

НАРЕДБА за системата от мерки, способности и средства за физическата сигурност на класифицираната информация и за условията и реда за тяхното използване

Приета с ПМС № 52 от 4.03.2003 г., обн., ДВ, бр. 22 от 11.03.2003 г., в сила от 11.03.2003 г. кн. 4/2003 г., стр. 289 т. 1, р. 6, № 809щ

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С наредбата се определят системата от мерки, способности и средства за физическа сигурност на класифицираната информация, както и условията и редът за тяхното използване.

(2) Системата от мерки, способности и средства включва общи и конкретни мерки за физическа сигурност на класифицираната информация, оценка на заплахите за физическата сигурност на класифицираната информация - "анализ на риска", изискванията и стандартите за физическа сигурност на класифицираната информация.

Чл. 2. Системата от мерки за физическа сигурност е част от общите изисквания за сигурност по защита на класифицираната информация.

Чл. 3. (1) Способи за предотвратяване на заплахите за физическата сигурност са:

1. "анализ на риска" - оценка на заплахите за физическата сигурност на класифицираната информация;

2. план за осигуряване на физическата сигурност на класифицираната информация.

(2) Целта на способите по ал. 1 е създаването на ефективни методи за противодействие на заплахите за физическата сигурност на класифицираната информация чрез използване на защитни мерки.

Чл. 4. Средствата за физическа сигурност се сертифицират за всяко ниво на класификация за сигурност на класифицираната информация съобразно изискванията на наредбата и се определят в списък, утвърден от Държавната комисия по сигурността на информацията (ДКСИ).

Чл. 5. Ръководителите на организационните единици отговарят за прилагането и спазването на системата от мерки, способности и средства за физическа сигурност на класифицираната информация.

Чл. 6. (1) Изискванията на наредбата се отнасят до всички сгради, помещения и съоръжения, в които се създава, обработва, съхранява и предоставя класифицирана информация.

(2) 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.

Чл. 7. Разпоредбите на наредбата се прилагат и за чуждестранна класифицирана информация, предоставена от друга държава или международна организация, доколкото влязъл в сила международен договор, по който Република България е страна, не предвижда друго.

Глава втора

ВИДОВЕ МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Чл. 8. (1) Мерките за физическа сигурност на класифицираната информация са общи, конкретни и специални.

(2) Общите мерки за физическа сигурност са организационни и се изразяват в определяне и изграждане на зоните за сигурност.

(3) Конкретните мерки са физически и технически и включват:

1. определяне и изграждане на периметъра по чл. 15, ал. 1;
2. защитно осветление;
3. алармена система против проникване (АСПП);
4. контрол на физическия достъп;
5. защита срещу подслушване, осъществявано със или без технически средства;
6. защита срещу неправомерно визуално наблюдение, осъществявано със или без технически средства;
7. осъществяване на визуално наблюдение за защита на физическата сигурност на класифицираната информация със или без използване на технически средства минимум през 2 часа;
8. сили за реагиране;
9. пожарогасителна или пожароизвестителна система.

(4) За осигуряване физическата сигурност на класифицирана информация, съдържаща се в материални носители, които поради своето естество или размери не могат да бъдат пренасяни (транспортирани) по общия ред, предвиден в Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ), се прилагат специалните мерки, определени в глава шеста.

(5) Мерките за физическа сигурност имат за цел:

1. предотвратяване на нерегламентиран достъп или на опит за нерегламентиран достъп до класифицирана информация;
2. предотвратяване, пресичане и установяване на действия, които поставят под съмнение надеждността на служителите;
3. групиране на служителите съобразно издаденото им разрешение за достъп до класифицирана информация и в съответствие с принципа "необходимост да се знае";
4. своевременно установяване и противодействие при нарушаване или при опит за нарушаване на мерките за физическа сигурност.

Глава трета

ИЗГРАЖДАНЕ НА ЗОНИ ЗА СИГУРНОСТ

Чл. 9. (1) В изпълнение на чл. 74 от Закона за защита на класифицираната информация (ЗЗКИ) и с цел предотвратяване на нерегламентиран достъп до класифицирана информация 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.

(2) 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.

Чл. 10. (1) 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.

(2) Зоната по ал. 1 отговаря на следните 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.

Чл. 11. (1) 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.

(2) Зоната по ал. 1 отговаря на следните 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.

Чл. 12. (1) Информация с ниво на класификация "Строго секретно" се съхранява при наличието поне на едно от условията, предвидени в наредбата.

(2) За 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) непрекъснатата 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 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.

(3) 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" по ал. 1, или една от следните мерки:

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

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

а) непрекъснатата 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.

(4) 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.

(5) Информация с ниво на класификация "За служебно ползване" се съхранява в заключващи се канцеларски шкафове.

Чл. 13. Откритата зона по чл. 12, ал. 2, т. 2 се изгражда в съответствие със следните стандарти по отношение на:

1. конструкция - стените, подовите и таваните на периметъра на откритата зона трябва да бъдат с непрекъсната конструкция, да отговарят на изискванията на чл. 77, ал. 1 ЗЗКИ и материалите, от които се изграждат, да са сертифицирани по реда на чл. 77, ал. 3 ЗЗКИ;

2. врати - трябва да са направени от дърво, метал или друг стабилен материал и да са осигурени с брави, сертифицирани по реда на чл. 77, ал. 3 ЗЗКИ;

3. отдушници, тръби и други подобни отвори - всички отдушници, тръби и подобни отвори, които са с размери повече от 620 кв. см (и над 15 см в най-малките им размери), които излизат или минават през откритата зона за съхраняване, се защитават с решетки, спуснати метални прегради, заглушители срещу производствен шум или детекторна система;

4. прозорци:

а) прозорците, които могат да осигурят подходящо визуално наблюдение на дейности, свързани с класифицирана информация вътре в зоните за сигурност, се затъмняват или оборудват с транспаранти, завеси или с други подходящи покрития;

б) прозорците на приземните етажи или други леснодостъпни прозорци (например от покриви, веранди или пристроени сгради) се включват към АСПП и се изграждат от или се покриват с материали, които осигуряват защита срещу влизане с взлом; защитата на прозорците не е необходимо да бъде по-усилена, отколкото е здравината на съседните стени.

Чл. 14. (1) Ръководителите на организационните единици с помощта на служителите по сигурността на информацията могат:

1. да създават регистри за класифицирана информация само в зони за сигурност клас I или клас II, които отговарят на следните изисквания:

а) да са разположени в отделни помещения по възможност на средни етажи с изглед към вътрешни дворове или части на сграда;

б) да са осигурени метални решетки за вратите и прозорците;
в) в помещението да е изграден параван, обособяващ зона за лица потребители, и работна зона - за служителите в регистратурата;
г) да са оборудвани с АСПП, свързана с контролен център;

2. да определят около зоните за сигурност клас I и клас II административна зона, която отговаря на следните изисквания:

а) видимо определен периметър, позволяващ контрол на лица и транспортни средства;

б) осигурен пропускателен режим на входа и на изхода на периметъра по буква "а".

(2) В административната зона по ал. 1, т. 2 може да се създава, обработва, съхранява или предоставя единствено класифицирана информация с ниво на класификация "За служебно ползване".

Глава четвърта

КОНКРЕТНИ МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Чл. 15. (1) Периметърът представлява ясно обозначена външна граница на зоните за сигурност, които изискват защита.

(2) По периметъра се изграждат физически бариери, които могат да бъдат оборудвани и с технически средства, утвърдени в списъка по чл. 77, ал. 3 ЗЗКИ, възпрепятстващи нерегламентирания достъп.

(3) 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.

Чл. 16. (1) 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.

(2) Изискванията, на които следва да отговаря защитното осветление, се определят по реда на чл. 77, ал. 3 ЗЗКИ.

Чл. 17. (1) За повишаване нивото на защита на периметъра в зоните за сигурност се използват АСПП.

(2) Алармените системи против проникване сигнализират при опит за нерегламентиран достъп или осъществен такъв достъп и осигуряват необходимото време за реакция на силите за реагиране.

(3) Алармените системи против проникване се използват съгласно плана за физическа сигурност на обекта.

Чл. 18. (1) Контролът на физическия достъп се осъществява по отношение на обектите по чл. 6, ал. 1.

(2) Контролът по ал. 1 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.

(3) 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.

(4) Проверката по ал. 3 може да бъде заложена като задължително условие за влизане в дадена сграда или обект. В такъв случай се поставя известяващ проверката надпис.

(5) Проверката по ал. 3 се извършва чрез технически средства или чрез визуален оглед.

Чл. 19. (1) Служителите от звеното за сигурност и охрана прилагат системата от мерки за физическа сигурност на класифицираната информация с цел предотвратяване на нерегламентиран достъп до класифицирана информация в зоните за сигурност.

(2) Дейността на служителите от звеното за сигурност и охрана се регламентира с инструкция, утвърдена от ръководителя на организационната единица.

(3) 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.

(4) 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.

Чл. 20. (1) В зависимост от плана за физическа сигурност в организационната единица могат да се създават сили за реагиране.

(2) 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.

(3) 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.

Чл. 21. (1) 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.

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

Чл. 22. (1) 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.

(2) Контролният център по ал. 1 е специално оборудвано помещение в организационната единица, 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.

Глава пета

КОНТРОЛ НА КЛЮЧОВЕТЕ И ШИФРОВИТЕ КОМБИНАЦИИ НА ЗАЩИТЕНИТЕ КАСИ

(ШКАФОВЕ, СЕЙФОВЕ)

Чл. 23. (1) Защитените каси (шкафове, сейфове) се затварят задължително с ключове, а тези, които съхраняват информация с ниво на класификация "Строго секретно" - и с шифрови комбинации.

(2) Защитените каси (шкафове, сейфове) имат по два ключа, единият от които се използва постоянно, а другият е резервен.

(3) Забранява се изнасянето на ключове на защитените каси (шкафове, сейфове) извън зоните за сигурност, намиращи се в съответната организационна единица.

(4) Шифровите комбинации на защитените каси (шкафове, сейфове) се определят от служителя, на когото е зачислена съответната каса (шкаф, сейф).

(5) Служителят е длъжен да възпроизведе писмено шифровата комбинация и заедно с резервния ключ от защитената каса (шкаф, сейф) да ги предостави в запечатан плик на дежурната част, съответно на ръководителя на звеното за сигурност и охрана в организационната единица.

(6) Резервните ключове и шифровите комбинации по ал. 5 се използват само при бедствия и аварии.

(7) Ключовете, които се използват постоянно, и резервните ключове се съхраняват в отделни каси (шкафове, сейфове).

(8) Записът на всяка шифрова комбинация се съхранява в отделни пликове.

(9) Всички ключове, писмени шифрови комбинации и пликове се поставят под защита не по-ниска от защитата на класифицираната информация, към която те осигуряват достъп.

(10) Служителят, на когото е зачислена защитената каса (шкаф, сейф), е длъжен да възпроизвежда единствено по памет шифровата комбинация.

(11) Забранява се писменото възпроизвеждане на шифровата комбинация освен в случаите по ал. 5.

Чл. 24. (1) Право да знаят шифровите комбинации на защитените каси (шкафове, сейфове) имат служителите, на които те са зачислени, техните преки ръководители и ръководителят на организационната единица при спазване изискванията на ЗЗКИ за достъп до класифицирана информация.

(2) Шифровите комбинации се променят:

1. при първоначално използване;
2. в случай на смяна на някое от лицата по ал. 1;
3. в случай на нерегламентиран достъп или на опит за нерегламентиран достъп;
4. през период не по-дълъг от 12 месеца.

Глава шеста

СПЕЦИАЛНИ МЕРКИ ЗА ФИЗИЧЕСКА СИГУРНОСТ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ,

СЪДЪРЖАЩА СЕ В МАТЕРИАЛНИ НОСИТЕЛИ, КОИТО ПОРАДИ СВОЕТО ЕСТЕСТВО ИЛИ

РАЗМЕРИ НЕ МОГАТ ДА БЪДАТ ПРЕНАСЯНИ (ТРАНСПОРТИРАНИ) ПО ОБЩИЯ РЕД

Чл. 25. (1) Специалните мерки за физическа сигурност на класифицирана информация, съдържаща се в материални носители, които поради своето естество или размери не могат да бъдат пренасяни (транспортирани) по общия ред, предвиден в ППЗЗКИ, се определят в наредбата.

(2) Специалните мерки по ал. 1 включват:

1. подготвяне на материалния носител, съдържащ класифицирана информация с ниво на класификация "Поверително" и по-високо, за пренасяне (транспортиране);

2. поставяне на материални носители в контейнер или в друга твърда опаковка по начин, непозволяващ визуално определяне на неговата форма и предназначение;

3. надеждно запечатване на контейнерите или опаковките по начин, позволяващ откриването на следи от опит за нерегламентиран достъп до пренасяния (транспортирания) материален носител на класифицирана информация.

Чл. 26. (1) Преди транспортирането на материален носител на класифицирана информация ръководителят на организационната единица изпращач изготвя план за транспортирането му.

(2) Планът по ал. 1 се изработва след "анализ на риска" и включва:

1. определяне особеностите на материалния носител на класифицирана информация;

2. целта на физическата защита;

3. уведомяване на организационната единица - получател на материалния носител на класифицирана информация;

4. уведомяване на компетентната служба за сигурност;

5. определяне на вида транспорт в зависимост от особеностите на материалния носител (железопътен, автомобилен, воден или въздушен);

6. определяне на основен и резервен маршрут след предварително проучване на възможните маршрути, както и на мерки за осигуряване на охрана и периметър, непозволяващ нерегламентиран достъп до материалния носител на класифицирана информация;

7. определяне на времето за транспортиране;

8. посочване на конкретните мерки за физическа сигурност;

9. определяне на органите, отговорни за планирането и прилагането на мерките по т. 8;

10. контрол по изпълнението на плана.

(3) Материалните носители се пренасят по възможност заедно със съпътстващата ги техническа документация (паспорти, формуляри, чертежи и др.).

Чл. 27. (1) Мерките по чл. 25 гарантират физическата сигурност на пренасяния (транспортирания) материален носител на класифицирана информация във всички етапи на пренасянето (транспортiranето) или претоварването му от един вид транспорт на друг.

(2) Пренасянето (транспортiranето) на материалния носител, съдържащ класифицирана информация, се извършва по максимално кратък маршрут и по най-бързия възможен начин, доколкото позволяват обстоятелствата.

(3) Маршрут е пътят, по който се извършва пренасянето (транспортiranето) на материалния носител, съдържащ класифицирана информация.

(4) В зависимост от начина за осъществяване пренасянето (транспортiranето) се извършва:

1. етапно - чрез предаване на материалния носител на класифицирана информация между различни звена за сигурност и охрана по маршрута за предаване и транспортиране;

2. директно - когато материалните носители се пренасят (транспортират) от едно и също звено за сигурност и охрана от началото до крайния пункт, независимо от смяната на вида транспорт.

(5) Звената за сигурност и охрана могат да изпълняват и задачи за двупосочно (обратно) пренасяне (транспортиране).

Чл. 28. Служителите от звената за сигурност и охрана, охраняващи материалния носител, съдържащ класифицирана информация, при неговото пренасяне (транспортиране) следва да имат разрешение за достъп, съответстващо или по-високо от нивото на класификация на материалния носител, съдържащ класифицирана информация.

Чл. 29. Ръководителите на организационни единици, отговорни за пренасянето (транспортирането) на материални носители на класифицирана информация по смисъла на тази глава, приемат инструкция, регламентираща конкретните действия по изработването на плана по чл. 26.

Глава седма

АНАЛИЗ НА РИСКА

Чл. 30. (1) Способът "анализ на риска" е непрекъснат аналитично-информационен процес по събирането на данни и техния анализ и оценка от гледна точка на физическата защита на класифицираната информация.

(2) Анализът на риска цели установяване на всякаква заплаха или вреда в резултат на нерегламентиран достъп, опит за нерегламентиран достъп, терористична дейност или саботаж, както и влиянието и последиците при тяхното проявление.

Чл. 31. Анализът на риска се извършва въз основа на:

1. нивото на класификация на информацията;
2. обема на класифицираната информация и вида на нейните носители;
3. броя на издадените разрешения за достъп на служителите и нивата на класификация, за които те са издадени, при спазване на принципа "необходимост да се знае";
4. начина на съхраняване на информацията.

Чл. 32. Процесът по анализ на риска включва:

1. определяне на обекта по чл. 6, ал. 1, подложен на риск;
2. установяване степента на застрашеност и уязвимост на обекта от нерегламентиран достъп до класифицирана информация;
3. анализ на съществуващите мерки за физическа защита;
4. изграждане и усъвършенстване на системата от мерки за физическа защита;
5. определяне стойността на мерките по т. 4;
6. избор на вариант за осъществяване на физическа защита;
7. описание на остатъчната заплаха и нейното допустимо проявление;
8. периодични проверки, преразглеждане и преоценка.

Глава осма

ИЗГОТВЯНЕ НА ПЛАН ЗА ФИЗИЧЕСКА СИГУРНОСТ

Чл. 33. (1) В изпълнение на чл. 22, ал. 1, т. 3 ЗЗКИ служителят по сигурността на информацията след анализ на риска разработва план за физическа сигурност.

(2) Планът по ал. 1 отчита особеностите на обекта и включва:

1. целта на физическата защита;
2. конкретно посочване на всички параметри на обектите, които изискват физическа защита;
3. определяне на зоните за сигурност;
4. посочване на конкретните мерки за физическа сигурност;
5. органите, отговорни за планирането и прилагането на мерките по т. 4;

6. периодични проверки;
7. контрол по изпълнението на плана.

(3) Планът по ал. 1 се съставя при спазване на принципа "защита в дълбочина".

(4) Принципът "защита в дълбочина" представлява разполагане на силите и средствата за защита в зоните за сигурност и включва:

1. определяне на охраняваната територия и предотвратяване на нерегламентиран достъп до нея;
2. регистриране на нерегламентиран достъп или опит за такъв достъп и сигнализиране на силите за реагиране на съответната организационна единица;
3. забавяне и ограничаване на нарушителя до задържането му от компетентните органи; времето за реакция на силите за реагиране следва да бъде по-малко от времето, необходимо на нарушителя за преодоляване на мерките за физическа сигурност.

Глава девета

ФИЗИЧЕСКА ЗАЩИТА СРЕЩУ ПОДСЛУШВАНЕ И НАБЛЮДЕНИЕ

Чл. 34. (1) Зони клас I или клас II, в които се създава, обработва, съхранява или предоставя класифицирана информация с ниво на класификация "Поверително" или по-високо, се защитават срещу пасивни и активни опити за подслушване и наблюдение чрез мерки за физическа защита и контрол на физическия достъп в съответствие с оценката, получена при прилагането на способа "анализ на риска".

(2) Анализът на риска се извършва от служителя по сигурността на информацията съвместно с технически специалисти в областта на защитата срещу подслушване с технически средства.

(3) Пасивният опит за подслушване включва нерегламентиран достъп до класифицирана информация чрез незащитени комуникации, директно подслушване без специални средства или прихващане на електромагнитните излъчвания от комуникационните и информационните системи.

(4) Активният опит за подслушване включва нерегламентиран достъп до класифицирана информация чрез жични микрофони, радиомикрофони или други вградени устройства.

Чл. 35. Защитата срещу пасивен опит включва мерки, насочени към:

1. намаляване и изолиране на електромагнитните излъчвания;
2. криптиране на информацията;
3. звукоизолиране на помещенията в зони клас I или клас II, в които се създава, обработва, съхранява или предоставя класифицирана информация.

Чл. 36. (1) Защитата срещу активно подслушване включва техническа или физическа проверка за сигурност на конструкцията, мебелировката и инсталациите, офис оборудването, включително машини (механични и електрически), средства за комуникация и др.

(2) Проверката по ал. 1 е първоначална и периодична (най-малко веднъж на 6 месеца) и се извършва от сертифициран и оторизиран, обучен в областта на физическата сигурност персонал, и от технически специалисти в областта на защитата срещу подслушване с технически средства.

Чл. 37. (1) Физическата защита срещу наблюдение през светлата и тъмната част на денонощието включва изграждането на физически прегради, възпрепятстващи прякото наблюдение със или без технически средства.

(2) Физическите прегради могат да бъдат затъмнени стъкла, щори, пердета, паравани и др.

Глава десета

ОБОСОБЯВАНЕ НА ТЕХНИЧЕСКИ ОСИГУРЕНИ ЗОНИ

Чл. 38. (1) С цел осигуряване физическата защита на класифицираната информация с ниво на класификация "Поверително" и по-високо при срещи, разговори, съвещания, заседания и др., предмет на които е такава информация, се обособяват технически осигурени зони.

(2) В технически осигурените зони се прилагат всички мерки за физическа защита срещу подслушване и наблюдение.

(3) В технически осигурените зони могат да се прилагат и допълнителни мерки за сигурност.

Чл. 39. Допълнителните мерки по чл. 38, ал. 3 включват:

1. контрол на физическия достъп;
2. извършване на технически и физически проверки за наличие на средства за подслушване;
3. проверка за наличие на подслушвателни устройства в обзавеждането и оборудването или в части от тях преди внасянето им в зоната.

Чл. 40. Контролът на физическия достъп включва:

1. надеждна защита чрез технически и физически средства срещу нерегламентиран достъп;
2. регистриране на всички лица, пребивавали в зоната;
3. списък с вида, серийните и инвентарните номера на обзавеждането, оборудването или на части от тях, намиращи се в технически осигурената зона, внасяни или изнасяни от нея.

Чл. 41. (1) Проверките по чл. 39, т. 2 и 3 се извършват:

1. при първоначално използване;
2. преди и след провеждането на срещи, разговори, съвещания, заседания и др. с предмет класифицирана информация с ниво на класификация "Поверително" и по-високо;
3. при наличие на нерегламентиран достъп или при опит за нерегламентиран достъп;
4. периодично, но най-малко веднъж на 6 месеца;
5. след извършване на ремонтни и строително-монтажни дейности.

(2) За резултатите от всяка проверка се оформя протокол, включващ описание на проверените помещения и оборудване, използваната апаратура и получените резултати.

Чл. 42. (1) В технически осигурените зони се забраняват:

1. инсталирането и използването на комуникационни устройства; ако инсталацията им е крайно наложителна, се разрешава монтирането на безопасен жичен телефон;
2. носенето и използването на мобилни телефони или други електромагнитни устройства;
3. монтирането и използването на записваща и озвучаваща апаратура;
4. използването на електронноизчислителна техника, неотговаряща на изискванията за работа със съответното ниво на класификация и имаща връзка с апаратури и мрежи извън технически осигурената зона.

(2) В случай че инсталирането на телефон е крайно наложително, той следва да бъде снабден с устройство за положително прекъсване на телефонната връзка или да бъде физически прекъснат при провеждане на конфиденциален разговор в помещението, в което се намира телефонът.

Чл. 43. Около технически осигурената зона се установява наблюдение и се извършват периодични проверки за наличие на средства за подслушване и наблюдение.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Наредбата се приема на основание чл. 78 от Закона за защита на класифицираната информация.

§ 2. Изпълнението на наредбата се възлага на председателя на ДКСИ, на министъра на вътрешните работи, на министъра на отбраната, на ръководителите на службите за сигурност и службите за обществен ред, както и на ръководителите на организационни единици по чл. 20, ал. 1 във връзка с § 1, т. 3 от допълнителните разпоредби на ЗЗКИ.