НАРЕДБА за сигурността на комуникационните и информационните системи

Приета с ПМС № 28 от 24.02.2020 г., обн., ДВ, бр. 18 от 28.02.2020 г., в сила от 28.02.2020 г.

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С наредбата се определят задължителните общи условия за сигурност на комуникационните и информационните системи, наричани по-нататък "КИС", за осъществяване на една или няколко от функциите по създаване, обработване, ползване, съхраняване и обмен на класифицирана информация в електронна форма.

(2) Задължителните общи условия по ал. 1 включват:

1. органите по сигурността на КИС;

2. условията и реда за акредитиране на КИС;

3. задължителните общи изисквания за сигурност на КИС в областта на:

а) физическата сигурност;

б) персоналната сигурност;

в) документалната сигурност;

г) комуникационната сигурност;

д) криптографската сигурност;

е) контрамерките по TEMPEST;

ж) компютърната сигурност;

з) сигурност при свързване.

Глава втора
ОРГАНИ ПО СИГУРНОСТТА НА КИС

Раздел I
Държавна комисия по сигурността на информацията

Чл. 2. Държавната комисия по сигурността на информацията (ДКСИ) осъществява общ контрол:

1. по защита на класифицираната информация в КИС;

2. на процеса на акредитиране на КИС.

Раздел II
Орган по акредитиране на сигурността на КИС

Чл. 3. (1) Орган по акредитиране на сигурността на КИС (ОАС) по смисъла на наредбата е Специализирана дирекция "Информационна сигурност" на Държавна агенция "Национална сигурност".

(2) Органът по акредитиране на сигурността:

1. дава препоръки и указания по сигурността на КИС;

2. дава препоръки за стандарти и средства, които могат да се използват в КИС за защита на класифицирана информация;

3. утвърждава документите по сигурността на КИС;

4. извършва комплексна оценка на сигурността на КИС;

5. издава сертификати за сигурност на КИС;

6. определя условията, при които следва да се извърши допълнително или ново акредитиране на КИС;

7. координира и контролира дейностите по TEMPEST и определя контрамерките за защита на КИС от компрометиращи електромагнитни излъчвания;

8. провежда обучение на служители по сигурността на КИС и издава свидетелство по образец съгласно приложение № 4;

9. води регистър на сертифицираните КИС;

10. отнема и прекратява действието на сертификати за сигурност на КИС при условията, посочени в глава шеста, раздел V от Закона за защита на класифицираната информация (ЗЗКИ);

11. одобрява механизмите за защита на границата на КИС;

12. определя стандарти и списъци на одобрени продукти, които могат да се използват при избор на компоненти и устройства за защита на границата;

13. определя конкретните условия и етапи за акредитиране на всяка КИС.

(3) Указанията по ал. 2, т. 1 са задължителни.

Раздел III
Служител по сигурността на КИС

Чл. 4. (1) Ръководителят на организационната единица, в която се използват или се предвижда използване на КИС, по предложение на служителя по сигурността на информацията назначава в административното звено по сигурността служител по сигурността на КИС или възлага функции по чл. 5 на служител от същото звено, а при липса на такова звено – на служител от организационната единица. При необходимост може да бъдат определени повече от един служител по сигурността на КИС.

(2) Служителят по сигурността на КИС трябва да има разрешение за достъп до най-високото ниво на класифицирана информация в КИС в организационната единица.

(3) В органите на държавната власт, в които са обособени повече от една организационна единица, служителят по сигурността на КИС може да е от състава на друга организационна единица в рамките на съответния орган.

(4) Функции на служител по сигурността на КИС в случаите по ал. 3 се възлагат със заповед на съответния компетентен орган на държавната власт по предложение на ръководителя на организационната единица, в която ще се

изпълняват функциите на служител по сигурността на КИС, съгласувано с ръководителя на организационната единица, в състава на която е служителят.

(5) Задълженията на служителя по сигурността на КИС в случаите по ал. 3 се определят с акта по чл. 25, ал. 1.

(6) След назначаването или възлагането на функции служителят по сигурността на КИС задължително преминава обучение в ОАС в областта на защитата на класифицираната информация в КИС.

Чл. 5. Служителят по сигурността на КИС:

1. създава необходимата организация и осъществява контрол на сигурността на КИС в организационната единица;

2. координира изготвянето на документите по сигурността на КИС и на изработените на тяхна основа експлоатационни документи по сигурността;

3. съгласува изготвените документи по сигурността на КИС и ги предоставя на служителя по сигурността на информацията;

4. координира обучението по сигурността на КИС;

5. при случаи или съмнения за компрометиране на сигурността на КИС:

а) незабавно уведомява отговорните длъжностни лица по сигурността в ОЕ;

б) предприема действия за ограничаване или предотвратяване на вредите;

в) координира и участва в процеса по установяването и анализирането на обстоятелства, свързани с компрометиране сигурността на КИС;

г) докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОАС.

Раздел IV
Орган по развитие и експлоатация на КИС (ОРЕ)

Чл. 6. (1) Ръководителят на организационната единица определя със

заповед ръководител и състав на ОРЕ в организационната единица и възлага функции по чл. 6, ал. 2.

(2) Органът по развитие и експлоатация на КИС:

1. разработва и предлага изискванията за сигурност на КИС;

2. изготвя документите по сигурността за всяка КИС;

3. участва в подбора и тестването на техническите и програмните средства, и механизмите за сигурност, които ще се използват в КИС;

4. осигурява изпълнението на изискванията за акредитиране на КИС;

5. определя мерките за сигурност и границите на отговорност при осъществяване на връзки с други КИС;

6. прави предложение за възлагане функции на администратор по сигурността на всяка КИС;

7. организира обучение по сигурността в КИС и провежда обучение по сигурността на служителите, на които е възложена дейността по развитието, управлението или сигурността на КИС, включително администраторите по сигурността на КИС, както и на лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС;

8. организира прилагането на одобрените мерки за сигурност в КИС;

9. при междусистемна връзка на КИС извършва подбор на механизми за защита на границата;

10. прави преглед на свързаната със сигурността документация – периодично или при предложени промени в техническото или в програмното осигуряване, връзките с други КИС, режима за сигурност, нивото на класификация на информацията или при други дейности, които могат да повлияят на сигурността на КИС, като за резултатите информира служителя по сигурността на КИС;

11. участва заедно със служителя по сигурността на КИС в установяването и анализирането на обстоятелствата, свързани с

компрометиране сигурността на КИС.

(3) В една организационна единица може да има повече от един ОРЕ.

(4) В органите на държавната власт, в които са обособени повече от една организационна единица, може да бъде създаден един ОРЕ за няколко или за всички организационни единици.

(5) В случаите по ал. 4 ОРЕ се определя със заповед на съответния компетентен орган на държавната власт.

(6) В случаите, когато КИС обхваща повече от една организационна единица, ОРЕ може да се определи с акта по чл. 25, ал. 1.

Раздел V
Администратор по сигурността на КИС

Чл. 7. (1) За всяка КИС със заповед на ръководителя на организационната единица по предложение на ОРЕ съгласувано със служителя по сигурността на информацията се възлагат функции по чл. 9, ал. 1 на администратор по сигурността на КИС.

(2) В органите на държавната власт, в които са обособени повече от една организационна единица, администраторът по сигурността на КИС може да е от състава на друга организационна единица в рамките на съответния орган.

(3) Функции на администратор по сигурността на КИС в случаите по ал. 2 се възлагат със заповед на компетентния орган на държавната власт по предложение на ръководителя на организационната единица, в която ще се изпълняват функциите на администратор по сигурността на КИС, съгласувано с ръководителя на организационната единица, в състава на която е служителят.

(4) Задълженията на администратора по сигурността на КИС в случаите по ал. 3 се определят с акта по чл. 25, ал. 1.

Чл. 8. (1) Администраторът по сигурността на КИС е от състава на ОРЕ или от друго звено в организационната единица, имащо отношение към съответната КИС.

(2) При необходимост могат да се определят повече от един администратор по сигурността на КИС, отговарящи за обособени нейни части, като един от тях се определя за администратор по сигурността на цялата КИС.

(3) Задълженията на администратора по сигурността на КИС и на администратора на КИС трябва да са ясно разграничени, като не могат да се изпълняват от едно и също лице.

(4) Администраторът по сигурността на КИС трябва да има разрешение за достъп до най-високото ниво на класифицирана информация в КИС.

(5) Когато КИС обхваща няколко организационни единици, всяка от тях определя администратор по сигурността за нейната част. Администраторът по сигурността на цялата КИС се определя от организатора на КИС по чл. 25, ал. 1.

Чл. 9. (1) Администраторът по сигурността на съответната КИС:

1. участва в изготвянето и актуализирането на процедурите за сигурност на КИС;

2. изготвя експлоатационни документи по сигурността на КИС на базата на утвърдените процедури за сигурност;

3. изпълнява възложените му процедури за сигурност в КИС;

4. периодично информира потребителите по въпросите за сигурността на КИС;

5. предоставя на потребителите достъп до ресурсите на КИС в съответствие с определените им права;

6. осъществява пряк контрол по отношение на изпълнението на мерките и процедурите за сигурност в КИС, като:

а) следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на КИС;

б) следи за спазването на мерките и процедурите за сигурност при

инсталирането, конфигурирането, поддръжката и промените в КИС;

в) следи за правилното функциониране на механизмите за сигурност, включително на механизмите за защита на границата;

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата;

д) осигурява резервиране и съхраняване на одитните записи в определените срокове;

7. участва заедно със служителя по сигурността на КИС и с ОРЕ в установяването и анализирането на обстоятелствата, свързани с компрометиране на сигурността на КИС;

8. може да изпълнява функциите на администратор по криптографска сигурност на информацията, ако в КИС се прилагат криптографски методи и средства, одобрени и регистрирани по реда на наредбата по чл. 85 от ЗЗКИ;

9. уведомява служителя по сигурността на КИС за случаи или съмнения за компрометиране на сигурността на КИС;

10. провежда обучение по сигурността на конкретната КИС на администраторите на КИС и потребителите.

(2) Функциите по ал. 1 могат да бъдат разпределени между няколко администратори по сигурността на КИС.

Раздел VI
Администратор на КИС

Чл. 10. (1) Администратор на КИС е лице:

1. с възложени функции и предоставени права по системно, приложно, мрежово и/или друго администриране в съответната КИС;

2. което има издадено разрешение за достъп до най-високото ниво на класификация за сигурност на информацията в КИС;

3. което е преминало обучение в областта на сигурността на КИС.

(2) При необходимост функциите и правата по ал. 1, т. 1 могат да бъдат разпределени на повече от един администратор на КИС.

Чл. 11. (1) Администраторът на КИС изпълнява задълженията, посочени в експлоатационните документи по сигурността на КИС.

(2) Администраторът на КИС изпълнява указанията на администратора по сигурността на КИС, свързани със сигурността й.

(3) Администраторът на КИС уведомява администратора по сигурността на КИС за случаи или съмнения за компрометиране на сигурността й.

Раздел VII
Потребители в КИС

Чл. 12. Потребител в КИС е лице:

1. което има издадено разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която има право да работи в съответната КИС;

2. което е преминало обучение в областта на сигурността на КИС;

3. на което са предоставени права за достъп до ресурсите на КИС.

Чл. 13. (1) Потребителите в КИС изпълняват задълженията, посочени в експлоатационните документи по сигурността на КИС.

(2) Потребителите изпълняват указанията на администратора по сигурността на КИС, свързани със сигурността й.

(3) Потребителите уведомяват администратора по сигурността на КИС за случаи или съмнения за компрометиране на сигурността й.

Глава трета
АКРЕДИТИРАНЕ НА КИС

Раздел I
Условия и ред за акредитиране

Чл. 14. Процедурата по акредитиране на КИС започва от етапа на нейното проектиране. В периода на акредитирането ОРЕ взаимодейства с ОАС за уточняване на изискванията за сигурност към изгражданата КИС.

Чл. 15. (1) В етапа на проектиране на КИС ръководителят на организационната единица, наричан по-нататък "заявителя", подава до ОАС заявление за започване на процедура по акредитиране.

(2) Заявлението по ал. 1 се изготвя от ОРЕ и се съгласува със служителя по сигурността на информацията.

(3) В заявлението по ал. 1 се посочват:

1. общи сведения за КИС, които включват:

а) форма на представяне и ниво на класификация на информацията;

б) очакван брой и типове потребители и съответните специфични за системата нива на достъп;

в) средата, в която ще се експлоатира КИС;

г) информация за планирано използване на криптографски средства (тип криптографски средства и описание на предвижданата организация на тяхното използване);

2. общи сведения за връзки с други КИС и/или други системи, които включват:

а) наименования на свързаните КИС и/или други системи;

б) най-високото ниво на класификация на информацията в свързаните КИС;

в) за всяка връзка – посоката на обмен и нива на класификация на информацията, която ще се обменя;

г) предвиждани информационни услуги, които ще се предоставят или ползват при междусистемната връзка с всяка от системите;

д) предвиждани механизми за защита на границата;

3. ръководителят на ОРЕ и администраторът по сигурността на КИС;

4. етапите и сроковете за изграждане на КИС.

Чл. 16. (1) В срок до 15 работни дни ОАС взема решение за откриване на процедура по акредитиране и уведомява писмено заявителя.

(2) В уведомлението по ал. 1 се посочват срокове за предоставяне на документите по сигурността по чл. 32, съобразени с етапите и сроковете за изграждане на КИС, условията, редът и етапите за акредитиране.

Чл. 17. В съответствие с етапите за акредитиране по чл. 16, ал. 2 за извършване на комплексна оценка на сигурността на КИС заявителят предоставя на ОАС:

1. документите по сигурността съгласно чл. 32;

2. документи, удостоверяващи изпълнението на отделни мерки за сигурност;

3. сертификати за сигурност на отделни средства и подсистеми, ако има такива.

Чл. 18. (1) Органът по акредитиране на сигурността извършва комплексна оценка на сигурността, като:

1. проверява представените документи по чл. 17;

2. проверява изпълнението на предвидените мерки за сигурност;

3. изготвя протокол за резултатите от извършените проверки по т. 1 и 2.

(2) На основание чл. 90, ал. 3 от ЗЗКИ ОАС утвърждава документите по чл. 32.

(3) По предложение на ОЕ и с решение на ОАС утвърждаването на документите по ал. 2 може да предхожда проверките по ал. 1, т. 2.

(4) Проверките по ал. 1, т. 1 и 2 се извършват от комисия с председател – представител на ОАС, и членове – представители на ОАС, на организационната единица и при необходимост на организатора на КИС в случаите по чл. 25. При необходимост може да се привличат специалисти по видовете сигурност.

(5) Комплексната оценка по ал. 1 може да не включва проверки по ал. 1, т. 2 за КИС, предназначени за класифицирана информация с ниво "За служебно ползване".

(6) В случаите, когато проверките по ал. 1, т. 1 и 2 се извършват в периода на действие на валиден сертификат за сигурност на КИС, новите предвидени мерки за сигурност могат да бъдат реализирани от ОЕ преди изтичане на валидността на сертификата и след разрешение от ОАС.

(7) Комисията по ал. 4 се назначава със съвместна заповед на ръководителите на ОАС и на организационната единица. В органите на държавната власт, в които са обособени повече от една организационна единица, в случаите, когато КИС обхваща повече от една ОЕ, комисията по ал. 2 може да се назначи със заповед на ръководителя на ОАС и на съответния компетентен орган на държавната власт.

Чл. 19. В случай на установени несъответствия при проверките по чл. 18, ал. 1, т. 1 и 2 ОАС изисква от заявителя да ги отстрани.

Чл. 20. (1) При положителна комплексна оценка на сигурността ОАС издава сертификат за сигурност на КИС по чл. 14, т. 2 от ЗЗКИ съгласно приложение № 1.

(2) Сертификатът по ал. 1 може да се издава и за обособени части на КИС по реда на тази глава.

Чл. 21. Сертификатът съдържа:

1. идентификация на сертификата;

2. правното основание за издаването на сертификата;

3. идентификация на КИС;

4. идентификация на заявителя;

5. най-високото ниво на класификация за сигурност на информацията в КИС;

6. срок на валидност на сертификата:

а) "Строго секретно" – 3 години;

б) "Секретно" – 4 години;

в) "Поверително" – 5 години;

г) "За служебно ползване" – 6 години;

7. дата и място на издаването;

8. подпис и печат.

Чл. 22. (1) За резултатите от оценката по чл. 18 ОАС изготвя сертификационен отчет, който е неразделна част на сертификата.

(2) Сертификационният отчет съдържа:

1. общо описание на КИС;

2. заключения от комплексната оценка;

3. опис на документите за сигурност, представени при акредитирането;

4. видовете изменения на КИС, които изискват извършване на допълнително акредитиране;

5. условията, които изискват повторна оценка на контрамерките по TEMPEST.

(3) Сертификационният отчет по ал. 2 се класифицира по реда на ЗЗКИ и Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ).

Чл. 23. (1) В случай че за изпълнението на важни за държавата задачи е необходимо КИС или обособена нейна част да бъде въведена в експлоатация, преди да бъде завършен процесът на акредитиране, ОАС може да издаде сертификат за сигурност на КИС или обособената част за определен период, но не по-дълъг от една година.

(2) За издаване на сертификат по ал. 1 заявителят подава до ОАС искане, съдържащо:

1. подробна информация за важните за държавата задачи, които ще бъдат изпълнявани;

2. ниво на класификация на информацията в КИС за периода на действие на сертификата по ал. 1;

3. периода, за който да бъде издаден сертификатът.

(3) След получаването на искането по ал. 2 ОАС изпраща на ОЕ задължителни общи изисквания за сигурност на КИС.

(4) Ръководителят на ОЕ определя комисия за извършване на проверка за изпълнението на изискванията за сигурност по ал. 3 и уведомява ОАС за резултатите от проверката.

Чл. 24. (1) Органът по акредитиране на сигурността извършва комплексна оценка на сигурността, като проверява представените от организационната единица документи с резултатите от извършената проверка по чл. 23, ал. 4.

(2) Предоставянето на информация от ОЕ за изпълнение на изискванията по чл. 23, ал. 3 в пълен обем е задължително условие за положителна комплексна оценка.

(3) Сертификатът по чл. 23, ал. 1 се издава след:

1. положителна комплексна оценка;

2. съгласуване от ДКСИ.

(4) Сертификатът по чл. 23, ал. 1 съдържа:

1. ниво на класификация на информацията в КИС за периода на действие на сертификата;

2. задължителните условия за сигурност, които трябва да се спазват при експлоатацията на КИС в периода на действие на сертификата;

3. условия за окончателно акредитиране на КИС;

4. срок на валидност на сертификата.

Чл. 25. (1) Когато КИС обхваща повече от една организационна единица, между тях се сключва споразумение, определящо коя организационна единица е организатор на КИС, границата на КИС и разпределението на отговорностите за съставните части на КИС, както и процеса на акредитиране. В органите на държавната власт, в които са обособени повече от една организационна единица, вместо споразумение може да се издаде заповед на компетентния орган на държавна власт.

(2) Организаторът на КИС по ал. 1 координира дейностите по: изграждането на системата за сигурност на КИС; цялостното акредитиране на КИС; прилагането и контрола за изпълнението на мерките за сигурност в периодите на експлоатация и снемане от експлоатация на КИС.

(3) Споразумението или заповедта по ал. 1 се прилага към заявлението по чл. 15 от организатора на КИС.

(4) Всяка организационна единица осигурява изпълнението на изискванията за акредитирането на частта от КИС, която е в нейна отговорност по споразумението или заповедта по ал. 1.

(5) Организационните единици по Наредбата за дейността по организирането и осъществяването на електронните комуникации и криптографската сигурност на служебната кореспонденция, обменяна по електронни комуникационни канали между организационните единици в Република България и задграничните й представителства, не сключват споразумение по ал. 1.

Чл. 26. За всяка КИС в процедура по акредитиране ОАС поддържа

акредитационно дело, което съдържа:

1. преписката по акредитирането и допълнителните акредитирания;

2. екземпляр на сертификата по чл. 20 и сертификационния отчет по чл. 22;

3. отчетите за допълнителните акредитирания по чл. 31, ал. 1, т. 3;

4. екземпляр на документите по сигурността по чл. 32.

Чл. 27. (1) Органът по акредитиране на сигурността води регистър на сертифицираните КИС. За всяка сертифицирана КИС в регистъра се вписват:

1. данните от сертификата;

2. регистрационните номера на заявленията по чл. 15 и 28;

3. регистрационните номера на документите по сигурността, представени при акредитирането и при допълнителните акредитирания;

4. регистрационните номера на сертификационния отчет по чл. 22 и допълнителните отчети по чл. 31, ал. 1, т. 3;

5. регистрационните номера на документите, съдържащи изменения на специфичните изисквания за сигурност и процедурите за сигурност, утвърдени от ОАС;

6. наличие на междусистемни връзки.

(2) Данни от регистъра се предоставят в срок до 15 работни дни по писмено искане на ДКСИ.

Раздел II

Условия и ред за допълнително акредитиране

Чл. 28. (1) При необходимост от изменения в КИС, попадащи в обхвата на чл. 22, ал. 2, т. 4, ръководителят на съответната организационна единица подава до ОАС заявление за допълнително акредитиране.

(2) Заявлението по ал. 1 се изготвя от ОРЕ и се съгласува със служителя по сигурността на информацията.

(3) В заявлението по ал. 1 се посочват:

1. общо описание на измененията, които налагат допълнителното акредитиране;

2. очаквано влияние на промените върху сигурността на КИС;

3. етапите и сроковете за извършване на промените;

4. информацията по чл. 15, ал. 3, т. 2, когато промените са свързани с изграждане на междусистемна връзка.

Чл. 29. (1) В срок до 15 работни дни ОАС взема решение за откриване на процедура за допълнително акредитиране и уведомява писмено заявителя.

(2) В уведомлението по ал. 1 се посочват условията, редът и етапите за допълнително акредитиране.

Чл. 30. В съответствие с определения от ОАС ред и етапите за допълнително акредитиране, за извършване на оценка на измененията и влиянието им върху сигурността на КИС заявителят представя на ОАС:

1. измененията в специфичните изисквания за сигурност и процедурите за сигурност на КИС;

2. сертификати за сигурност на отделни механизми, средства и подсистеми, свързани с промените, ако има такива.

Чл. 31. (1) Органът по акредитиране на сигурността на КИС:

1. прави проверка на изпълнението на мерките за сигурност, свързани с промените в специфичните изисквания за сигурност и в процедурите за сигурност;

2. утвърждава промените в специфичните изисквания за сигурност и в процедурите за сигурност;

3. изготвя отчет за допълнителното акредитиране.

(2) Проверките по ал. 1, т. 1 се извършват от комисия, назначена по реда на чл. 18.

(3) Освен в случаите, когато промяната е свързана с осъществяването на междусистемна връзка, проверките по ал. 1, т. 1 може да не бъдат извършвани за КИС, предназначена за класифицирана информация с ниво "За служебно ползване".

(4) Отчетът по ал. 1, т. 3 е неразделна част от сертификата и съдържа:

1. общо описание на промените;

2. основни изводи от оценката на сигурността и проверката на изпълнението на мерките за сигурност в КИС;

3. изменения в условията за допълнително акредитиране, ако има такива.

Глава четвърта
ДОКУМЕНТИ ПО СИГУРНОСТТА, НЕОБХОДИМИ ЗА АКРЕДИТИРАНЕ

Раздел I
Видове документи

Чл. 32. (1) Документи по сигурността, необходими за извършване на акредитирането на всяка КИС, са:

1. специфични изисквания за сигурност (СИС);

2. процедури за сигурност, изготвени на основата на СИС.

(2) За случаите по чл. 20, ал. 2 ОАС може да изиска допълнителни СИС и/или процедури за сигурност за обособените части на КИС.

(3) Документите по сигурността по ал. 1 и 2 се класифицират по реда на ЗЗКИ и ППЗЗКИ.

Раздел II
Специфични изисквания за сигурност

Чл. 33. (1) За всяка КИС се изготвят СИС съгласно чл. 90, ал. 3 и 4 от ЗЗКИ.

(2) Специфичните изисквания за сигурност се формулират по време на най-ранния стадий от проектирането на КИС и се детайлизират и развиват в процеса на разработване и изпълнение на проекта.

(3) В процеса на детайлизиране на изискванията за сигурност ОРЕ взаимодейства с ОАС за постигане на съгласие относно прилаганите мерки за сигурност за осигуряване на необходимото ниво на защита на КИС.

(4) Специфичните изисквания за сигурност в завършен вид представляват описание на КИС и приложените мерки за сигурност и съдържат следните раздели:

1. описание на конкретната КИС;

2. описание на глобалната, локалната и електронната среда за сигурност на КИС;

3. анализ на риска за сигурността на КИС;

4. мерките за сигурност относно:

а) контрол на достъпа;

б) идентификация и автентификация;

в) отчетност и одит;

г) интегритет на информацията;

д) достъпност на информацията;

е) комуникационна сигурност;

ж) контрамерки по TEMPEST;

5. управление на сигурността при експлоатацията на КИС;

6. мерките за сигурност при критични ситуации;

7. мерките за сигурност при прекратяване на експлоатацията на КИС, обособена част от КИС или междусистемна връзка.

Чл. 34. Анализът на риска за сигурността на конкретната КИС е процес на идентифициране на рисковете, оценяване на всеки от тях, определяне на необходимите допълнителни мерки за сигурност, оценка на остатъчния риск и последващо управление на риска.

Чл. 35. (1) Идентифицирането на рисковете включва установяване на заплахите и уязвимите места при конкретната реализация и ресурси на КИС.

(2) Оценяването на всеки риск включва определяне на вероятността за осъществяване на съответната заплаха при приложените мерки за сигурност и на последствията от успешното реализиране на заплахата. Оценяването на рисковете цели определяне на необходимите допълнителни мерки за сигурност, които да се приложат в КИС за достигане на приемлив резултат от анализа на всеки конкретен риск.

(3) Остатъчен риск е рискът, който остава след прилагане на мерките за сигурност, отчитайки, че не всички рискове могат да бъдат елиминирани.

(4) Управлението на риска е непрекъснат процес на извършване на анализ на риска през целия жизнен цикъл с цел осигуряване на конфиденциалност, достъпност и интегритет на информацията в КИС.

Чл. 36. Анализ на риска се извършва от екип от специалисти по видовете сигурност по чл. 1, ал. 2, т. 3, като могат да се привличат и представители на проектантите.

Чл. 37. Възможните резултати от анализа на всеки конкретен риск са:

1. елиминиране на риска – цялостно елиминиране на реална или потенциална уязвимост на конкретната КИС чрез пълно прилагане на мерки за сигурност;

2. предотвратяване загубата на физически и/или информационни ресурси – прилагане на мерки за предотвратяване на загубите, доколкото това е

възможно, отчитайки, че някои рискове не могат да бъдат елиминирани поради технологични или други причини;

3. ограничаване загубата на физически и/или информационни ресурси – прилагане на мерки за сигурност, ограничаващи загубите до приемливо ниво;

4. приемане на риска от загуба на физичес- ки и/или информационни ресурси – когато загубата не е голяма, вероятността за загуба е малка или цената на необходимите мерки за предотвратяване на загубите е много голяма.

Чл. 38. (1) Документирането на анализа на риска се извършва в документа по чл. 32, ал. 1, т. 1.

(2) Степента на детайлизация на документирането по ал. 1 се уточнява съгласно чл. 33, ал. 3 и включва минимум:

1. описание на приложената методология за извършване на анализа на риска;

2. оценката и резултатите от анализа на всеки идентифициран риск.

Чл. 39. Във всички етапи на жизнения цикъл на КИС СИС следва да се изготвят и изменят на основата на извършения анализ на риска.

Раздел III
Процедури за сигурност на КИС

Чл. 40. Процедурите за сигурност са подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на мерките за сигурност от СИС.

Чл. 41. (1) Процедурите за сигурност съдържат следните раздели:

1. организация на сигурността;

2. персонална сигурност;

3. физическа сигурност;

4. документална сигурност;

5. компютърна сигурност (включително при осигуряване със средства на КИС и управление на конфигурацията);

6. комуникационна сигурност;

7. контрамерки по TEMPEST;

8. действия при критични по отношение на сигурността ситуации.

(2) При междусистемна връзка процедурите за сигурност на всяка КИС трябва да определят ред и отговорност за обмена на информация, свързана с инцидент със сигурността на КИС.

(3) Конкретните параметри на информацията по ал. 2 и формата на обмен се определят в споразумението или в заповедта по чл. 25.

Глава пета
ОБЩИ ИЗИСКВАНИЯ ЗА СИГУРНОСТ НА КИС

Раздел I
Сигурност на КИС

Чл. 42. (1) Сигурността на КИС включва прилагане на балансирана система от мерки за сигурност в областите по чл. 1, ал. 2, т. 3.

(2) С прилагането на системата от мерки за сигурност се цели осигуряване на конфиденциалност, интегритет и достъпност на информацията в КИС.

Раздел II
Физическа сигурност

Чл. 43. (1) Зоните, в които се разполагат ресурсите на КИС, предназначени за класифицирана информация с ниво "Поверително" и по-високо, трябва да са определени като зони за сигурност съгласно наредбата по чл. 78 от ЗЗКИ.

(2) Зоните, в които се разполагат ресурсите на КИС, предназначени за

класифицирана информация с ниво само "За служебно ползване", с изключение на случаите по ал. 3, трябва да са определени като зони за сигурност или административни зони съгласно наредбата по чл. 78 от ЗЗКИ.

(3) Зоните, в които се разполага критично от гледна точка на сигурността оборудване на КИС, трябва да са определени като зони за сигурност съгласно наредбата по чл. 78 от ЗЗКИ.

(4) Зоните по ал. 1 и 2 се защитават със съответни на най-високото ниво на класификация на информацията в КИС мерки, способи и средства за физическа сигурност, определени в наредбата по чл. 78 от ЗЗКИ, с цел недопускане на нерегламентиран достъп.

Чл. 44. За критичните от гледна точка на сигурността места, определени от анализа на риска, се вземат допълнителни мерки за защита, като:

1. контрол на достъпа, включително с технически средства;

2. системи за наблюдение;

3. недопускане присъствието само на един служител в тях.

Раздел III
Персонална сигурност

Чл. 45. (1) Потребителите на КИС трябва да имат разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която имат право да работят в КИС.

(2) Служителите, на които е възложена дейността по развитието, управлението или сигурността на КИС, както и лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС, трябва да имат разрешение за достъп до най-високото ниво на класификация на информацията в КИС.

Чл. 46. (1) Всички лица по чл. 45 преминават обучение по сигурността на конкретната КИС.

(2) Обучението по ал. 1 се организира от ОРЕ и се провежда:

1. от ОРЕ за служителите, на които е възложена отговорността за развитието, управлението или сигурността на КИС, администраторите по сигурността на КИС, както и за лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС;

2. от ОРЕ или администраторите по сигурността на КИС – за администраторите на КИС и потребителите.

(3) При успешно завършило обучение лицата по ал. 1 се допускат до работа в конкретната КИС.

Чл. 47. Правомощията на лицата по чл. 45, ал. 2 се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на конкретната КИС.

Раздел IV
Документална сигурност

Чл. 48. (1) Всички документи в КИС, съдържащи класифицирана информация, се идентифицират, маркират и контролират.

(2) Маркировката на документите по ал. 1 трябва винаги да осигурява еднозначна информация за нивото на класификация при работа с тях.

(3) Начините за идентифициране, маркиране и контролиране по ал. 1 се определят в документите по сигурността на конкретната КИС.

(4) Документите по ал. 1 не се регистрират в регистратурата по чл. 51, ал. 1 от ППЗЗКИ.

Чл. 49. Извеждането на документи, съдържащи класифицирана информация от сертифицирани КИС, се извършва:

1. в съответствие с изискванията на чл. 137 от ППЗЗКИ;

2. в зоните по чл. 43, ал. 1 и 2.

Чл. 50. Пренос на документи, съдържащи класифицирана информация, от една КИС към друга се извършва само ако приемащата КИС е сертифицирана за ниво на класификация на информацията, същото или по-високо от нивото

на класификация на пренасяните документи.

Чл. 51. (1) Материални носители за многократен запис на класифицирана информация, използвани в КИС, се маркират, регистрират се в регистратурата по чл. 51, ал. 1 от ППЗЗКИ и се съхраняват по начин, съответстващ на нивото на класификация на носителя.

(2) Регистрирането, маркирането, контролът и унищожаването на материалните носители за многократен запис на класифицирана информация се извършват по реда на глава пета, раздел XII от ППЗЗКИ.

(3) Съхраняването и периодичният контрол на носителите по чл. 51, ал. 2 се извършват в съответствие с утвърдените процедури за сигурност на КИС.

Чл. 52. Материалите и записаната на хартиен носител информация (пароли, пин, кодове и др.), осигуряващи достъп до КИС или ресурси на КИС, се класифицират с ниво на класификация за сигурност на информацията, съответстващо на най-високото ниво на класификация на информацията, за която дават достъп в КИС, и се унищожават по ред, определен в документите по сигурността на конкретната КИС, а не по реда на ППЗЗКИ.

Чл. 53. (1) Преносими компютърни устройства, предназначени за класифицирана информация, се маркират като носители на такава информация и се разглеждат като КИС или част от КИС.

(2) Пренасянето на устройствата по ал. 1 извън зоните за сигурност се извършва по реда на ППЗЗКИ.

Раздел V

Комуникационна и криптографска сигурност, контрамерки по TEMPEST

Чл. 54. (1) Комуникационната сигурност представлява система от мерки за сигурност, прилагани с цел защита на класифицираната информация от нерегламентиран достъп при нейното пренасяне по комуникационни системи.

(2) Системата от мерки по ал. 1 включва защита с криптографски методи и средства, контрамерки по TEMPEST и защита при пренасяне на информацията в рамките на зоните за сигурност.

Чл. 55. (1) Комуникационните средства, организирани за пренос на

класифицирана информация, включително при междусистемна връзка, трябва да осигуряват механизми за:

1. надеждна и защитена идентификация и автентификация на изпращача и на получателя на информацията, които да се извършват преди началото на преноса на информацията;

2. осигуряване на конфиденциалност, интегритет и достъпност на пренасяната информация;

3. потвърждаване получаването на информацията.

(2) Комуникационните средства по ал. 1 се разполагат в зони за сигурност съгласно наредбата по чл. 78 от ЗЗКИ.

Чл. 56. В КИС не се допуска безжичен пренос на класифицирана информация, освен в случаите, когато е защитена с одобрени по реда на наредбата по чл. 85 от ЗЗКИ криптографски средства.

Чл. 57. За защита на класифицирана информация в КИС се прилагат само криптографски средства, одобрени по реда на наредбата по чл. 85 от ЗЗКИ.

Чл. 58. (1) Класифицирана информация от КИС се пренася по комуникационни системи извън зоните за сигурност или административни зони, когато е защитена с одобрени по реда на наредбата по чл. 85 от ЗЗКИ криптографски средства.

(2) Допуска се средата за разпространение на сигнала от КИС, предназначени за класифицирана информация с ниво "Поверително" и "Секретно", да бъде разположена в административна зона при прилагане на чл. 74.

(3) Форма на информация, получена чрез обработка на класифицирана информация с одобрени криптографски средства, не представлява класифицирана информация по смисъла на ЗЗКИ.

Чл. 59. (1) Комуникационните и информационните системи, предназначени за класифицирана информация с ниво "Поверително" и по-високо, трябва да са осигурени с контрамерки по TEMPEST.

(2) Контрамерките по TEMPEST съответстват на най-високото ниво на класификация на информацията в КИС.

(3) Контрамерките по TEMPEST включват:

1. определяне на защитеността на работните помещения и съоръжения, в които ще се разполага техническо оборудване на КИС, по отношение на затихването на електромагнитните вълни;

2. изпълнение на изискванията към техническото оборудване на КИС по отношение на максимално допустимите нива на компрометиращи електромагнитни излъчвания;

3. изпълнение на изискванията при разполагане, инсталиране и захранване на КИС;

4. допълнителни мерки съобразно спецификата на конкретната КИС.

Раздел VI
Минимални изисквания за компютърна сигурност

Чл. 60. Компютърната сигурност представлява система от мерки за сигурност, прилагани с цел осигуряване на конфиденциалност, интегритет и достъпност на класифицираната информация в КИС. Тези мерки за сигурност се реализират чрез възможностите на техническите и програмните средства на компютърните системи и на специализирани средства.

Чл. 61. (1) Минималните изисквания за компютърна сигурност на КИС включват:

1. еднозначна идентификация и автентификация на потребителя, които трябва да предхождат всички останали негови действия в КИС;

2. контрол на достъпа по преценка – предоставяне на права за достъп до обектите на КИС на базата на идентификацията на потребителя или неговата принадлежност към потребителска група; правата за достъп се предоставят само от администратора по сигурността на конкретната КИС или от упълномощени потребители; механизмите за контрол трябва да осигуряват възможност за разделяне на потребителите и за достъп до информацията според принципа "необходимост да се знае";

3. непрекъснат и синхронизиран по време запис на събития, свързани със сигурността на конкретната КИС (одитни записи); записват се действия, свързани с контрола на достъпа (включително неуспешни опити за достъп), действия по отношение на обекти и действия на оторизирани субекти, влияещи върху сигурността; информацията в одитните записи трябва да осигурява възможност за установяване на действия на отделните субекти, свързани със сигурността на КИС;

4. защита на одитните записи, свързани със сигурността, срещу неоторизиран преглед, промяна и изтриване;

5. обработка на обекти на конкретната КИС, така че при следващото им разпределяне към субект той да не може да установи предишното им съдържание или да получи права за достъп на използвалите ги преди това субекти;

6. актуална защита от вредни програмни средства.

(2) За осигуряване на минималните изисквания за сигурност се реализират програмни и технически механизми, спрямо които трябва да се осъществява конфигурационен контрол и които трябва да са защитени от нерегламентиран достъп.

Раздел VII
Режими за сигурност

Чл. 62. Комуникационните и информационните системи се експлоатират в един или в няколко от следните режими за сигурност:

1. "С общ достъп";

2. "С общо ниво";

3. "С много нива".

Чл. 63. (1) При работа на КИС в режим за сигурност "С общ достъп":

1. всички потребители имат разрешение за достъп до най-високото ниво на класификация на информацията в КИС;

2. всички потребители са упълномощени да работят с цялата класифицирана информация.

(2) Компютърната сигурност за КИС по ал. 1 се осигурява с минималните изисквания за компютърна сигурност, като правата за достъп до обектите се предоставят само от администратора по сигурността на конкретната КИС.

(3) При работа на КИС в режим за сигурност "С общ достъп" цялата информация в конкретната КИС се защитава като информация с най-високо ниво на класификация, освен ако е налице гарантиран механизъм за разпознаване нивото на класификация на информацията.

Чл. 64. (1) При работа на КИС в режим за сигурност "С общо ниво":

1. всички потребители имат разрешение за достъп до най-високото ниво на класификация на информацията в КИС;

2. достъпът на потребителите до класифицирана информация, за която те имат разрешение, се осъществява съгласно принципа "необходимост да се знае".

(2) Компютърната сигурност за КИС по ал. 1 се осигурява с минималните изисквания за компютърна сигурност.

(3) При работа на КИС в режим за сигурност "С общо ниво" цялата информация в конкретната КИС се защитава като информация с най-високо ниво на класификация, освен ако е налице гарантиран механизъм за разпознаване нивото на класификация на информацията.

Чл. 65. (1) При работа на КИС в режим за сигурност "С много нива":

1. не всички потребители имат разрешение за достъп до класифицирана информация с най-високо ниво на класификация;

2. достъпът на потребителите до класифицирана информация, за която те имат разрешение, се осъществява съгласно принципа "необходимост да се знае".

(2) Компютърната сигурност за КИС по ал. 1 се осигурява с минималните

изисквания за компютърна сигурност и прилагане на задължителен контрол на достъп на субектите до обектите на конкретната КИС.

(3) Задължителният контрол на достъпа по ал. 2 трябва да осигурява:

1. присвояване на атрибут за сигурност на всеки субект и обект на конкретната КИС; сравняването на атрибутите за сигурност на субектите с атрибутите за сигурност на обектите е основа за решения при осигуряване на достъпа;

2. изключително упълномощаване на администратора по сигурността на конкретната КИС за присвояване и изменяне на атрибутите за сигурност на субектите на конкретната КИС по реда, установен в документите по сигурността на конкретната КИС;

3. упълномощаване на определени потребители да присвояват атрибути за сигурност на входящи обекти, ако те не са притежавали такива атрибути;

4. способност да се обозначи класификационното ниво на изходящия от конкретната КИС обект на базата на неговия атрибут за сигурност;

5. разпределяне на предварително дефинирани стойности на атрибутите за сигурност на новосъздадени обекти и съхраняване на атрибутите за сигурност при копиране на обекти;

6. защита на интегритета на атрибутите за сигурност.

Раздел VIII

Сигурност по време на експлоатацията и развитието на сертифицирани КИС

Чл. 66. (1) Експлоатацията и развитието на сертифицирана КИС се извършват в пълно съответствие с установените мерки и процедури за сигурност и при съблюдаване на условията за нейното допълнително акредитиране.

(2) Органът по развитие и експлоатация на КИС, служителят и администраторът по сигурността на конкретната КИС в рамките на своите отговорности контролират и оценяват всички промени в глобалната, локалната и електронната среда за сигурност на конкретната КИС и предлагат изменение на мерките и процедурите за сигурност.

(3) Когато промените по ал. 2 налагат изменение на СИС и/или процедурите за сигурност, променените СИС и/или процедури за сигурност, както и описанието на промените по ал. 2 се представят на ОАС, който утвърждава променените СИС и/или процедури за сигурност или прави мотивиран отказ. Промените по ал. 2 не се извършват преди утвърждаването.

(4) Когато промените по ал. 2 налагат допълнително акредитиране за сигурност на конкретната КИС, се започва процедура по реда на глава трета, раздел II.

(5) Най-малко 6 месеца преди изтичане срока на валидност на издадения сертификат за сигурност на конкретната КИС в случаите, когато е необходимо да се продължи експлоатирането й, заявителят подава до ОАС заявление за ново акредитиране по реда на глава трета, раздел I.

(6) В случаите по ал. 5, когато не са настъпили промени на мерките за сигурност в глобалната, локалната или електронната среда за сигурност на конкретната КИС, проверката по чл. 18, ал. 1, т. 2 може да не бъде извършвана.

Чл. 67. По време на експлоатацията и развитието на КИС:

1. се извършва проверка на материални носители за многократен запис на класифицирана информация за наличието на вредни програмни средства, преди те да бъдат използвани в КИС;

2. се извършва резервиране на системната и одитната информация, както и на класифицираната информация, ако тя е необходима и не се съхранява на друг носител; резервните копия се съхраняват по начин, недопускащ нерегламентиран достъп до тях;

3. се извършва инсталиране на одобрени елементи и конфигуриране на КИС само от оторизирани служители на организационната единица или от доставчика на КИС под контрола на администратора по сигурността;

4. се извършва внедряване на технически и програмни средства или на техни версии само след проверка и тестване за сигурност; внедряването се извършва след одобрение от ОРЕ и от ОАС, когато е необходимо допълнително акредитиране на КИС;

5. се организира и извършва сервизна дейност по начин, недопускащ компрометиране сигурността на КИС;

6. се извършва ремонт на криптографски средства по реда на наредбата по чл. 85 от ЗЗКИ;

7. се извършва повторна оценка на контрамерките по TEMPEST в случаите по чл. 22, ал. 2, т. 5;

8. не се допуска използване на носители на информация, технически и програмни средства, които са лична собственост.

Раздел IX

Сигурност на КИС, предназначени за класифицирана информация с ниво "Строго секретно"

Чл. 68. Класифицирана информация с ниво на класификация "Строго секретно" се създава, обработва, съхранява и пренася в КИС, изградени в зона за сигурност, която е защитена от компрометиращи електромагнитни излъчвания.

Чл. 69. Класифицирана информация с ниво на класификация "Строго секретно" не се пренася по комуникационни системи извън зоните по чл. 68.

Чл. 70. Класифицирана информация с класификационно ниво "Строго секретно" не се обработва с преносими компютърни устройства.

Чл. 71. Комуникационните и информационните системи, в които се създава, обработва, съхранява или пренася информация с ниво на класификация "Строго секретно", работят в експлоатационен режим за сигурност "С общо ниво".

Чл. 72. Не се допуска междусистемна връзка на КИС, предназначени за класифицирана информация с ниво "Строго секретно".

Чл. 73. (1) Материални носители за многократен запис на класифицирана информация, използвани за съхраняване на информация с ниво на класификация "Строго секретно", се водят в отделен регистър.

(2) Материалните носители за многократен запис на класифицирана информация с ниво на класификация "Строго секретно" не се ремонтират и не подлежат на понижаване или премахване на нивото им на класификация, а се унищожават по реда на чл. 141 от ППЗЗКИ.

Раздел X
Възможност за заместване на мерките за компютърна и комуникационна сигурност

Чл. 74. (1) В случай на прекомерни разходи или при наличие на технологична невъзможност за осъществяване на някои мерки за компютърна сигурност и/или комуникационна сигурност те могат да се заместят с мерки от другите видове сигурност на КИС след съгласуване с ОАС.

(2) Заместващите мерки се предоставят на ОАС от заявителя за утвърждаване като неразделна част от СИС след направен анализ на риска в рамките на процедурите по акредитиране или допълнително акредитиране.

(3) В случаите по ал. 1 се спазват следните принципи:

1. заместваната мярка за сигурност трябва да се реализира напълно;

2. качеството и нивото на заместваната мярка за сигурност трябва да бъдат запазени.

Глава шеста
СИГУРНОСТ ПРИ СВЪРЗВАНЕ НА КИС

Раздел I
Общи изисквания при свързване на КИС

Чл. 75. (1) Сигурност при свързване на КИС представлява система от мерки за защита от нерегламентиран достъп до класифицираната информация при осъществяване на междусистемна връзка с други системи.

(2) Други системи по ал. 1 могат да бъдат:

1. комуникационните и информационните системи, сертифицирани за работа с класифицирана информация със същото или с различно ниво на класификация на информацията;

2. информационни системи от затворен тип;

3. системи с публичен достъп, като интернет и други подобни.

Чл. 76. (1) Ръководителите на организационните единици вземат решение за необходимостта от осъществяване на междусистемна връзка.

(2) Решението по ал. 1 трябва да бъде взето след отчитане на специфичните рискове за сигурността на системата, произтичащи от междусистемната връзка.

Чл. 77. (1) За всяка междусистемна връзка на КИС с други системи, между ръководителите на организационни единици, в чиято отговорност са системите, се сключва споразумение.

(2) В органите на държавната власт, в които са обособени повече от една организационна единица, вместо споразумение може да се издаде заповед на съответния компетентен държавен орган.

(3) При междусистемна връзка на КИС с други системи, които са в отговорността на една организационна единица, вместо споразумение се издава заповед на ръководителя й.

(4) При междусистемна връзка на КИС, предназначени за работа с класифицирана информация с ниво на класификация "За служебно ползване", с публична мрежа като интернет споразумение по ал. 1 не се сключва.

Чл. 78. (1) В споразумението или в заповедта по чл. 77 се посочват минимум:

1. границите на всяка от системите;

2. лицата по чл. 92, ал. 1, т. 2, когато е приложимо;

3. типът на информацията и/или информационните услуги, които всяка от страните ще получава и/или предоставя;

4. нивото на класификация на информацията, която всяка от страните ще получава и/или предоставя;

5. изискванията за осигуряване на конфиденциалност, интегритет и достъпност на информацията и услугите, които се получават и/или предоставят;

6. разпределението на отговорностите по въпроси на сигурността на информацията и услугите, които се получават и/или предоставят;

7. редът за уведомяване и взаимодействие при инциденти, както и длъжностните лица за контакт по въпроси, свързани със сигурността на всяка от системите;

8. съществуващи връзки с други системи, ако има такива, и техните параметри;

9. редът за предварително уведомяване при решение за реализация на нова връзка на свързаните системи;

10. редът за уведомяване и взаимодействие при прекратяване на експлоатацията на връзката;

11. параметрите за техническа и програмна съвместимост на средствата, осигуряващи свързаността, и на механизмите за защита на границата;

12. типът и форматът на обменяната информация при възникване на инцидент в сигурността на всяка от системите.

(2) Споразумението или заповедта по ал. 1 се предоставя на ОАС в съответствие с етапите за акредитиране по чл. 16, ал. 2 или по чл. 29, ал. 2.

Раздел II

Минимални изисквания към механизмите за защита на границата

Чл. 79. За всяка КИС, участваща в междусистемна връзка, се планират и внедряват механизми за защита на нейната граница.

Чл. 80. Механизмите за защита на границата трябва да осигуряват:

1. предоставяне само на услуги и преминаване само на потоци от информация, които са необходими за постигане на целите на свързването –

принцип на минималност;

2. предоставяне само на необходимите привилегии и разрешения за изпълнение на задачите и функциите на процесите, които са част от междусистемната връзка – принцип на най-малко привилегии;

3. възпрепятстване на всякакви дейности и информационни потоци, които не са част от междусистемната връзка;

4. защита, реализирана в различни компоненти от архитектурата на междусистемната връзка, с цел недопускане само една линия на защита – принцип на защита в дълбочина;

5. гарантиран механизъм за предотвратяване на пренос на информация с по-високо ниво на класификация към свързана система с по-ниско ниво на класификация.

Чл. 81. (1) Компонентите за защита на границата са програмни и/или технически средства, реализиращи механизмите за защита на границата на КИС. Реализацията на даден механизъм за защита на границата може да изисква комбинация от множество компоненти за защита, както и един компонент може да участва в различни механизми за защита на границата.

(2) Устройствата за защита на границата са специализирани компоненти, които се инсталират на границите на КИС, определени в споразумението или в заповедта по чл. 77 (защитни стени, устройства за откриване и/или за противодействие на проникване, регулатори на информационни потоци и др.).

Чл. 82. Чрез компонентите по чл. 81 трябва да се осигури:

1. еднозначна идентификация и автентификация на потребителите, услугите и процесите, участващи в междусистемна връзка;

2. контрол на достъпа на потребителите, устройствата и процесите, участващи в междусистемна връзка; достъпът до класифицирана информация и/или до услуги, предоставящи достъп до такава информация от потребители, устройства и процеси, принадлежащи към свързаните КИС, се извършва през предназначени за целта компоненти от механизма за защита на границата, непозволяващи достъпът да е директен;

3. конфиденциалност, интегритет и достъпност на пренасяната класифицирана информация;

4. автентичност на пренасяната информация и/или на предоставяните информационни услуги, където това е необходимо;

5. възможност за установяване на извършено действие или възникнало събитие, свързани със сигурността на КИС и класифицираната информация в нея, по начин, недопускащ тяхното отричане;

6. непрекъснатост на реализираните от тях услуги за сигурност;

7. защита на пренасяната информация от вредни програмни средства; в случай че тя е криптографски защитена, проверката за вредни програмни средства се извършва непосредствено след премахване на криптографската защита;

8. времево синхронизирани записи на събития, свързани със сигурността на реализираните услуги за системите, участващи в междусистемната връзка; информацията в одитните записи трябва да осигурява възможност за установяване на обстоятелства, свързани с компрометиране сигурността на КИС;

9. защита на одитните записи, свързани със сигурността, срещу неоторизиран преглед, промяна и изтриване;

10. задействане на подходящи блокировки при невъзможност за изпълнение на предвидената защита на класифицираната информация.

Чл. 83. Достъпът до управлението на всички компоненти за защита на границата трябва да бъде обект на надеждна идентификация и автентификация.

Чл. 84. През периода на експлоатация на междусистемната връзка механизмите за защита трябва да бъдат контролирани за правилното функциониране на компонентите им, което включва:

1. възлагане на отговорности по контрола;

2. обучение на персонала, отговорен за контрола;

3. периодично тестване за коректна работа;

4. документиране на проверките;

5. конфигурационен контрол върху механизмите за защита на междусистемната връзка и на системите за отчитане на работата им;

6. непрекъснато управление на риска.

Раздел III

Планиране, одобряване и въвеждане в експлоатация на механизми за защита на границата при междусистемна връзка

Чл. 85. (1) Планирането и одобряването на механизмите за защита на границата се извършват в рамките на процедурата по акредитиране на всяка КИС, участваща в междусистемна връзка.

(2) В етапа на планирането по ал. 1 ОРЕ:

1. взаимодейства с ОАС за уточняване на изискванията за сигурност към механизмите за защита на границата;

2. извършва подбор на подходящи механиз- ми за защита на границата на конкретната КИС при отчитане на резултатите от извършения анализ на риска.

Чл. 86. В съответствие с етапите за акредитиране по чл. 16, ал. 2 или по чл. 29, ал. 2 ОРЕ изпраща до ОАС:

1. подробно описание и схеми на логическата и физическа архитектура на реализиране на механизмите за защита на границата;

2. подробно описание на форматите на входящите и изходящите данни от и към механизмите за защита на границата;

3. описание на предвижданите компоненти за защита на границата и техническа документация на същите;

4. подробно описание на предвижданите настройки и режими на работа на компонентите за защита на границата за конкретната реализация на КИС;

5. описание на начините за сигнализация, когато не се реализират механизмите за защита, както и блокировките, които се задействат в такива случаи.

Чл. 87. В процеса на одобряване на механизми за защита на границата ОАС извършва:

1. проверка на пълнотата на документацията по чл. 86;

2. проверка за съответствие на избраните механизми за сигурност и реализиращите ги компоненти и устройства с минималните изисквания по раздел II;

3. определяне на контрамерките по TEMPEST.

Чл. 88. За извършване на дейностите по чл. 87 ОАС може да изиска от ОРЕ допълнителна информация, необходима за одобряването.

Чл. 89. (1) За всеки одобрен механизъм за защита на границата на съответната КИС ОАС уведомява писмено заявителя.

(2) В документа по ал. 1 се включват:

1. описание на одобрения механизъм за защита на границата;

2. списък на компонентите му;

3. условия за валидност на одобрението.

Чл. 90. Условията по чл. 89, ал. 2, т. 3 се включват в документа по чл. 32, ал. 1, т. 1.

Чл. 91. При установяване на неспособност на одобрения механизъм да осигури необходимото ниво на защита на класифицираната информация ОАС уведомява заявителя за предприемане на необходимите действия.

Раздел IV

Изисквания за сигурност при осъществяване на междусистемна връзка към информационни системи от затворен тип и към системи с публичен достъп

Чл. 92. (1) Информационна система от затворен тип, участваща в междусистемна връзка с КИС, трябва:

1. да не предоставя публичен достъп и да не е свързана към публични мрежи;

2. да има определени лица, в чиято отговорност е експлоатирането, развитието, управ- лението и сигурността на системата, както и разпределение на отговорностите, когато системата обхваща повече от една организация;

3. да има документално установени правила за:

а) достъп до електронната среда в системата – след еднозначна идентификация и автентификация на потребителя;

б) предоставяне на достъп до системата; достъпът се предоставя само от определена категория потребители;

в) запис на събития и възможност за изучаване на одитните записи, свързани с успешни и неуспешни опити за достъп от всички категории потребители;

г) защита от вредни програмни средства.

(2) Разпределението на отговорностите по ал. 1, т. 2, както и правилата по ал. 1, т. 3 трябва да са включени в споразумението или в заповедта по чл. 77.

Чл. 93. Междусистемна връзка на КИС към системи с публичен достъп като интернет или други подобни се реализира посредством доставчик на услугата – при сключен договор за осигуряване на достъпност, качество и защита на предоставяната услуга.

Глава седма
РЕД ЗА ОТНЕМАНЕ И ПРЕКРАТЯВАНЕ НА СЕРТИФИКАТИ ЗА СИГУРНОСТ НА КИС

Чл. 94. (1) Отнемането на сертификата по чл. 93 от ЗЗКИ се извършва с акт по образец съгласно приложение № 2.

(2) Органът по акредитиране на сигурност- та на КИС уведомява съответната организационна единица, като изпраща екземпляр от отнемането на сертификата за сигурност на конкретната КИС.

(3) След получаване на акта по отнемане на сертификата ръководителят на организационната единица незабавно предприема мерки за прекратяване на дейността по създаване, обработване, съхраняване и пренасяне на класифицирана информация по тази КИС.

Чл. 95. (1) При наличие на основание по чл. 93, ал. 2, т. 1 от ЗЗКИ действието на сертификата за конкретната КИС се прекратява автоматично без издаване на писмен акт.

(2) При наличие на основание по чл. 93, ал. 2, т. 2, 3 и 4 от ЗЗКИ за прекратяване действието на издаден сертификат по чл. 14, т. 2 от ЗЗКИ:

1. заявителят подава до ОАС заявление за прекратяване на издадения сертификат, изготвено от ОРЕ и съгласувано със служителя по сигурността на информацията, в което се посочват основанието за прекратяване действието на сертификата и предприетите мерки за защита на класифицираната информация, обработвана в конкретната КИС;

2. в случаите на промяна на нивото на класификация по чл. 93, ал. 2, т. 2 от ЗЗКИ заявителят подава и заявление за започване на процедура по акредитиране по чл. 15;

3. органът по акредитиране на сигурността на КИС уведомява органа по прекия контрол за подаденото заявление за прекратяване действието на сертификата с изключение на случаите, в които основание за прекратяване е промяна на нивото на класификация към по-високо;

4. органът по прекия контрол извършва проверка и уведомява ОАС за резултатите от нея.

(3) Въз основа на данните от заявлението и/или резултатите от извършената проверка по ал. 2, т. 4 ОАС взема решение за прекратяване действието на сертификата за сигурност с акт по образец съгласно

приложение № 3.

(4) Органът по акредитиране на сигурността на КИС уведомява заявителя, като изпраща екземпляр от акта за прекратяване на действието на сертификата за сигурност.

(5) В случаите по ал. 2, т. 2, когато нивото на класификация на КИС се променя към по-ниско и не са настъпили промени на мерките за сигурност в глобалната, локалната или електронната среда за сигурност на конкретната КИС, проверката по чл. 18, ал. 1, т. 2 не се извършва.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на наредбата:

1. "Комуникационна система" е съвкупност от взаимносвързани комуникационни средства, криптографски средства и среда за разпространение на сигнала, предоставящи комуникационен ресурс на КИС.

2. "Заплаха към КИС" е възможност за случаен или целенасочен нерегламентиран достъп до класифицираната информация.

3. "Уязвимост на КИС" е слабост в системата от мерки за сигурност или в контрола за тяхното изпълнение, които могат да доведат до компрометиране или да улеснят компрометирането на сигурността на КИС. Уязвимостта може да бъде пропуск или да се дължи на недостатъчно ефективен надзор, недобра комплектованост и устойчивост на работата на КИС или на неефективна физическа защита. Уязвимостта може да бъде от техническо, програмно, технологично или процедурно естество.

4. "Риск за КИС" е възможността определена заплаха да използва уязвимите места на КИС и да компрометира в определена степен нейната сигурност.

5. "Ресурси на КИС" са използваните в нея технически и програмни средства и техните характеристики, потребителската и системната информация на КИС.

6. "Обект на КИС" (или само "обект") е пасивен елемент на КИС, който съдържа или приема информация.

7. "Субект на КИС" (или само "субект") е активен елемент на КИС (лице, процес или устройство), който осъществява обмен на информация между обектите или изменение в състоянието на КИС.

8. "Атрибути за сигурност" са уникални характеристики на обектите и субектите, използвани от механизмите за сигурност при осигуряване на достъпа на субектите до обектите. За обектите атрибутите за сигурност отразяват нивото на класификация и категорията на информацията. За субектите атрибутите за сигурност отразяват разрешението за достъп до класифицирана информация и категориите информация, до които имат право на достъп на основата на принципа "необходимост да се знае".

9. "Механизъм за сигурност" е реализиране на мярка за сигурност в КИС чрез технически и програмни средства.

10. "Идентификация на субекта" е разпознаване на субекта от механизмите за сигурност на КИС.

11. "Автентификация на субекта" е процес на проверка от механизмите за сигурност на КИС на идентичността на субекта.

12. "Оторизация на субекта" е даване на определени права на субекта за изпълнение на определени действия с ресурсите на КИС.

13. "Конфиденциалност на информацията" е характеристика на класифицираната информация в КИС, която изисква защитата й от разкриване от неоторизиран субект.

14. "Интегритет на информацията" е характеристика на информацията в КИС, която изисква защитата й от промяна от неоторизиран субект.

15. "Достъпност на информацията" е характеристика на информацията в КИС, която изисква осигуряване на гарантиран и своевременен достъп на оторизираните субекти до нея.

16. "Компрометиране на сигурността на КИС" е пълна или частична загуба на конфиденциалност, интегритет или достъпност на информацията в КИС.

17. "Одитен запис" е запис за събитие, което има отношение към сигурността на КИС.

18. "Глобална среда за сигурност на КИС" е средата, в която е разположена КИС и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на служителя по сигурността на информацията на организационната единица и са извън контрола на ОРЕ.

19. "Локална среда за сигурност на КИС" е средата, в която е разположена КИС и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на ОРЕ.

20. "Електронна среда за сигурност на КИС" е съвкупността от мерките за сигурност от областта на компютърната, комуникационната и криптографската сигурност и контрамерките по TEMPEST, които са приложени в самата КИС и са в отговорността на ОРЕ.

21. "Вредни програмни средства" са програмни средства, изпълнението на които може да доведе до нарушаване работата на КИС или до загуба на достъпност, конфиденциалност или интегритет на информацията.

22. "Администратор на КИС" е лице, изпълняващо функциите по системно, приложно, мрежово или друго администриране в КИС.

23. "Критично от гледна точка на сигурност- та на КИС оборудване" е сървърно оборудване, комуникационни и криптографски средства от комуникационната система, подсистеми за управление и друго оборудване, определено от анализа на риска.

24. "Компонент за защита на границата" е техническо или програмно средство, реализиращо една или няколко функции от механизма за защита на границата.

25. "Методология" е система от принципи и средства за организиране и провеждане на дадена дейност.

26. "Автентичност на информацията" е гаранцията, че същата е оригинална и е от доверен източник.

27. "Жизнен цикъл на КИС" е целият период на съществуване на КИС, който включва концепция, планиране, разработка, развитие, тестване, въвеждане, функциониране, поддръжка и извеждане от експлоатация.

28. "Приемане на риска" е решение за приемане на съществуването на остатъчен риск.

29. "Акредитиране на КИС" е процес, водещ до издаване от ОАС на сертификат за сигурност в уверение на това, че дадена КИС е одобрена да функционира в конкретната среда на експлоатация и при приемливо ниво на риска, въз основа на приложен одобрен комплекс от мерки за сигурност.

30. "Сертифицирана КИС" е комуникационна и информационна система, която е преминала през процедура по акредитиране и е получила сертификат за сигурност, издаден от ОАС.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. За процедурите по акредитиране, които към момента на влизането в сила на наредбата не са завършили, се прилага тази наредба.

§ 3. Издадените до влизането в сила на наредбата сертификати за сигурност на автоматизирани информационни системи или мрежи или на комуникационни и информационни системи се считат за валидни до изтичане на сроковете им.

§ 4. Срокът по чл. 21, т. 6, буква "г" за действащи сертификати за сигурност на автоматизирани информационни системи или мрежи или на комуникационни и информационни системи започва да тече от датата на влизането в сила на наредбата.

§ 5. Издадените до влизането в сила на наредбата свидетелства за обучение на служители по сигурността на АИС или мрежи за преминато обучение в ОАС в областта на защитата на класифицирана информация, която се създава, обработва, съхранява и пренася в АИС или в мрежи, се считат за валидни.

§ 6. Наредбата се приема на основание чл. 90, ал. 1 от Закона за защита на класифицираната информация.

Приложение № 1

към чл. 20, ал. 1

ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ"

СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ "ИНФОРМАЦИОННА СИГУРНОСТ"

СЕРТИФИКАТ ЗА СИГУРНОСТ НА КОМУНИКАЦИОННА И ИНФОРМАЦИОННА СИСТЕМА

№ .....

На основание чл. 14, т. 2 от Закона за защита на класифицираната информация и чл. 3, ал. 2, т. 5 от Наредбата за сигурност на комуникационните и информационните системи и резултатите от извършена комплексна оценка на сигурността Специализирана дирекция "Информационна сигурност" издава настоящия сертификат за сигурност на .....

.....,*(наименование на комуникационната и информационна система (КИС)* изградена за нуждите на .....

.....*(наименование на организационната единица – заявител)*

Настоящият сертификат удостоверява, че в посочената по-горе.....

.....

(КИС) може да се създава, обработва, ползва, съхранява и обменя класифицирана информация в електронна форма с ниво на класификация за сигурност до .....

.....

.....

.... включително.

Срок на валидност до .....

.....

..... Подпис:

.....*(дата на издаване)*

Печат:.....
.....*(място на издаване)*
*(фамилия)***Приложение № 2**
към чл. 94, ал. 1 ДЪРЖАВНА АГЕНЦИЯ
"НАЦИОНАЛНА СИГУРНОСТ"
СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ
"ИНФОРМАЦИОННА СИГУРНОСТ"
ОТНЕМАНЕ НА СЕРТИФИКАТ ЗА
СИГУРНОСТ НА КОМУНИКАЦИОННА
И ИНФОРМАЦИОННА СИСТЕМА
№ .....На основание чл. 93, ал. 1 от Закона за защита на класифицираната
информация и чл. 94, ал. 1 от Наредбата за сигурността на комуникационните
и информационните системи, поради констатирани системни нарушения на
изискванията за сигурност на класифицираната информация, създавана,
обработвана, ползвана, съхранявана или обменяна в комуникационната и
информационната система (КИС), Специализирана дирекция "Информационна
сигурност" отнема издаден сертификат за сигурност № .....на ....
....., *(наименование на КИС)*изградена за нуждите на
.....
.....
..... *(наименование на организационната единица – заявител)*Отнемането не подлежи на обжалване по съдебен ред.Отнемането може да бъде оспорено по реда на глава пета, раздел V от ЗЗКИ
пред Държавната комисия по сигурността на информацията в 7-дневен срок от
уведомяването на организационната единица.Екземпляр от отнемането да се връчи на ръководителя на организационната
единица..... Подпис:
.....*(дата на издаване)*
Печат:..... .....*(място*

*на издаване) (фамилия)***Приложение № 3**

към чл. 95, ал. 3 ДЪРЖАВНА АГЕНЦИЯ

"НАЦИОНАЛНА СИГУРНОСТ"

СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ

"ИНФОРМАЦИОННА СИГУРНОСТ"

ПРЕКРАТЯВАНЕ НА СЕРТИФИКАТ

ЗА СИГУРНОСТ НА КИС

№ .....На основание чл. 93, ал. 2, т. ..... от Закона за защита на

класифицираната информация и чл. 95, ал. 3 от Наредбата за сигурността на

комуникационните и информационните системи, поради .....

(премахване или промяна на нивото на класификация на информацията, която се

създава, обработва, ползва, съхранява или обменя; прекратяване

експлоатацията на комуникационната и информационната система (КИС);

закриване на организационната единица без правоприемник) Специализирана

дирекция "Информационна сигурност" прекратява действието на издаден

сертификат за сигурност № .....на .....

....., *(наименование на КИС)*изградена за нуждите на .....

..... *(наименование на организационната единица – заявител)*Прекратяването не подлежи на обжалване по съдебен ред.Прекратяването може да бъде оспорено по реда на глава пета, раздел V от

ЗЗКИ пред Държавната комисия по сигурността на информацията в 7-дневен срок

от уведомяването на организационната единица.Екземпляр от прекратяването да се връчи на ръководителя на организационната

единица..... Подпис:

.....*(дата на издаване)*
Печат:.....
.....*(място на издаване)*
*(фамилия)***Приложение № 4**
към чл. 3, ал. 2, т. 8
ДЪРЖАВНА АГЕНЦИЯ
"НАЦИОНАЛНА СИГУРНОСТ"
СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ
"ИНФОРМАЦИОННА СИГУРНОСТ"
СВИДЕТЕЛСТВО ЗА ОБУЧЕНИЕ №
.....На основание чл. 3, ал. 2, т. 8 от Наредбата за сигурността на
комуникационните и информационните системи Специализирана дирекция
"Информационна сигурност" издава настоящото свидетелствона
.....
.....
.....,
*(трите имена на лицето)*определен за служител по сигурността на КИС в
.....
.....,
*(организационна единица)*в уверение на това, че същият е преминал успешно курс на обучение по
задължителните общи условия за сигурност на комуникационните и
информационните системи (КИС).Обучението е проведено от Органа по акредитиране на сигурността на КИС..... Подпис:
.....*(дата на издаване)*
Печат:.....
.....*(място на издаване)*
(фамилия)