникване. Има лека строителна конструкция или притежава устойчива мобилна конструкционна клетка.

Изисквания:

Вратите, прозорците и другите отвори трябва да бъдат защитени с механични възпиращи средства, които осигуряват същата степен на устойчивост срещу разбиване като другите гранични части на обекта от тип 2. Това условие не е валидно, когато долната част на прозореца или отвора отговаря на следните изисквания:

Намира се най-малко на 5,5 метра над земята.

В него не може да се проникне от покрива, чрез използването на гръмоотводи, водосточни тръби, парапети или други елементи на конструкцията, земни неравности, дървета или други сгради.

Отговаря на изискванията за сигурност на сградата.

3.4. Обект – тип 1	S3 = 1 точка

Обект тип 1 е изграден от лека сглобяема конструкция, използва се за защита на хората, материалите и оборудването, които се намират в него, от климатичните условия.

4. КОНТРОЛ НА ФИЗИЧЕСКИЯ ДОСТЪП В ЗОНАТА ЗА СИГУРНОСТ ИЛИ ОБЕКТА, ПРОИЗВОЛЕН КОНТРОЛ И РЕЖИМ НА ВЛИЗАНЕТО.

4.1. КОНТРОЛ НА ФИЗИЧЕСКИЯ ДОСТЪП В ЗОНАТА ЗА СИГУРНОСТ ИЛИ ОБЕКТА.

Контролът на физическия достъп се осъществява по отношение на всички сгради, помещения и съоръжения, в които се създава, обработва, съхранява и предоставя класифицирана информация. Ръководителите на организационните единици, с помощта на служителите по сигурността, определят необходимата система от мерки за физическа сигурност, въз основа на способите по чл.3, ал. 1 от Наредба за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване (Наредбата).

Контролът се осъществява чрез:

1. Електронни средства, работещи самостоятелно или съвместно със служител от охраната;

2. Електромеханични средства, работещи съвместно със служител от звеното за сигурност и охрана, или

3. Служители от звеното за сигурност и охрана.

4.1.1. Контрол на физическия достъп – тип 4	SS6 = 4 точки

Контрол на физическия достъп тип 4 се отнася до автоматичните електронни системи за контрол на входа, които дават такава степен на сигурност, изискваща само минимум наблюдение от страна на физическата охрана на обекта, в който се съхранява информация с ниво на класификация "Строго секретно".

Изисквания:

1. За контрол на физическия достъп тип 4 се използва автоматична електронна система.
2. Контролът на физическия достъп се осъществява на всички входове/изходи на обекти или на зоната за сигурност.
3. В системата за контрол на физическия достъп се използва уникалният персонален идентификационен номер (ПИН) или биометрична идентификационна система.
4. Системата за контрол на физическия достъп не трябва да позволява последователното преминаване в една и съща посока.
5. Излъчването на предупредителни сигнали от системата за контрол на входа/изхода трябва да бъде свързано с физическата охрана.

Изисквания съгласно БДС и стандартите на Европейския съюз:

БДС EN 50 133-1 относно автоматичната електронна система за контрол на входа/изхода за ниво на класификация СТРОГО СЕКРЕТНО.

4.1.2. Контрол на физическия достъп – тип 3	SS6 = 3 точки

Контролът на физическия достъп тип 3 се отнася до автоматичните електронни системи за контрол на входа/изхода за обекти, в които се съхранява информация с ниво на класификация "Секретно".

Изисквания:

1. За контрол на физическия достъп тип 3 се използва автоматична електронна система за контрол на входа/изхода.
2. Контрол на физическия достъп се осъществява на всички входове/изходи на обекти или на зоната за сигурност.
3. В системата за контрол на входа/изхода се използва комбинация от уникалния персонален идентификационен номер (ПИН) или биометрична идентификационна система.
4. Системата за контрол на входа/изхода трябва да се наблюдава от охраната.

4.1.3. Контрол на физическия достъп – тип 2	SS6 = 2 точки

Контрол на физическия достъп тип 2 представлява контрол, извършван от охрана в обекти, в които се съхранява информация с ниво на класификация "Поверително".

Изисквания:

1. Контрол на физическия достъп се осъществява на всички входове и изходи на обекта или на защитената зона.

2. За контрол на физическия достъп тип 2 се използва охрана, която проверява идентификационните входни карти или временни разрешения. Може да се използва и автоматична електронна система за контрол на входа.

Изисквания съгласно стандартите на БДС EN 50 133-1 относно автоматичната електронна система за контрол на входа, оценена като ниво СЕКРЕТНО.

Автоматичната електронна система за контрол на входа/изхода отговаря на изискванията на клас на разпознаване 2 и клас на достъп B за достъп (термините се отнасят до категории според стандарт БДС EN 50 133-1).

4.1.4. Контрол на физическия достъп – тип 1	SS6 = 1 точка

Контрол на физическия достъп тип 1 представлява контрол чрез механична преграда. Такъв контрол тип 1 може да се използва само при влизане в защитена зона на сигурност в обект,в който се съхранява информация с гриф за сигурност "За служебно ползване".

Изисквания:

1. Контрол на физическия достъп се осъществява на всички входове/изходи на обектите и зоните на сигурност.

2. Контрол на физическия достъп се осъществява чрез заключваща се врата, която позволява влизането с помощта на механична или електрическа ключалка или с дадени ключове само на упълномощени за това лица.

4.2. СЛУЧАЙНО ВЛИЗАНЕ И КОНТРОЛ

4.2.1. Избирателен /случаен/ контрол	SS12 = 1 точка

Във всички организационни единици се предприема избирателна проверка на багаж и лични вещи при влизане и излизане с цел предотвратяване на внасянето и изнасянето на класифицирани материали извън установения ред.

Проверката може да бъде заложена като задължително условие за влизане в дадена сграда или обект. В такъв случай се поставя известяващ проверката надпис.

Проверката се извършва чрез технически средства или чрез визуален оглед.

4.3. РЕЖИМ НА ПОСЕЩЕНИЯ В ОБЕКТА

Изисквания на НАТО:

Националността на посетителя, нивото на достъп в неговото разрешение, ограничението за достъп до класифицирана информация и други изисквания, произтичащи от риска за нерегламентиран достъп, са решаващи за определяне на това дали това лице ще се движи с или без охрана в обекта.

4.3.1 Посещения с охрана	SS7 = 3 точки

Изисквания:

1. Режимът на посещения се определя със заповед от ръководителя на организационната единица с помощта на служителя по сигурността на информацията.
2. Посетителите трябва да бъдат придружавани през цялото време на престоя им в обекта. Ако посетителят трябва да посети повече места или служители, той може да бъде предаден на подходящия човек, заедно с необходимите указания.
3. Трябва да се поддържа регистър с идентификационните данни на посетителите и сведения за мястото и часа на техните посещения.

4.3.2. Посещения без охрана	SS7 =1 точка

Изисквания:

Този режим за посещения може да се използва само в административната зона по чл.14, ал.1, т.2 от НАРЕДБАТА за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

1. Посетителите, влизащи без охрана, трябва да носят обозначение. Този начин на идентификация е ефективен само ако всички останали служители също носят обозначения.
2. Трябва да се поддържа регистър с идентификационните данни на посетителите и сведения за мястото и часа на техните посещения.

4.3.3. Посещения без контрол	SS7 = 0 точки

5. ОХРАНА И СИСТЕМИ ЗА СИГУРНОСТ /СОТ/, КОНТРОЛ НА ДОСТЪПА В ЗОНИТЕ ЗА СИГУРНОСТ И ВИДЕОНАБЛЮДЕНИЕ

5.1. ОХРАНА

Охраната се определя като средство за противопоставяне на опити за нерегламентиран достъп до класифицирана информация в зоните за сигурност. Служителите от звеното за сигурност и охрана прилагат системата от мерки за физическа сигурност на класифицираната информация.

Дейността на служителите от звеното за сигурност и охрана се регламентира с инструкция, утвърдена от ръководителя на организационната единица. За служители в звеното за сигурност и охрана (в звеното за сигурност) се назначават лица, получили разрешение за достъп до ниво на класификация "Поверително" или по-високо, ако спецификата на работата им го налага. Задълженията, дежурствата и честотата на обхода на служителите от звеното за сигурност и охрана се определят в зависимост от анализа на риска, наличието и вида на конкретните мерки за физическа сигурност.

В зависимост от плана за физическа сигурност в организационната единица могат да се създават сили за реагиране. Силите за реагиране се състоят най-малко от двама служители, които могат да бъдат служители от звената за сигурност и охрана или други служители от организационната единица. Силите за реагиране забавят и

ограничават нарушителя при навлизане в периметъра на зоните за сигурност до предаването му на компетентните органи, без това да отслабва защитата в останалите места.

В организационните единици, където има изградени функциониращи технически средства за физическа сигурност, организирани в система, за нуждите на звеното за сигурност и охрана се изгражда контролен център.

Контролният център е специално оборудвано помещение, предназначено за приемане, визуализиране и архивиране на информацията, получена от прилагането на техническите мерки за физическа сигурност, организирани в система, и служи за сигнализиране, контрол и ръководство на силите за реагиране.

За повишаване на физическата защита и подпомагане на звеното за сигурност и охрана в обектите се изгражда система за видеонаблюдение, която може да бъде самостоятелна или технически свързана с контрола на достъпа, с алармената система против проникване и с други конкретни мерки за физическа сигурност.

Системата за видеонаблюдение изисква изграждането на контролен център и представлява елемент от общата защитна система.

Изисквания на НАТО:

В случай, че охраната се използва за гарантиране на сигурността и целостта на класифицирана информация на НАТО, лицата, които са охранители, трябва да бъдат проучени по съответния начин и обучени за изпълнение на специфичните задължения по охрана на обекта.

Групата, която извърша охрана на обекта, трябва да може да окаже намеса на мястото на нерегламентиран достъп посредством двама души, така че да не се нарушава броят на присъстващата охрана на другите места на обекта.Трябва да се провери реакцията на охраната на сигнал за тревога. Целта на тези проверки е да се установи дали скоростта на намеса е адекватна с цел предотвратяване на нерегламентиран достъп до класифицирана информация на НАТО.

5.1.1 Охрана – тип 5	SS8 = 5 точки

Охрана тип 5 се осъществява чрез вътрешни неправилни (нерегулирани, произволни) обходи в обекта.

Изисквания:

1. Физическата охрана на обекта се извършва съгласно предписанията на чл.19 и чл. 20 от Наредбата за системата от мерки, способи и средства за физическата сигурност на ксласифиицраната информация и за условията и реда за тяхното използване.

2. Охраната извършва обходите си в обекта по произволно избрани маршрути и на произволни интервали, непревишващи два часа. При извършване на обходите охраната трябва да има точно поставени конкретни задачи.

3. При извършване на обходите, поне едно лице трябва да остане на постоянния пост.

5.1.2 Охрана – тип 4	SS8 = 4 точки

Охрана тип 4 се осъществява чрез вътрешни редовни (регулирани) обходи в обекта

Изисквания:

1. Физическата охрана на обекта се извършва съгласно предписанията на чл. 19 и чл.20 от Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

2. Охраната извършва редовни обходи в обекта на интервали, непревишващи шест часа. През нощта и в неработно време честотата на обходите се увеличава. При извършване на обходите охраната трябва да има точно поставени конкретни задачи.

3. При извършване на обходите, поне едно лице трябва да остане на постоянния пост.

5.1.3. Охрана – тип 3	SS8/CC8 = 3 точки

Охрана тип 3 се осъществява чрез обходи във външния район (извън обекта)

Изисквания:

Физическата охрана на обекта се осъществява в съответствие с чл. 19 и чл. 20 Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

Охраната извършва обходи извън обекта, без да има достъп до него, а само контролира неговата сигурност в обхвата на периметъра. Интервалите на обходите зависят от вътрешното състояние и от степента на риска.

При извършване на обходите, поне едно лице трябва да остане на постоянния пост.

5.1.4. Охрана – тип 2	SS8 = 2 точки

Охрана тип 2 се извършва от местен охранител.

Изисквания:

Физическата охрана на обекта се осъществява съгласно разпоредбите на чл. 19 и чл. 20 от Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

Не се изискват обходи. За контрол на обекта и осигуряване на района и проверка на съмнителни инциденти се използва персонал, който, ако е необходимо търси помощ (определени и обучени служители на обекта, или служители на упълномощена охранителна служба).

5.1.5. Охрана – тип 1	SS8 = 1 точка

Охрана тип 1 се извърша чрез външни проверки по периметъра, като се поддържа връзка с централизираната охрана. Охрана тип 1 може да се използва за защита на класифицирана информация с ниво ПОВЕРИТЕЛНО и по-ниско.

Изисквания:

Физическата охрана на обекта се извършва съгласно разпоредбите на чл. 19 и чл. 20 от Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

Охраната трябва да контролира външния район, специално извън работно време.Контролът се извършва по периметъра. Охраната обикновено няма разрешение да извършва проверки вътре в обекта и в случай на необходимост осъществява контакти с лицето, което е упълномощено да влезе в обекта или в защитената зона .

5.2. АЛАРМЕНИ СИСТЕМИ ПРОТИВ ПРОНИКВАНЕ /АСПП/.

АСПП се използват съгласно чл. 17 от Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване и в съответствие с изискванията на БДС EN 50131, БДС EN 50132 и БДС EN 50133 и серията БДС IEC 839. АСПП се изгражда като напълно самостоятелна система.

Ако АСПП не е инсталирана, тогава:

а) когато навсякъде в зоната на сигурност се осигурява постоянно присъствие на там работещите служители - SS9 е равно на 4.

б) когато физическата охрана на обекта, която е упълномощена да извършва независимо влизане в зоната на сигурност, се извършва от охрана тип 5, SS9 тогава е равна на 0.

5.2.1. Оценка на нивото на техническите средства на АСПП.

5.2.1.1. Ниво на техническите средства за АСПП – тип 4	SS91 = 4 точки

АСПП тип 4 се изгражда в обекти, в които се съхранява информация с ниво на класификация "Строго секретно", съответства на категория 4 от БДС EN 50131.

Изисквания:

1. Двустепенна вътрешна АСПП - контрол на вратите с МКД (магнитно-контактен детектор), прозорците с МКД и акустични детектори и обема на помещенията с необходимия брой ПИР - пасивни инфрачервени детектори.
2. Охрана на металните шкафове и каси със сеизмични детектори.
3. При наличието на архив се монтират микровълнови детектори.
4. Монтират се вибрационни детектори за охрана на стените.
5. На входните врати задължително се монтират сеизмични детектори против разбиване.
6. Монтират се вибрационни детектори на пода и тавана.
7. При необходимост се монтират паник бутони за служителите.
8. Устройството за управление и индикация има над 1000 събития енергонезависима памет и се дели на не по-малко от 4 групи.
9. Предаването на сигналите до мониторинг центъра се осъществява по радиоканал.
10. Предаването на сигналите се дублира и по проводна линия.
11. Възможност за работа на батерии над 24 часа.
12. Не се допуска свързване на повече от един охранителен детектор в зона.

5.2.1.2. Ниво на техническите средства за АСПП – тип 3 SS91 = 3 точки

АСПП тип 3 се изгражда в обекти, в които се съхранява информация с ниво на класификация "Секретно", съответства на категория 3 от БДС EN 50131

Изисквания:

1. Двустепенна вътрешна АСПП - контрол на вратите с МКД, прозорците с МКД и акустични детектори и обема на помещенията с необходимия брой ПИР.
2. Охрана на металните шкафове и каси със сеизмични детектори.
3. При наличието на архив се монтират микровълнови детектори.
4. При необходимост се монтират вибрационни детектори за охрана на стените.
5. На входните врати задължително се монтират вибрационни детектори против разбиване.
6. При необходимост се монтират вибрационни детектори на пода и тавана и паник бутони за служителите.
7. Устройството за управление и индикация има над 700 събития енергонезависима памет и се дели на не по-малко от 4 групи.
8. Предаването на сигналите до мониторинг центъра се осъществява по радиоканал.
9. Предаването на сигналите се дублира и по проводна линия.
10. Възможност за работа на батерии над 24 часа.
11. Не се допуска свързване на повече от един охранителен детектор в зона.

5.2.1.3. Ниво на техническите средства за АСПП – тип 2 SS91 = 2 точки

АСПП тип 2 се изгражда в обекти, в които се съхранява информация с ниво на класификация "Поверително", съответства на категория 2 от БДС EN 50131.

Изисквания:

1. Двустепенна вътрешна АСПП - контрол на вратите с МКД, прозорците с МКД и акустични детектори и обема на помещенията с необходимия брой ПИР.
2. При необходимост на металните шкафове и каси се инсталират сеизмични детектори.
3. При наличието на архив се монтират микровълнови детектори.
4. При необходимост се монтират вибрационни детектори за охрана на стените.
5. Устройството за управление и индикация има над 500 събития енергонезависима памет и се дели на не по-малко от 2 групи.
6. Предаването на сигналите до мониторинг центъра се осъществява по радиоканал.
7. Предаването на сигналите се дублира и по проводна линия.
8. Възможност за работа на батерии над 24 часа.
9. Не се допуска свързване на повече от два еднотипни охранителни детектора в зона.

5.2.1.4. Ниво на техническите средства за АСПП – тип 1 SS91 = 1 точка

АСПП тип 1 се изгражда в обекти, в които се съхранява информация с ниво на класификация "За служебно ползване", съответства на категория 2 от БДС EN 50131

Изисквания:

1. Двустепенна вътрешна АСПП - контрол на вратите с МКД, прозорците с МКД и акустични детектори и обема на помещенията с необходимия брой ПИР.
2. При необходимост - допълнителна охрана на металните шкафове и каси със сеизмични детектори.
3. Устройството за управление и индикация има над 250 събития енергонезависима памет.
4. Предаването на сигналите до мониторинг центъра се осъществява по радиоканал или по проводна линия..
5. Възможност за работа на батерии над 24 часа.
6. Не се допуска свързване на повече от четири еднотипни охранителни детектора в зона.

5.2.2. Инсталиране на техническите средства на АСПП.

5.2.2.1 Инсталиране на техническите средства на АСПП – тип 4 SS92 = 4 т.

Изисквания:

1. Трябва да се осигури защитата на цялата зона на сигурност, пълно повърхностно покритие на зоната, система за извънрено положение (алармена система), на касите трябва да се инсталират защитни средства (напр. детектори за трезори).
2. Инсталирането на детектор за каси не се изисква в зоните на сигурност, определени като помещения за заседания и в помещенията, където не се съхранява класифицирана информация.
3. Контролирането на АСПП в зоната на сигурност трябва да бъде независимо от контрола на АСПП в другите зони или помещения.
4. Изходните сигнали от средствата на АСПП трябва да бъдат свързани с центъра за приемане на алармени сигнали за обекта.

5.2.2.2. Инсталиране на техническите средства на АСПП – тип 3 SS92 = 3 точки

Изисквания:

1. Трябва да се осъществи пространствена защита на цялата зона на сигурност, пълно повърхностно покритие на зоната на сигурност и система за извънредни случаи.
2. Контролирането на АСПП в зоната на сигурност трябва да бъде независимо от контрола на АСПП в другите зони или помещения.
3. Изходните сигнали от средствата на АСПП трябва да бъдат свързани с центъра за приемане на алармени сигнали на обекта.

5.2.2.3. Инсталиране на технически средства на АСПП – тип 2 SS92 = 2 точки

Изисквания:

Трябва да се осъществи пространствена и повърхностна защита в зоните, където се съхранява класифицирана информация. Прозорците и други отвори в границите на зоната на сигурност в случай на инсталиране на АСПП от този тип, трябва да бъдат защитени чрез елементи за повърхностна защита, ако долният им край не отговаря на следните условия :

1. Има поне 5,5 метра разстояние от земята.
2. В отвора или прозореца не може да се проникне от покрива, чрез гръмоотводи, водосточни тръби, парапети ли други конструкционни елементи, земни неравности, дървета или други сгради.
3. Отговарят на изискванията за сигурност на сградата.
4. Изходните сигнали от средствата на АСПП трябва да бъдат свързани с центъра за приемане на алармени сигнали на обекта.

5.2.2.4. Инсталиране на технически средства на АСПП – тип 1 SS92 = 1точка

Изисквания:

1. Трябва да се осъществи пространствена защита на зоната на сигурност, където се съхранява класифицирана информация.
2. Изходните сигнали от средствата на АСПП трябва да бъдат свързани с центъра за приемане на алармени сигнали на обекта.

5.3. СИСТЕМА ЗА ВИДЕОНАБЛЮДЕНИЕ

5.3.1. Система за видеонаблюдение	без точки

Техническите средства трябва да отговарят на стандартите БДС EN 50 132-2-1, БДС EN 50 132-7. Системата за видеонаблюдение се проектира и изгражда като напълно самостоятелна система като не позволява по какъвто и да е начин добиване на класифицирана информация.

Изисквания:

1. Система за видеонаблюдение на входните врати на зоната и регистратурата се изгражда за ниво "Строго секретно" и "Секретно".
2. Центъра за управление на системата за видеонаблюдение да позволява непрекъснат запис или такъв с включена детекция на движение 24 часа в денонощието.
3. При изграждане на система за цифров запис централното управление на системата да поддържа разделителна способност не по-малко от 640 x 480, с не по-малко от 5 кадъра в секунда за всеки вход, паралелен запис на два носителя и дисково пространство позволяващо запис на видеоинформация за не по-малко от 30 денонощия при включена детекция на движение.
4. При изграждане на система за аналогов запис на видеоинформация да се предвижда дуплексен мултиплексор за непрекъснат запис с достатъчен брой входове и бавнозаписващ видеомагнитофон с възможност за запис над 72 часа.
5. Камерите от системата да имат следните характеристики: над 460 TVL за черно-бели със светлочувствителност върху обекта не по-малка от 0.5 Lux върху обекта и над 400 TVL за цветни със светлочувствителност върху обекта не по ниска от 1.0 Lux

върху обекта комплектовани с подходящи обективи и аксесоари. Допуска се монтиране на инфрачервени прожектори.

6. При съхранение на информация с ниво на класификация "Строго секретно" да се добави наблюдение на външния периметър на зоните за сигурност.

5.2.4. Оценка на системата за извънредно положение	без точки

Изисквания за одобрение на система за извънредни случаи за ниво СТРОГО СЕКРЕТНО:

1. Системата за извънредни случаи отговаря на стандарт БДС EN 50 134-2-1, "Система за викане на помощ".

В случай, че в зоната на сигурност е осигурено постоянно присъствие, поне на двама човека, работещи там и при условие, че е оборудвана с АСПП, каса тип 4 и заключващо устройство тип 4, тогава SS9 е равно на 4.

6. ЗАЩИТА НА ПЕРИМЕТЪРА

6.1.ФИЗИЧЕСКИ БАРИЕРИ (ОГРАДИ)

Физическите бариери (огради) се изискват по целия периметър на границата на обекта. Ефективността на физическите бариери зависи от степента на нивото на защита на точките на достъп. Конструкцията на точките на достъп (входни врати) трябва да бъде от същото ниво на сигурност като конструкцията на физическата бариера (оградата). По всички точки на достъп трябва да бъде осигурен един и същ стандарт на контрол на влизането.

6.1.1 Физическа бариера – тип 4	SS10 = 4 точки

Физическа бариера тип 4 се определя за места, изискващи най-силна защита.

Изисквания:

Бариерата (оградата) по периметъра трябва да осигурява възможност за наблюдение (мониторинг) на съседните терени без проблем. Ако е възможно, тя трябва да отстои от обекта на 25 метра. Минималната височина на вертикалната част на бариерата е 2,15 метра. Тя трябва да бъде проектирана и направена така, че да осъществява колкото е възможно по-голямо препятствие срещу проникване чрез взлом. Горната част на бариерата трябва да осигурява защита от преминаване чрез катерене (от двете страни трябва да има продълговати пръти, стърчащи навън и навътре под ъгъл 40 градуса с минимална дължина 40 см, по които е закачена бодлива тел) . Физическата бариера тип 4 трябва да бъде оборудвана със система за наблюдение на периметъра.

6.1.2. Физическа бариера – тип 3	SS10 = 3 точки

Физическа бариера тип 3 се определя за места, изискващи средна степен на защита.

Изисквания:

Бариерата (оградата) по периметъра трябва да да осигурява наблюдение (мониторинг) на съседните терени без проблем. Ако е възможно, тя трябва да отстои от обекта на 25 метра. Минималната височина на вертикалната част на бариерата е 2,15 метра. Тя трябва да бъде проектирана и направена така, че да осъществява колкото е възможно по-голямо препятствие срещу проникване чрез взлом. Горната част на бариерата трябва да осигурява защита от преминаване чрез катерене.

6.1.3. Физическа бариера – тип 2	SS10 = 2 точки

На физическа бариера тип 2 отговаря защитна ограда.

Изисквания:

Защитната ограда трябва да бъде препятствие срещу опита да бъде премината чрез катерене или срещу проникване чрез взлом. Минималната височина на вертикалната част на бариерата е 2,15 метра.

6.1.4. Физическа бариера – тип 1	SS10 = 1 точка

Физическа бариера тип 1 отговаря на ограда без специални изисквания за сигурност.

Изисквания:

Целта на тази ограда е само да маркира границата и да осигури минимално ниво на обезкуражаване или устойчивост. Ограда тип 1 може да бъде направена от всеки вид материал, както и с жив плет.

6.2. КОНТРОЛ НА ВХОДА НА ФИЗИЧЕСКАТА БАРИЕРА

6.2.1. Контрол се осъществява на всички входове по периметъра	SS11 = 1 т.

6.2.2. Контрол не се осъществява на всички входове по периметъра	SS11 = 0 т.

6.3. ДЕТЕКТОРНА СИСТЕМА ЗА НАБЛЮДЕНИЕ НА ПЕРИМЕТЪРА

Системите за наблюдение на периметъра осигуряват контрол на границите на зоната на сигурност.

6.3.1. Детекторна система за наблюдение на периметъра (ДСНП)	SS13 = 2 точки

Изисквания:

Системата за наблюдение на периметъра трябва да бъде използвана за контрол на периметъра, което увеличава нивото на сигурност на границата на обекта, осигурено от оградата. ДСНП може да бъде инсталирана като скрита (обикновено от естетична

гледна точка) или открита като отблъскващо средство. Целесъобразно е ДСНП да бъдат комплектовани с други контролни системи, напр. системи за видеонаблюдение.

6.3.2. Защитните светлини като допълнение към защитата на периметъра SS14 = 2 точки

Изисквания:

Защитните светлини се инсталират като част от защитата на периметъра. Изискванията за инсталиране произтичат от изискванията за системите за видеонаблюдение.

6.3.3. Система за видеонаблюдение като допълнение на сигурността на периметъра. SS15 = 2 точки

Изисквания:

Системата за видеонаблюдение се инсталира като част от защитата на периметъра.

7. ПОЖАРОИЗВЕСТИТЕЛНИ И ПОЖАРОГАСИТЕЛНИ СИСТЕМИ

Помещенията според нивата на класификация за сигурност на информацията и техния гриф се оборудват със системи за пожароизвестяване и пожарогасене, както следва:

7.1. "За служебно ползване"
Помещенията е препоръчително да се осигурят с пожароизвестителна система.

7.2. "Поверително"
Помещенията задължително да бъдат защитени с пожароизвестителна система.

7.3. "Секретно"
7.3.1. Помещенията, разположени в зоната за сигурност се защитават с пожароизвестителна система.
7.3.2. Всички съседни помещения, коридори и стълбища, пространства от сградата, непосредствено над и под помещението се защитават от пожароизвестителна система.

7.4. "Строго секретно"
7.4.1. Помещенията се защитават с пожароизвестителна система.
7.4.2. Всички съседни помещения, коридори и стълбища, пространства от сградата, непосредствено над и под помещението се защитават от пожароизвестителна система.
7.4.3. С газови пожарогасителни системи за обемно гасене се съоръжават помещения с площ по-голяма от 50 кв. м, в които:
- информацията се обработва по електронен път;
- информацията се съхранява в каси, сейфове и шкафове, нямащи изискващите се от тази Методика граница на огнеустойчивост.

7.4.4. При наличие на сървър, обслужващ 5 и повече работни места – същият се защитава локално с газово пожарогасене, независимо от площта на помещението.

Общи изисквания към системите:

1. Компонентите за изграждане на пожароизвестителните системи да са в съответствие с частите от БДС EN – 54, като проектирането се извършва при спазване препоръките, записани pr EN – 54, част 14.

2. Газовите пожарогасителни системи се проектират в съответствие с частите на ISO – 14520. Допускат се пожарогасителни системи с въглероден диоксид /CO2/ при спазване изискванията на ISO – 6839. Управлението на пожарогасителните системи да е в съответствие с pr EN 12094.

Изисквания:

1. В помещенията за съхранение на информация, без тези за служебно ползване, облицовките на подове, стени и тавани, да са негорими.

2. Границата на огнеустойчивост за всички конструктивни елементи и продуктите, регламентирани в Методиката, се определят по БДС 6316 – 81 или EN 1363.

3. Групите на горимост на използваните материали се определят по действащите в Р България БДС и БДС EN.

4. Секретна и строго секретна информация се допуска да не се съхранява в огнеустойчиви сейфове и каси, когато помещенията са защитени със система за обемно пожарогасене.

8. ДЕТЕКТОРИ НА СУБСТАНЦИИ ИЛИ СРЕДСТВА, ИЗПОЛЗВАНИ ГЛАВНО ЗА ОТКРИВАНЕ НА МЕТАЛИ

Изисквания:

Инсталирането на детектор на субстанции е необходимо на входа на обекта или зоната за сигурност на обекти, в които се съхранява информация с ниво на класификация "Строго секретно".

9. РЕЗАЧКИ ЗА УНИЩОЖАВАНЕ НА ИНФОРМАЦИОННИ НОСИТЕЛИ

9.1. Резачки за унищожаване на информационни носители – тип 4	без точки

Изисквания:

Резачките за унищожаване на информационни носители тип 4 се изискват за унищожаване на класифицирана информация от ниво "Строго секретно" или по-ниско.

Изисквания на НАТО и ЕС:

Резачките за унищожаване на информационни носители тип 4 могат да бъдат използвани за унищожаване на класифицирана информация от всички нива на НАТО и ЕС .

Изисквания за резачките за унищожаване на информационни носители с ниво на класификация " Строго секретно":

Информационен носител	Размери на отпадъците	
Напр. хартия, филм от полиестер с информация в оригинален размер, метал, пластмаса, идентификационни карти	ширина на парчетата	≤ 0,8 мм
	дължина на парчетата	≤ 13,0 мм
Напр. филми от полиестер с информация в с намален размер като микрофилми, чип карти	повърхнина на парчетата	≤ 0, 2 кв.мм

9.2. Резачки за унищожаване на информационни носители – тип 3 без точки

Изисквания:

Резачките за унищожаване на информационни носители тип 3 се изискват за унищожаване на класифицирана информация с ниво на класификация "Секретно" или по-ниско.

Изисквания на НАТО и ЕС:

Резачките за унищожаване на информационни носители тип 3 могат да бъдат използвани за унищожаване на класифицирана информация от всички нива на НАТО и ЕС само ако отговарят на изискването за напречен разрез на частите с размери 0,8 мм х 12,5 мм (максимално 1,5 х 20 мм).

Изисквания за резачките за унищожаване на информационни носители с ниво на класификация "Секретно":

Информационен носител	Размери на отпадъците	
Напр. хартия, филм от полиестер с информация в оригинален размер, метал, пластмаса, идентификационни карти	ширина на частиците	≤ 2,0 мм
	дължина на частиците	≤ 15,0 мм
Напр. филми от полиестер с информация в с намален размер като микрофилми, чип карти	повърхнина на частиците	≤ 0, 5 кв.мм

9.3. Резачки за унищожаване на информационни носители – тип 2 без точки

Изисквания:

Резачките за унищожаване на информационни носители тип 2 се изискват за унищожаване на класифицирана информация с ниво на класификация "Поверително" .

Изисквания на НАТО и ЕС:

Резачките за унищожаване на информационни носители тип 2 не могат да бъдат използвани за унищожаване на класифицирана информация на НАТО и ЕС.

Изисквания за резачките за унищожаване на информационни носители с ниво на класификация "Поверително":

<table>
<tr><td>Информационен носител</td><td colspan="3">Размер на отпадъците</td></tr>
<tr><td rowspan="6">Напр. хартия, филм от полиестер с информация в оригинален размер, метал</td><td rowspan="2">напречен разрез</td><td>ширина на парчетата</td><td>≤ 4,0 мм</td></tr>
<tr><td>дължина на парчетата</td><td>≤ 80,0 мм</td></tr>
<tr><td rowspan="3">директен разрез</td><td>ширина на парчетата</td><td>≤ 2,0</td></tr>
<tr><td>дължина на парчетата</td><td>≤ 297,0 мм</td></tr>
<tr><td>повърхнина на парчетата</td><td>≤ 320, 0 кв.мм</td></tr>
<tr><td rowspan="2">Пластмасови материали, идентификационни карти</td><td colspan="2">ширина на парчетата</td><td>≤ 4,0 мм</td></tr>
<tr><td colspan="2">Дължина на парчетата</td><td>≤ 80,0 мм</td></tr>
<tr><td>Напр. филми от полиестер с информация в намален размер като микрофилми, чип карти</td><td colspan="2">повърхнина на парчетата*</td><td>≤ 1 кв. мм</td></tr>
</table>

Заб.
** Това е валидно само за средство с голям капацитет от порядъка на 500 kg/h.*

9.4. Резачки за унищожаване на информационни носители – тип 1 без точки

Изисквания:

Резачките за унищожаване на информационни носители тип 1 се изискват за унищожаване на класифицирана информация с ниво на класификация "За служебно ползване".

Изисквания на НАТО и ЕС:

Резачките за унищожаване на информационни носители тип 1 не могат да бъдат използвани за унищожаване на класифицирана информация на НАТО и ЕС.

Изисквания за резачките за унищожаване на информационни носители с ниво на класификация "За служебно ползване":

<table>
<tr><td>Информационен носител</td><td colspan="3">Размер на отпадъците</td></tr>
<tr><td>Напр. хартия, филм от полиестер с</td><td>Директен</td><td>ширина на лентата</td><td>≤ 6,0 мм</td></tr>
</table>

информация в оригинален размер, метал	разрез	дължина на лентата	неограничена
		повърхнина на парченцата *	≤ 320,0 кв.мм

Заб.
** Това е валидно само за средство с голям капацитет от порядъка на 500 kg/h.*

10. ИЗИСКВАНИЯ ЗА ЗАЩИТА СРЕЩУ НЕРЕГЛАМЕНТИРАН ДОСТЪП ДО КЛАСИФИЦИРАНА ИНФОРМАЦИЯ И ИЗИСКВАНИЯ ЗА ЗАЩИТА НА ОБОСОБЕНИ ТЕХНИЧЕСКИ ОСИГУРЕНИ ЗОНИ

При анализ на риска и разработване на план за физическата сигурност се извършва първоначална проверка за комплексна оценка на физическата защита срещу нерегламентирано прихващане на класифицирана информация.

След комплексната оценка проверяващия орган издава протокол и предписание за състоянието на проверяваната зона.

Протоколът отразяващ извършената проверка трябва да включва следното съдържание:

1. Данни за организацията, която извършва проверката
2. Дата на извършената проверка
3. Използвани технически средства
4. Описание на проверяваната зона
5. Извършени дейности
6. Резултати от проверката
7. Участници в проверката

Проверките за комплексна оценка на физическата защита срещу нерегламентирано прихващане на класифицирана информация (по чл.36, ал.2 от НАРЕДБАТА за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване) се извършват от органите по чл.20 от ЗСРС /МВР, НРС, МО и ДАТО/ след писмено искане от ръководителя на съответната организационна единица, съгласно чл.20, ал.1, т.2 от Инструкция № I—5 от 21.01.2003 г. за реда за използване, осигуряване и прилагане на специални разузнавателни средства от службите на МВР

Контролът срещу нерегламентиран достъп до класифицирана информация се осъществява от органите по чл.20 от ЗСРС /МВР, НРС, МО и ДАТО / след писмено искане от ръководителя на контролиращия орган по смисъла на чл. 3, ал. 2 от Наредбата за реда за извършване на проверките за осъществяване на пряк контрол по защита на класифицираната информация.

11. УСЛОВИЯ ЗА ИЗПОЛЗВАНЕ И РЕД ЗА ИЗГРАЖДАНЕ НА СРЕДСТВАТА И СИСТЕМИТЕ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

11.1. Ред за изграждане на средствата и системите за физическа сигурност на класифицираната информация

11.1.1. Етапи на изграждане

1. Изработване на техническо задание.

2. Изготвяне на технически проект от кандидатите за изпълнители.

3. Определяне на изпълнител и възлагане изпълнението на техническия проект.

4. Изграждане и сертифициране на системите за сигурност.

5. Проверка за изпълнение на изискванията за защита на класифицирана информация.

6. Последващ контрол за изпълнение на изискванията за физическа сигурност.

11.1.2. Изработване на техническото задание – изработването на техническото задание включва мотивиран избор на общи и конкретни мерки за физическа сигурност в зависимост от нивата на класификация и обема на класифицираната информация, с която организационната единица работи при оценка и анализ на риска.

1. Избор на място за изграждане на регистратурата (зони за сигурност) при спазване на изискванията на Наредбата за системата от мерки, способи и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване.

2. Определяне на конкретните физически и технически мерки съгласно чл. 8 , ал. 3 от Наредбата и при спазване изсквания за техническите параметри на всяко физическо средство, съобразно Методиката за изграждане и оценка на средствата за физическата сигурност на класифицираната информация.

3. Оценка на определените в Техническото задание елементи на физическа сигурност, съобразно изискванията за минимален сбор точки по Методиката за изграждане и оценка на средствата за физическата сигурност на класифицираната информация.

4. Утвърждаване на Техническото задание от ръководителя на организационната еднница.

11.1.3. Изготвяне на технически проект от кандидатите за изпълнители – кандидатите за изпълнители изготвят технически проект, който отговаря на всички параметри от Техническото задание и го представя на възложителя.

11.1.4. Определяне на изпълнител и възлагане изпълнението на техническия проект

1. Физическите и юридическите лица, които ще изграждат системи за физическа сигурност на класифицираната информация, трябва да отговарят на изискванията на индустриалната сигурност, ако изпълнението на Техническия проект е свързано с достъп до класифицирана информация-държавна тайна.

2. Изпълнителите трябва да отговарят и на всички нормативни изисквания за извършване на съответната дейност, ако има такива.

11.1.5. Изграждане и сертифициране на системите за сигурност.

1. Изграждане – изпълнителите изграждат системите за сигурност при спазване на Техническия проект, реда и условията за достъп и правилата за работа, приложими в съответната организационна единица.

2. Сертифициране – извършва се за всяко средство и система за физическа сигурност на всеки етап от тяхното изграждане.

3. Компетентни да сертифицират отделните средства и системи за физическа сигурност са както следва:

3.1. Архитектурно-строителна част – инженер-конструктор, съгласно чл. 147, ал. 2 от ЗУТ - за всички организационни единици и за всички нива на класифицирана информация, ако няма разрешение за ползване, издадено от Дирекция за независим строителен контрол към МРРБ.

3.2. Метални каси (контейнери, сейфове) и шкафове и заключващи механизми:

За организационните единици в системата на Министерство на отбраната (МО) и Българската армия (БА) – "Института по отбрана" към министъра на отбраната и други специализирани органи в МО и БА, определени със заповед на министъра на отбраната, за всички нива на класифицирана информация;

За нуждите на Национална разузнавателна служба - Национална разузнавателна служба за всички нива на класифицирана информация;

За нуждите на Служба "Военна информация" - Служба "Военна информация" за всички нива на класифицирана информация;

За всички организационни единици в системата на МВР - Институт за специална техника – МВР и други специализирани органи в системата на МВР за всички нива на класифицирана информация;

За нуждите на Държавната комисия по сигурността на информацията (ДКСИ) - ДКСИ или някой от гореизброените компетентни органи, определен от нея, за всички нива на класифицирана информация;

За всички останали организационни единици – някой от гореизброените компетентни органи за всички нива на класифицирана информация.

3.3. Контрол на физическия достъп:

3.3.1. Алармени системи против проникване /АСПП/;

3.3.2. Система за видеонаблюдение;

3.3.3. Система за контрол на достъпа;

3.3.4. Защита на периметъра;

3.3.5. Металодетектори.

За организационните единици в системата на Министерство на отбраната (МО) и Българската армия (БА) – "Института по отбрана" към министъра на отбраната и други специализирани органи в МО и БА, определени със заповед на министъра на отбраната, за всички нива на класифицирана информация;

За нуждите на Национална разузнавателна служба - Национална разузнавателна служба за всички нива на класифицирана информация;

За нуждите на Служба "Военна информация" - Служба "Военна информация" за всички нива на класифицирана информация;

За нуждите на Министерство на вътрешните работи - Дирекция "Национална служба полиция" - МВР, Институт за специална техника - МВР и други специализирани органи за всички нива на класифицирана информация;

За нуждите на Държавната комисия по сигурността на информацията (ДКСИ) - ДКСИ или някой от гореизброените компетентни органи, определен от нея, за всички нива на класифицирана информация;

За всички останали организационни единици - Дирекция "Национална служба полиция" - МВР и някой от гореизброените компетентни органи за всички нива на класифицирана информация.

3.4. Резачки за унищожаване на информационни носители:

За организационните единици в системата на Министерство на отбраната (МО) и Българската армия (БА) –"Института по отбрана" към министъра на отбраната и други специализирани органи в МО и БА, определени със заповед на министъра на отбраната, за всички нива на класифицирана информация;

За нуждите на Национална разузнавателна служба - Национална разузнавателна служба за всички нива на класифицирана информация;

За нуждите на Служба "Военна информация" - Служба "Военна информация" за всички нива на класифицирана информация;

За всички организационни единици в системата на МВР - Институт за специална техника – МВР и други специализирани органи в системата на МВР за всички нива на класифицирана информация;

За нуждите на Държавната комисия по сигурността на информацията (ДКСИ) - ДКСИ или някой от гореизброените компетентни органи, определен от нея, за всички нива на класифицирана информация;

За всички останали организационни единици – някой от гореизброените компетентни органи за всички нива на класифицирана информация.

3.5. Системи, осигуряващи пожарна и аварийна безопасност:

За всички организационни единици - "Национална служба пожарна и аварийна безопасност" - МВР за всички нива на класифицирана информация.

4. Компетентните за сертифициране органи оказват съдействие на организационните единици – възложители на всички етапи от изграждане на регистратурите като консултират и утвърждават Техническия проект на лицето, определено за изпълнител.

5. Сертифицирането на средствата и системите за физическа сигурност се извършва от съответния компетентен орган по т. 3, който удостоверява съответствието между използваните физически средства и цялостното изпълнение на възложения Технически проект с минималните изисквания на Методиката за изграждане и оценка на средствата за физическата сигурност на класифицираната информация.

6. При установено съответствие по т. 5 компетентният орган издава удостоверение (сертификат), екземпляр от който се изпраща в организационната единица.

11.1.6. Проверка за изпълнение на изискванията за защита на класифицирана информация (ЗЗКИ и ППЗЗКИ).

1. Проверката се извършва от комисия, назначена от ръководителя на организационната единица по реда и условията на ЗЗКИ, ППЗЗКИ и Задължителните указания на ДКСИ.

2. Комисията проверява изпълнение на изискванията за защита на класифицирана информация и наличието на издадени удостоверения от съответните компетентни органи за всяко средство и система за физическа сигурност на класифицираната информация.

3. Компетентен орган да провери изпълнението на изискванията за защита на класифицирана информация и наличието на издадени удостоверения от съответните компетентни органи за всяко средство и система за физическа сигурност на класифицираната информация при изграждане на регистратури в областта на международните отношения е ДКСИ.

11.1.7. Последващ контрол за изпълнение на изискванията за физическа сигурност.

1. Всеки компетентен орган по т. 11.1.5. т.3. има право по всяко време да проверява средствата и системите за физическа сигурност, сертифицирани от него за тяхното съответствие с изискванията за физическа сигурност.

2. Компетентните органи за осъществяване на пряк контрол по чл. 12 от ЗЗКИ и ДКСИ имат право да извършват контрол за спазване на законовите разпоредби в областта на физическата сигурност.

11.2. Удостоверение (Сертификат) на техническите средства и системи.

11.2.1. Съдържание на Удостоверението (сертификата).

Удостоверението (сертификатът) се издава за всяко отделно техническо средство и система с определена идентификация (напр. производствен номер), която изрично се посочва в удостоверението (сертификата). Удостоверението (сертификатът) се издава по искане на организационната единица-възложител или на изпълнителя.

11.2.2. Срок на Удостоверението (сертификата).

Удостоверението (сертификатът) се издава за срок, определен от компетентния да го издаде орган. Три месеца преди изтичане на този срок ръководителят на организационната единица е длъжен да поиска проверка от съответния компетентен орган на всички използвани технически средства и системи за тяхното състояние и съответствието им с изискванията за физическа сигурност. Компетентният орган по реда и условията на тази Методика издава ново удостоверение с посоченото в т. 11.2.1. съдържание. Ако компетентният орган констатира несъответствие на конкретното средство с изискванията за физическа сигурност отказва издаване на ново удостоверение. В този случай ръководителят на организационната единица е длъжен да предприеме всички необходими действия за привеждане на съответното средство или система в съответствие с изискванията за физическа сигурност на класифицираната информация.

11.3. Условия за използване на техническите средства за физическа сигурност.

След изтичане на първоначалния срок на валидност техническите средства могат да бъдат използвани при условие, че са напълно функционални. При всички случаи тяхната функционалност и съответствието на реалното състояние на мерките по сигурността с изискванията по физическа сигурност е необходимо да бъде проверена в рамките на издаване на новото удостоверение (сертификат) по реда на т. 11.2.

12. ОЦЕНКА НА ЕЛЕМЕНТИТЕ НА ФИЗИЧЕСКАТА СИГУРНОСТ

12.1 Каса и ключалки

Каси (виж 1.1):

Класификация на касите	**Оценка (SS1)**	**Стандарти по сигурността**
Тип 4	**4 точки**	**Виж 1.1.1**
Тип 3	**3 точки**	**Виж 1.1.2**
Тип 2	**2 точки**	**Виж 1.1.3**

Тип 1	**1 точка**	**Виж 1.1.4**

Ключалки на каси (виж 1.2):

Класификация на касите	**Оценка (SS2)**	**Стандарти по сигурността**
Тип 4	**4 точки**	**Виж 1.2.1**
Тип 3	**3 точки**	**Виж 1.2.2**
Тип 2	**2 точки**	**Виж 1.2.3**
Тип 1	**1 точка**	**Виж 1.2.4**

Обща оценка на касата и нейната ключалка:
(S1) =SS1 x SS2

12.2 Зони на сигурност и техните заключващи системи

Зони на сигурност (виж 2.1):

Класификация на зоните на сигурност	**Оценка (SS3)**	**Стандарти по сигурността**
Тип 4	**4 точки**	**Виж 2.1.1**
Тип 3	**3 точки**	**Виж 2.1.2**
Тип 2	**2 точки**	**Виж 2.1.3**
Тип 1	**1 точка**	**Виж 2.1.4**

Заключващи системи на зоните за сигурност (виж 2.2):

Класификация на заключващите системи	**Оценка (SS4)**	**Стандарти по сигурността**
Тип 4	**4 точки**	**Виж 1.2.1**
Тип 3	**3 точки**	**Виж 1.2.2**
Тип 2	**2 точки**	**Виж 1.2.3**
Тип 1	**1 точка**	**Виж 1.2.4**
Некласифицирани	**0 точки**	

Обща оценка на зоните за сигурност и техните заключващи системи:
(S2) = SS3 x SS4

12.3 Обект (виж 3)

Класификация на обектите	**Оценка (S3)**	**Стандарти по сигурността**
Тип 4	**5 точки**	**Виж 3.1**
Тип 3	**3 точки**	**Виж 3.2**
Тип 2	**2 точки**	**Виж 3.3**
Тип 1	**1 точка**	**Виж 3.4**

Обща оценка на обекта:
(S3) = 5,3,2 или 1

12.4 Контрол на входа и изхода на зоната на сигурност или обекта

Контрол на входа и изхода (виж 4.1):

Класификация	Оценка Междинни резултати(SS6)	Стандарти по сигурността
Тип 4	4 точки	Виж 4.1.1
Тип 3	3 точки	Виж 4.1.2
Тип 2	2 точки	Виж 4.1.3
Тип 1	1 точка	Виж 4.1.4
Некласифициран	0 точки	

Режим на посещения в обекта(виж 4.3):

Класификация на режима на посещения	Оценка Междинни резултати(SS7)	Стандарти по сигурността
Посещение с охрана	3 точки	Виж 4.3.1
Посещение без охрана	1 точка	Виж 4.3.2
Посещение без контрол	0 точки	Виж 4.3.2

Обща оценка на контрола на достъп:
(S4) = SS6 + SS7

12.5 Охрана и системи за наблюдение на влизането

Охрана (виж 5.1):

Класификация на охраната	Оценка Междинни резултати(SS8)	Стандарти по сигурността
Тип 5	5 точки	Виж 5.1.1
Тип 4	4 точки	Виж 5.1.2
Тип 3	3 точки	Виж 5.1.3
Тип 2	2 точки	Виж 5.1.4
Тип 1	1 точка	Виж 5.1.5
Некласифицирана	0 точки	

Алармена система против проникване (АСПП) (виж 5.2)

Ниво на техническите средства на АСПП (виж 5.2.1):

Класификация на нивото на АСПП	Оценка Междинни резултати(SS91)	Стандарти по сигурността
Тип 4	4 точки	Виж 5.2.1.1
Тип 3	3 точки	Виж 5.2.1.2
Тип 2	2 точки	Виж 5.2.1.3
Тип 1	1 точка	Виж 5.2.1.4

Инсталиране на технически средства на АСПП (виж 5.2.2):

Класификация на инсталирането на АСПП	Оценка Междинни резултати (SS92)	Стандарти по сигурността
Тип 4	4 точки	Виж 5.2.2.1
Тип 3	3 точки	Виж 5.2.2.2
Тип 2	2 точки	Виж 5.2.2.3
Тип 1	1 точка	Виж 5.2.2.4

Междинен резултат
(SS9) = ((SS91 + SS92) x К/2
Постановка:
Междинният резултат SS9 е необходимо да се закръгли до най-близкото интегрално число!!!Най-високото число, което може да се получи за SS9 е 4!!!
К е коефициент на инсталиране, което произлиза от изчисляване на междинните резултати от SS92.

К = SS92 / OBL

OBL е обозначение, определено от категорията на зоната за сигурност

Категория на зоната на сигурност	**Оценка OBL**
“СС”-Строго секретно	**4 точки**
“С” -Секретно	**3 точки**
“П” -Поверително	**2 точки**
“СП”-За служебно ползване	**1 точка**

Обща оценка на охраната и системите за наблюдение на влизането
(S5) = SS8 + SS9

12.6 Защита на периметъра

Физически бариери (виж 6.1):

Класификация на физическите бариери	**Оценка Междинни резултати (SS10)**	**Стандарти по сигурността**
Тип 4	**4 точки**	**Виж 6.1.1**
Тип 3	**3 точки**	**Виж 6.1.2**
Тип 2	**2 точки**	**Виж 6.1.3**
Тип 1	**1 точка**	**Виж 6.1.4**
Некласифицирани	**0 точки**	

Контрол на входа на физическите бариери (виж 6.2):

Контрол на на входа на местата за достъп	**Оценка Междинни резултати (SS11)**	**Стандарти по сигурността**
Осъществява се	**1 точка**	**Виж 6.2**
Не се осъществява	**0 точки**	**Виж 6.2**

Произволен (случаен) контрол на входовете и изходите(виж 4.2):

Случаен контрол на достъпа до входовете и изходите	**Оценка Междинни резултати (SS12)**	**Стандарти по сигурността**
Осъществява се	**1 точка**	**Виж 4.2**
Не се осъществява	**0 точки**	**Виж 4.2**

Системи на сигурност по периметъра (виж 6.3)

Детекторна система за наблюдение на периметъра (виж 6.3.1):

Детекторна система за наблюдение на периметъра	**Оценка Междинни резултати (SS13)**	**Стандарти по сигурността**
Съществува	**2 точки**	**Виж 6.3.1**
Не съществува	**0 точки**	**Виж 6.3.1**

Защитни светлини по периметъра(виж 6.3.2):

Защитни светлини	**Оценка Междинни резултати (SS14)**	**Стандарти по сигурността**
Има	**2 точки**	**Виж 6.3.2**
Няма	**0 точки**	**Виж 6.3.2**

12.6.1 Системи за видеонаблюдение за защита по периметъра (вж.6.3.3.)

Система за видеонаблюдение	**Оценка Междинни резултати (SS15)**	**Стандарти по сигурността**
Има	**2 точки**	**Виж 6.3.3**
Няма	**0 точки**	**Виж 6.3.3**

Обща оценка на сигурността на периметъра
(S6) = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15

13. МИНИМАЛНИ ИЗИСКВАНИ ПОКАЗАТЕЛИ ЗА ОЦЕНКА НИВОТО НА ФИЗИЧЕСКАТА СИГУРНОСТ

13.1. ТАБЛИЦА ЗА МИНИМАЛНО ИЗИСКВАНИТЕ ПОКАЗАТЕЛИ ЗА ОЦЕНКА НИВОТО НА ФИЗИЧЕСКА СИГУРНОСТ НА ЗОНИТЕ НА СИГУРНОСТ, КЪДЕТО СЕ СЪХРАНЯВА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ ИЛИ КЪДЕТО ИМА ЧАСТИ ОТ ИНФОРМАЦИОННА СИСТЕМА(ИС)

Зона на сигурност тип 4 (“Строго секретно”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**
Задължителни: S1 + S2 + S3	**10**	**11**	**13**
Задължителни: S4 + S5 *	**6**	**7**	**7**
Незадължителни: S6	**4**	**5**	**5**
Общ резултат	**20**	**23**	**25**

Зона на сигурност тип 3 (“Секретно”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**
Задължителни: S1 + S2 + S3	**8**	**9**	**10**
Задължителни: S4 + S5 **	**4**	**5**	**5**

Незадължителни: S6	**4**	**5**	**5**
Общ резултат	**16**	**19**	**20**

Зона на сигурност тип 2 (“Поверително”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**
Задължителни: S1 + S2 + S3	**6**	**8**	**9**
Задължителни: S4 + S5	**2**	**3**	**3**
Незадължителни: S6	**3**	**3**	**4**
Общ резултат	**11**	**14**	**16**

Зона на сигурност тип 1 (“За служебно ползване”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**
Задължителни: S1 + S2 + S3	**2**	**2**	**2**
Незадължителни: S4 + S5 + S6	**0**	**1**	**2**
Общ резултат	**2**	**3**	**4**

Забележка:
- Качество S5 трябва да достига поне 5 точки (за изчисление вж. 12.5)*
*-**Качество S5 трябва да достига най-малко 4 точки (за изчислението му вж.12.5.)*
Само едно от качестваS1, S2 или S3 може да бъде равно на 0.

13.2 ТАБЛИЦА НА МИНИМАЛНО ИЗИСКВАНИТЕ ПОКАЗАТЕЛИ ЗА ОЦЕНКА И ОБОЗНАЧАВАНЕ НА НИВОТО НА ФИЗИЧЕСКАТА СИГУРНОСТ НА ЗОНИТЕ НА СИГУРНОСТ, КЪДЕТО КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ Е ПРЕДМЕТ НА РАЗГОВОРИ

Тази таблица е валидна само за съвещателни зали, където класифицираната информация не се съхранява, а е само предмет на дискусии.

Зона на сигурност тип 4 (“Строго секретно”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**
Задължителни: S2 + S3	**6**	**6**	**7**
Задължителни: S4 + S5 *	**6**	**7**	**7**
Незадължителни: S6	**4**	**5**	**5**
Общ резултат	**16**	**18**	**19**

Зона на сигурност тип 3(“Секретно”)	**Степен на застрашеност**		
	Ниска	**Средна**	**Висока**

Задължителни: S2 + S3	**5**	**5**	**6**
Задължителни: S4 + S5 **	**4**	**5**	**5**
Не задължителни: S6/C6	**4**	**5**	**5**
Общ резултат	**13**	**15**	**16**

Забележка:
**КачествоS5 трябва да достига поне 5 точки (за изчисление вж.12.5.)*
*** Качество S5 трябва да достига поне 4 точки (за изчисление вж.12.5.)*

Качество S2 не трябва да бъде равно на 0.

Качества S1, S2, S3, S4, S5, S6 отговарят на общата сума съгласно глава 12.
S1: Каси и техните ключалки (вж.12.1.)
S2: Зони на сигурност и техните заключващи системи (вж.12.2.)
S3: Обекти (вж.12.3.)
S4: Контрол на достъпа (вж.12.4.)
S5: Охрана и детекторни системи за наблюдение на влизането (вж.12.5.)
S6: Защита на периметъра (вж. 12.6)

13.3. ТАБЛИЦА ЗА ОЦЕНКА НА МЕРКИТЕ ЗА СИГУРНОСТ В ЗОНАТА НА СИГУРНОСТ

Таблица 13.3. е необходимо да бъде попълнена с оценките на отделните средства за сигурност съгласно описанието в глава 1 до 10 от Методиката. В случай, че отделните мерки са без оценка, те се показват отделно в приложение към таблицата.

Заглавието на таблицата съдържа следната информация:
1. име на зоната на сигурност
2. категория и клас на зоната на сигурност
3. предназначение на зоната на сигурност (регистратура, зала за съвещания и др.)

Мерки за сигурност	**Вид**	**Оценка**
Каси (виж 1.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS1 =**
Ключалки на каси (виж 1.2)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS2 =**
Обща оценка на касата и нейната ключалка(виж12.1)	S1 = SS1 x SS2	**S1 =**
Зони на сигурност (виж 2.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS3 =**
Заключващи системи на зоните на сигурност(виж 2.2)	Тип 4 – 4 точки Тип 3 – 3 точки	**SS4 =**

	Тип 2 – 2 точки Тип 1 – 1 точка	
Обща оценка на зоната на сигурност и нейната заключваща система(виж 12.2)	S2 = SS3 x SS4	**S2 =**
Обекти (Сгради) (виж3)	Тип 4 – 5 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**S3 =**
Контрол на достъпа (виж 4.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS6 =**
Режим и посещения в обектите (виж 4.3) А) посещения с охрана Б) посещения без охрана В) посещения без контрол	Точка А) – 3 точки Точка Б) – 1 точка Точка В) – 0 точки	**SS7 =**
Обща оценка на контрола на достъп (виж12.4)	S4 = SS6 + SS7	**S4 =**
Охрана (виж 5.1)	Тип 5 – 5 точки Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS8 =**
Ниво на техническите средства на АСПП (виж5.2.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS91=**
Инсталиране на техническите средства на АСПП (виж 5.2.2.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS92=**
Междинни резултати(SS9) (за изчисление виж 12.5)		**SS9 =**
Обща оценка на охраната и на АСПП (виж 12.5)	S5 = SS8 +SS9	**S5 =**
Физически бариери (виж 6.1)	Тип 4 – 4 точки Тип 3 – 3 точки Тип 2 – 2 точки Тип 1 – 1 точка	**SS10 =**
Контрол на достъпа на физически бариери (виж 6.2) А) контрол се осъществява Б) контрол не се осъществява	Точка А) – 1 точка Точка Б) – 0 точки	**SS11 =**
Произволен контрол на достъпа на входове и изходи(виж 4.2) А) контрол се осъществява Б) контрол не се осъществява	Точка А) – 1 точка Точка Б) – 0 точки	**SS12 =**
Детекторна система за		**SS13 =**

наблюдение на периметъра (ДСНП)(виж6.3) А) ДСНП съществува Б) ДСНП не съществува	Точка А) – 2 точки Точка Б) – 0 точки	
Защитни светлини по периметъра (виж 6.3.2) А) има защитни светлини Б) няма защитни светлини	Точка А) – 2 точка Точка Б) – 0 точки	**SS14 =**
Система за видеонаблюдение (виж 6.3.3) А) Системата съществува Б) Системата не съществува	Точка А) – 2 точка Точка Б) – 0 точки	**SS15 =**
Обща оценка на защита на периметъра (виж 12.6)	S6 = (SS10 x SS11) +SS12 +SS13 +SS14 + SS15	**SS6 =**

Стойностите на вариращите S1 - S6, получени при попълване на таблицата за оценка на мерките за сигурност в зоната на сигурност, е необходимо да бъдат сравнени с таблиците за минимални стойности съгласно 13.1. или 13.2. На основата на това сравнение е възможно да се идентифицира дали възприетите мерки за сигурност съответстват (са достатъчни) за дадената степен на риска и категория на зоната на сигурност.

13.4. ОПИСАНИЕ И ИЗБОР НА МЕРКИ ЗА СИГУРНОСТ

Таблицата на минимално изискваните показатели за оценка и обозначаване нивото на физическата сигурност (вж.13.1., 13.2) и избора на мерки за сигурност с цел гарантиране на физическата сигурност (вж. глави от 1 до 10) съставляват броя на възможните мерки за осъществяване на т.нар. “дълбока сигурност”, която отговаря на изискванията, дадени в текста на Методиката за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация. Методиката за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация регламентира управлението на рисковете за сигурността във формата на предложение от средства, които от своя страна правят възможен изборът на най-подходящите и стойностно изгодни комбинации от мерки за сигурност срещу нерегламентиран достъп до класифицирана информация.

Изборът на средствата за физическа сигурност трябва да бъде адекватен на резултатите от извършена предварителна оценка на заплахите за физическата сигурност на класифицираната информация. С предварителната оценка се цели установяване на възможните заплахи и вреди в резултат на нерегламентиран достъп, опит за нерегламентиран достъп, както и влиянието и последиците при тяхното проявление. Тя включва:

1. Определяне на обекта, подложен на опасност или заплаха;

2. Установяване зависимостта на обекта и възможната опасност или заплаха от нерегламентиран достъп до класифицирана информация;

3. Определяне на възможните вреди в съответствие с § 1, т. 15 от Допълнителните разпоредби на Закона за защита на класифицираната информация.

Въз основа на горните констатации се извършва комплексна оценка относно степента на застрашеност, която може да бъде ниска, средна или висока.

Висока степен на застрашеност е налице в случаите, когато вследствие нерегламентиран достъп е настъпило или би могло да настъпи цялостно или частично разрушаване на националната сигурност или интересите на Република България, свързани с нея, като основни защитавани интереси.

Средна степен на застрашеност е налице в случаите, когато вследствие нерегламентиран достъп може да настъпи или е настъпило значително негативно въздействие върху националната сигурност или интересите на Република България, свързани с нея, като основни защитавани интереси, което не може да се компенсира без настъпване на вредни последици или вредните последици могат да бъдат смекчени само със значителни последващи мерки.

Ниска степен на застрашеност е налице в случаите, когато вследствие нерегламентиран достъп може да настъпи или е настъпило краткотрайно негативно въздействие върху националната сигурност и интересите на Република България, свързани с нея, което може да се компенсира без настъпване на вредни последици или вредните последици могат да бъдат смекчени с незначителни последващи мерки.

Минималните основни мерки са дадени в първата колона на таблици 13.1. или 13.2. (ниска степен на застрашеност). В другите колони са обозначенията на мерките за сигурност, които отговарят на по-висока степен на застрашеност.

Ако на базата на анализа се установи, че възприетите мерки за сигурност не са адекватни, дори да е достигната изискваната цифра на оценка, необходимо е да бъде оценено прилагането на допълнителни мерки или тяхната алтернативна комбинация.

Таблици 13.1. и 13.2. служат най-вече като модели, на базата на които се идентифицира минималното ниво на мерките за сигурност. За използване на подходящите мерки и процедури на физическа сигурност е определяща степента на застрашеност, произтичаща от средата, в която се извършват дейностите, свързани с класифицираната информация.

Обозначаването на мерките за сигурност в таблици 13.1. и 13.2, които се изискват за гарантиране защитата на съответното ниво на класифицирана информация, произтича от описанието на мерките за сигурност в главите от 1 до 10 на тази Методика. Първите две точки произтичат от задължителните мерки , а останалите - от допълнителните (незадължителни). Този начин от задължителни и незадължителни мерки цели осигуряването на чувствителния баланс на отделните стъпки и прави възможен гъвкавия напредък в избора на мерки за сигурност, който цели достигане на исканата степен на защита, като се има предвид дадената конкретна ситуация, техническата сигурност, оборудването и работния потенциал.

Таблици 13.1. и 13.2. могат да бъдат използвани така, че чрез тях да се избере степента на чувствителност на класифицираната информация и да се направи обща оценка, която трябва да се достигне на основата на описание на мерките за сигурност в главите 1 до 10. След осигуряване на изискваната обща качествена оценка се избират мерките, дадени в описанието на мерките за сигурност.

Описанието на мерките за сигурност се разделя на десет параграфа, всеки от които е посветен на определен аспект от сигурността. За улеснение може да се използва таблицата за обозначаване на мерките за сигурност в зоната на сигурност (вж.13.3. Проект по сигурността за защита на обекта). Таблица 13.3. се предлага като

предварителна и там са дадени оценките на отделните видове мерки. В тази таблица е оставено и празно място, за да се напише оценката на конкретното средство в нея.

При избора на мерки за сигурност е целесъобразно да се подходи по следния начин:

1. В таблица 13.3. напишете оценките на съществуващите мерки за сигурност
2. Попълнете общия резултат
3. Получените резултати сравнете с исканите показатели според таблици 13.1. и 13.2.
4. Установете дали съществуващите мерки за сигурност са адекватни или занижени
5. Изберете правилния начин на повишаване нивото на мерките за сигурност

Ако е необходимо усъвършенстване на мерките за сигурност, трябва да се прибегне към най-подходящото за дадена конкретна ситуация, като в същото време се използват най-добрите достъпни средства.

На значението на някои мерки за сигурност се набляга чрез факта, че оценката им с точки се умножава по оценката на други средства (напр. каси и ключалки), докато в други случаи – се прибавя (напр. огради, светлини, телевизионни системи).

ЗАДЪЛЖИТЕЛНИ УКАЗАНИЯ

ЗА РАЗКРИВАНЕ, ФУНКЦИОНИРАНЕ И ЗАКРИВАНЕ НА РЕГИСТРАТУРА ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА /ДКСИ/ в качеството си на държавен орган, осъществяващ политиката на Република България за защита на класифицираната информация, който организира, осъществява, координира и контролира дейността по защита на тази информация, и на основание чл. 10, ал. 1, т. 4 от Закона за защита на класифицираната информация /ЗЗКИ / въз основа на Решение на ДКСИ № 19-I /20.03.08 г., изм. с Решение на ДКСИ № 16-I/05.03.09 г. издава

ЗАДЪЛЖИТЕЛНИ УКАЗАНИЯ

до задължените по ЗЗКИ субекти в следните насоки:

I. ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите задължителни указания уреждат реда и условията за разкриване, функциониране и закриване на регистратура за класифицирана информация.

2. Регистратура за класифицирана информация се разкрива въз основа на предварителен анализ и преценка относно обективната необходимост за получаване, създаване, регистриране, обработване, съхраняване, разпределяне, предоставяне и размножаване на класифицирана информация на ръководителя на организационната единица, проверка за изпълнение на изискванията за защита на класифицираната информация и решение на ДКСИ за издаване на уникален идентификационен номер от. Нивото на съответната регистратура се определя в зависимост от най-високото ниво на класификация на съхраняваните или създаваните документи.

3. Закриване на регистратура за класифицирана информация е преустановяване на дейността на съответната регистратура за класифицирана информация. Закриването се счита за завършено след произнасяне на ДКСИ с решение за анулиране на уникалния идентификационен номер.

4. Регистратура за класифицирана информация се закрива в случаите на отпадане на основанията за регистриране, получаване, изпращане, разпределяне, изработване, размножаване, предоставяне и съхраняване на класифицирана информация и при спазване на реда и условията съгласно настоящите задължителни указания.

II. РАЗКРИВАНЕ НА РЕГИСТРАТУРА ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

1. Регистратурите за работа с национална класифицирана информация се откриват след проверка за изпълнение изискванията за защита на класифицираната информация.

2. Проверката по т. II.1. се извършва от комисия, назначена от ръководителя на организационната единица и 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 съответната служба за сигурност.

3. 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 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, трябва да има издадено разрешение за достъп до определеното ниво на класификация на изградената регистратура.

4. Процедурата за извършване на проверката задължително трябва да включва констатации по отношение на следните обстоятелства:

4.1. Изпълнение на изискванията за защита на класифицираната информация в съответната регистратура;

4.2. Реда и условията за работа в регистратурата;

4.3. 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;

4.4. 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;

4.5. Дали са въведени в експлоатация и начина на водене на новите регистри по ППЗЗКИ;

4.6. Проверка на наличните документи и начина им на съхранение в регистратурата;

4.7. Проверка дали регистратурата отговаря на изискванията за физическа сигурност по ЗЗКИ, ППЗЗКИ и Наредба за системата от мерки, способи и средства за физическа сигурност на класифицираната информация и за условията и реда за тяхното използване (нар. за краткост по-нататък само Наредбата). Средствата за физическа сигурност следва да са сертифицирани за всяко ниво на класификация съгласно изискванията на чл. 4 от Наредбата;

4.8. Проверка дали начина на унищожаване на документи съответства на изискванията на ЗЗКИ и ППЗЗКИ;

4.9. Проверка за съответствие със законовите изисквания на определяне грифовете за сигурност на създаваните в регистратурата документи;

4.10. Проверка за спазване на задължителните специфични изисквания за сигурност на автоматизираните информационни системи (АИС) или мрежи;

4.11. Проверка дали са изготвени и утвърдени от ръководителя на организационната единица следните документи:

- анализ на риска;
- план за физическата сигурност;
- заповед за изграждане на зоните за сигурност;
- инструкция за действия на служителите от звеното за сигурност при нерегламентиран достъп;
- заповед за контрол на ключовете и шифровите комбинации на защитените каси;
- инструкция за пропусквателния режим;
- вътрешни правила за правилното определяне на нивото на класификация, както и за неговата промяна или премахване;

- план за защита на класифицираната информация при положение на война, бедствия и аварии.

5. Проверката на комисията задължително завършва с протокол, в който се описват забележките и препоръките на комисията към начина на работа в регистратурата. / Приложение № 1 – Примерен протокол/. Към протокола задължително се изготвя "Таблица за оценка на мерките за сигурност в зоната на сигурност" съгласно т. 13.3. от Методиката за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация.

6. Едва след отстраняване на констатираните пропуски, един екземпляр от изготвения протокол заедно с попълнената таблица по т.V.5. от настоящите Задължителни указания се изпраща на ДКСИ и на съответната служба за сигурност. ДКСИ разглежда на свое заседание отразените в протокола констатации и взима решение за издаване на уникален идентификационен номер /УИН/ и сертификат на регистратурата.

III. ПРОМЯНА В СТАТУТА НА РЕГИСТРАТУРАТА

1. За всички промени, свързани със статута на регистратура за класифицирана информация следва да бъде отправено писмено уведомление до ДКСИ и органа по прекия контрол.

2. Потвърждаването на УИН на изградена и сертифицирана регистратура за класифицирана информация се извършва от ДКСИ в случаите на промяна на месторазположението на регистратурата, нивото на сигурност на регистратурата, респективно мерките за сигурност на класифицираната информация и промяна в наименованието на организационната единица, вследствие преструктуриране и/или преобразуване.

3. В случаите, когато промяната е свързана с месторазположението на регистратурата или повишаване нивото на сигурност, респективно мерките за сигурност на класифицираната информация, 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.

4. В случаите, когато се понижава нивото на сигурност на дадена регистратура, 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 към момента на разкриването й или опис на предадените в друга регистратура документи, при спазване на съответните нормативни изисквания.

5. В случаите, когато се променя наименованието на организационната единица, вследствие преструктуриране и/или преобразуване, ръководителят на организационната единица, както и др. обстоятелства, уведомителното писмо до ДКСИ следва да съдържа потвърждение (декларация), че в регистратурата са запазени мерките за физическа сигурност при изграждането й. Към уведомителното писмо до ДКСИ следва да бъде приложено и съдебно решение или друг документ за промените в статута, наименованието и т.н. на организационната единица, независимо от правноорганизационната й форма.

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

7. Издадените сертификати за регистратурите за класифицирана информация се преиздават с новите данни след връщането на предходно издадения сертификат.

IV. РЕД И УСЛОВИЯ ЗА ЗАКРИВАНЕ НА РЕГИСТРАТУРА ЗА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

1. 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 глава пета, раздел IX от ППЗЗКИ или по други причини.

2. 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. В случаите на обективна невъзможност предложението за закриване на регистратурата се изготвя от ръководителя на организационната единица или завеждащия регистратура.

3. В предложението по ал. 2 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.

4. Към предложението задължително се прилага издадения от ДКСИ сертификат на съответната регистратура за класифицирана информация.

5. 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. След приключване на проверката органът по прекия контрол изпраща до ДКСИ доклад за извършената проверка.

6. 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 чрез изпращане на препис – извлечение от решението след влизането му в сила.

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

Настоящите задължителни указания отменят приетите с решение на ДКСИ № 3 / 25.02.2003 г. “Задължителни указания относно регистратурите за класифицирана информация” и приетите с решение на ДКСИ № 24-I / 19.04.2007 г. “Задължителни указания за закриване на регистратура за класифицирана информация“

Настоящите задължителни указания подлежат на незабавно изпълнение.

ПРИЛОЖЕНИЕ № 1

ПРОТОКОЛ рег. №……..

За извършена проверка на регистратура за класифицирана информация

Днес,……..г. /дата/ в изпълнение на заповед на……. /ръководител на организационната единица/ №……., на основание чл.54 от Правилника за прилагане на Закона за защита на класифицираната информация, комисия в състав:

1. …… - служител по сигурността на информацията, разрешение №……., до ниво……., издадено от ДКСИ на ……./дата/;
2. …… - представител на …… /съответната организационна единица, длъжност/, разрешение №……., до ниво……., издадено от ДКСИ на ……./дата/;
3. ……. .....– представител на…….. /съответната служба за сигурност, длъжност/;

извърши проверка за изпълнение на нормативните изисквания за откриване на регистратура за класифицирана информация с ниво на класификация“……”
……../наименование на организационната единица/ и завеждащ регистратура ...../ имена/ , с издадено разрешение за достъп до класифицирана информация № ..... , ниво на достъп и констатира следното:

1. Регистратурата за класифицирана информация в ..... / наименование на организационната единица / е изградена съобразно изискванията на Глава VI, раздел I от ЗЗКИ и Наредбата за системата от мерки, способи и средства за физическа сигурност на класифицираната информация и реда за тяхното използване. Описват се конкретно приложените физически и технически мерки за защита на класифицираната информация в съответствие с чл.14 от Наредбата и в последователността на описаните средства за физическа сигурност в “Методиката за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация”, приета от ДКСИ по Протокол № 165 от 30.06.2004 г.: каси, заключващи механизми, зони за сигурност, изисквания към помещението, заключващи системи, врати и прозорци, контрол на достъпа, охрана и системи за сигурност, алармена система против проникване, система за видеонаблюдение, защита на периметъра, пожароизвестителни и пожарогасителни системи, резачки за унищожаване на информационни носители.

2. Редът и условията за работа в регистратурата отговарят на изискванията за защита на класифицираната информация съгласно ЗЗКИ, ППЗЗКИ и другите подзаконови нормативни актове в областта на защита на класифицираната информация.

3. Назначените служители за работа в регистратурата са включени в списъка по чл.37 от ЗЗКИ, респективно в списъка по чл. 23 от ППЗЗКИ, съхранявани в ДКСИ и отговарят на изискванията на чл.38, ал. 1, т.1 и 2 от ЗЗКИ и на чл. 61 от ППЗЗКИ.

4. Извършена е проверка на наличните документи и материали и начина на съхранението им в регистратурата.

5. Извършена е проверка за съответствие със законовите изисквания за определяне грифовете за сигурност на създаваните в регистратурата документи и материали. Оценка на изпълнението на задълженията по § 9 от Преходните и заключителните разпоредби на ЗЗКИ и изпратен протокол за извършеното в ДКСИ.

6. Извършена проверка за съответствие на начина на унищожаване на документи и материали с изискванията на ЗЗКИ и ППЗЗКИ.

7. Въвеждане в експлоатация на новите регистри по ППЗЗКИ и начин на воденето им.

8. Изготвени и утвърдени от ръководителя на организационната единица задължителни документи за физическата сигурност указани в т. II. 4. от настоящите Задължителни указания.

9. Мотивирано становище.

Приложение: Екземпляр от изготвената оценка на мерките за сигурност, съобразно изискванията на т.13.3 от "Методика за изграждане и оценка на средствата и системите за физическа сигурност на класифицираната информация".

Дата: Имена, подпис : 1.....
2.....
Място: Печат: 3.....

<u>Фирми, обявили се пред ДКСИ с акредитация за производство, внос и изпитвания на средства за физическа сигурност на класифицираната информация.</u>

- фирма „ЗИНО-П" АД, гр. Петрич – производител на сертифицирани каси и сейфове;
- фирма „Синхрон-С" ООД – производител на устройства за контрол на достъпа;
- фирма „Промет България' ЕООД – вносител на сейфове и метални шкафове, притежаващи необходимите сертификати съгласно Европейските стандарти;
- фирма „Стил Лайн" ООД - вносител на сейфове и метални шкафове, притежаващи необходимите сертификати съгласно EN – 1143 – 1 (за степен на съпротивление) и EN – 1300 (за сигурност на заключващите механизми);
- изпитателна лаборатория на „ТЕХНОСТ" – София с възможности за изпитване на продукти за физическа сигурност, използвани за

защита на класифицирана информация, с цел сертифицирането им по изискванията на стандартите: БДС EN 1143 -1, БДС EN 1143 -2, БДС ENV 1627, БДС EN 1522, БДС EN 1062 и БДС EN 356.