НАРЕДБА за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация

Приета с ПМС № 99 от 10.05.2003 г., обн., ДВ, бр. 46 от 20.05.2003 г., изм., бр. 44 от 9.05.2008 г., доп., бр. 57 от 24.07.2009 г., изм., бр. 101 от 18.12.2009 г., в сила от 18.12.2009 г., изм. и доп., бр. 108 от 17.12.2013 г., в сила от 17.12.2013 г., изм., бр. 41 от 16.05.2014 г., в сила от 16.05.2014 г.

Сборник закони - АПИС, кн. 6/2003 г., стр. 440

Библиотека закони - АПИС, т. 1, р. 6, № 809г

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С наредбата се определят задължителните общи условия за сигурност на автоматизираните информационни системи (АИС) или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, наричани по-нататък "АИС или мрежи".

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

1. органите по сигурността на АИС или мрежи;

2. условията и реда за извършване на комплексна оценка на сигурността и издаване на сертификати за АИС или мрежи, наричани по-нататък "акредитиране";

3. задължителните общи изисквания за сигурност на АИС или мрежи в областта на:

а) физическата сигурност;

б) персоналната сигурност;

в) документалната сигурност;

г) комуникационната сигурност;

д) криптографската сигурност;

е) защитата от паразитни електромагнитни излъчвания;

ж) компютърната сигурност.

Глава втора
ОРГАНИ ПО СИГУРНОСТТА НА АИС ИЛИ МРЕЖИ

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, съхранявана, обработвана и пренасяна в АИС или мрежи;

2. на процеса на акредитиране на АИС или мрежи.

Раздел II
Орган по акредитиране на сигурността на АИС или мрежи

Чл. 3. (1) (Изм. - ДВ, бр. 44 от 2008 г., бр. 41 от 2014 г. , в сила от 16.05.2014 г.) Орган по акредитиране на сигурността на АИС или мрежи (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 АИС или мрежи;

2. препоръчва стандарти и средства, които могат да се използват в АИС или мрежи за защита на класифицирана информация;

3. утвърждава документите по сигурността на АИС или мрежи;

4. извършва комплексна оценка на сигурността на АИС или мрежи;

5. издава сертификати за сигурност на АИС или мрежи;

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

7. координира и контролира дейността по защита от паразитни електромагнитни излъчвания на техническите средства, обработващи, съхраняващи и пренасящи класифицирана информация;

8. провежда обучение на служители по сигурността на АИС или мрежи;

9. води регистър на сертифицираните АИС или мрежи;

10. (нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) отнема и прекратява действието на сертификати за сигурност на АИС или мрежи при условията, посочени в глава шеста, раздел V от Закона за защита на класифицираната информация (ЗЗКИ).

Раздел III
Служител по сигурността на АИС или мрежи

Чл. 4. (1) (Изм. и доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Ръководителят на организационната единица, в която се експлоатират или се предвижда изграждането на АИС или мрежи за обработка на класифицирана информация, по предложение на служителя по сигурността на информацията назначава в административното звено по сигурността служител по сигурността на АИС или мрежи 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 АИС или мрежи.

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

(3) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В органите на държавната власт и на местното самоуправление, в които са обособени повече от една организационна единица, служителят по сигурността на АИС или мрежи може да е от състава на друга организационна единица в рамките на съответния орган.

(4) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Функции на служител по

сигурността на АИС или мрежи в случаите по ал. 3 се възлагат със заповед на ръководителя на ведомството или органа на местното самоуправление по предложение на ръководителя на организационната единица, в която ще се изпълняват функциите на служител по сигурността на АИС или мрежи, съгласувано с ръководителя на организационната единица, в състава на която е служителят.

(5) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Задълженията на служителя по сигурността на АИС или мрежи в случаите по ал. 3 се определят с акта по чл. 22, ал. 1.

Чл. 5. Служителят по сигурността на АИС или мрежи:

1. е отговорен за установяването на политиката за сигурност на АИС или мрежи в организационната единица;

2. определя изискванията за сигурност към АИС или мрежи, произтичащи от общата политика за сигурност на организационната единица;

3. координира изготвянето на специфичните изисквания за сигурност на АИС или мрежи, процедурите за сигурност и на изработените на тяхна основа експлоатационни документи по сигурността;

4. координира обучението по сигурността на АИС или мрежи;

5. осъществява контрол за спазване на изискванията за сигурност в АИС или мрежи;

6. разследва обстоятелствата, свързани с компрометиране сигурността на АИС или мрежи, и докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОАС.

Раздел IV
Орган по развитие и експлоатация на АИС или мрежи (ОРЕ)

Чл. 6. (1) Органът по развитие и експлоатация в организационната единица:

1. участва в определянето на политиката за сигурност на АИС или мрежи в организационната единица;

2. изготвя документите по сигурността на АИС или мрежата;

3. осигурява изпълнението на изискванията за акредитиране на АИС или мрежи и прави заявки за допълнително акредитиране на АИС или мрежата, когато това е необходимо;

4. участва в определянето на мерките за сигурност и границите на отговорност при осъществяване на връзки с други АИС или мрежи;

5. прави предложение за възлагане функции на администратор по сигурността на АИС или мрежата и осигурява подготовката му;

6. организира и провежда обучение по сигурността в АИС или мрежи на служителите в ОРЕ и на потребителите на АИС или мрежата;

7. прилага одобрените мерки за сигурност в АИС или мрежата;

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

9. участва заедно със служителя по сигурността на АИС или мрежи в установяването на обстоятелствата, свързани с компрометиране сигурността на АИС или мрежи.

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

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

Раздел V
Администратор по сигурността на АИС или мрежа

Чл. 7. (1) (Предишен текст на чл. 7 – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Със заповед на ръководителя на организационната единица по предложение на ОРЕ съгласувано със служителя по сигурността на информацията се възлагат функции на администратор по сигурността на АИС или мрежата.

(2) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В органите на държавната власт и на местното самоуправление, в които са обособени повече от една организационна единица, администраторът по сигурността на АИС или мрежата може да е от състава на друга организационна единица в рамките на съответния орган.

(3) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Функции на администратор по сигурността на АИС или мрежата в случаите по ал. 2 се възлагат със заповед на ръководителя на ведомството или на органа на местното самоуправление по предложение на ръководителя на организационната единица, в която ще се изпълняват функциите на администратор по сигурността на АИС или мрежата, съгласувано с ръководителя на организационната единица, в състава на която е служителят.

(4) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Задълженията на администратора по сигурността на АИС или мрежата в случаите по ал. 3 се определят с акта по чл. 22, ал. 1.

Чл. 8. (1) Администраторът по сигурността на АИС или мрежата е от състава на ОРЕ или от друго звено в организационната единица, имаща отношение към АИС или мрежата.

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

(3) (Доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Задълженията на администратора по сигурността на АИС или мрежата и на администратора на АИС или мрежата трябва да са ясно разграничени, като не могат да се изпълняват от едно и също лице.

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

(5) Когато автоматизираната мрежа обхваща няколко организационни единици, всяка от тях определя администратор по сигурността за нейната част от мрежата. Администраторът по сигурността на цялата мрежа се определя от организатора на мрежата по чл. 22, ал. 1.

Чл. 9. (1) Администраторът по сигурността на АИС или мрежата:

1. участва в изготвянето и актуализирането на процедурите по сигурността на АИС или мрежата;

2. изготвя експлоатационни документи по сигурността на АИС или мрежата за обслужващия персонал и потребителите на базата на утвърдените процедури за сигурност;

3. изпълнява възложените му процедури за сигурност в АИС или мрежата;

4. периодично информира обслужващия персонал и потребителите по въпросите на

сигурността на АИС или мрежата;

5. осигурява на потребителите достъп до ресурсите на АИС или мрежата в съответствие с предоставените им права;

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

а) следи за спазването на мерките и процедурите за сигурност в зоните за сигурност на АИС или мрежата;

б) следи за спазването на мерките и процедурите за сигурност при инсталирането, конфигурирането, поддръжката и промените в АИС или мрежата;

в) следи за правилното функциониране на механизмите за сигурност;

г) управлява, наблюдава и анализира свързаните със сигурността одитни записи на системата и при констатиране или при съмнения за компрометиране на сигурността докладва на ОРЕ и на служителя по сигурността на АИС или мрежи;

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

7. участва заедно със служителя по сигурността на АИС или мрежи и с ОРЕ в установяването на обстоятелствата, свързани с компрометиране на сигурността на АИС или мрежата;

8. изпълнява функциите на администратор по криптографска защита на информацията, ако в АИС или мрежата се прилагат криптографски методи и средства.

(2) Функциите по ал. 1 могат да бъдат разпределени между няколко специално определени администратори по сигурността на АИС или мрежата.

Раздел VI
Потребители в АИС или мрежи

Чл. 10. Потребител в АИС или мрежа 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 АИС или мрежата;

2. което е преминало обучение в областта на сигурността на АИС или мрежа;

3. на което са предоставени права за достъп до ресурсите на АИС или мрежа.

Чл. 11. (1) Потребителите в АИС или мрежа изпълняват задълженията, посочени в експлоатационните документи по сигурността на АИС или мрежа.

(2) Потребителите изпълняват указанията на администратора по сигурността на АИС или мрежа, свързани със сигурността на системата или мрежата.

(3) Потребителите уведомяват администратора по сигурността на АИС или мрежа за случаи или съмнения за компрометиране сигурността на АИС или мрежата.

Глава трета
АКРЕДИТИРАНЕ НА АИС ИЛИ МРЕЖИ

Раздел I
Условия и ред за акредитиране

Чл. 12. Процедурата по акредитиране започва от етапа на проектиране на системата. В периода на акредитирането ОРЕ взаимодейства с ОАС за уточняване на изискванията за сигурност към изгражданата АИС или мрежа.

Чл. 13. (1) (Изм. и доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В етапа на проектиране на АИС или мрежа 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 АИС или мрежата, 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 АИС или мрежата;

2. връзки с други АИС или мрежи;

3. ръководителят на ОРЕ и администраторът по сигурността на АИС или мрежи;

4. етапите и сроковете за изграждане на АИС или мрежата.

Чл. 14. (1) В срок до 15 работни дни ОАС взема решение за откриване на процедура по акредитиране и уведомява писмено заявителя.

(2) (Доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В уведомлението по ал. 1 се посочват срокове за предоставяне на документите по сигурността по чл. 29, съобразени с етапите и сроковете за изграждане на АИС или мрежата, условията и етапите за акредитиране.

Чл. 15. В съответствие с етапите за акредитиране по чл. 14, ал. 2 за извършване на комплексна оценка на АИС или мрежата преди въвеждането ѝ в експлоатация заявителят изпраща до ОАС:

1. документите по сигурността съгласно чл. 29, ал. 1;

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

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

4. решението за въвеждане в експлоатация на криптографски средства, ако такива се използват в АИС или мрежата;

5. информация за участниците в разработката и изпълнението на проекта.

Чл. 16. (1) Органът по акредитиране на сигурността извършва комплексна оценка, като:

1. проверява представените документи по чл. 15;

2. проверява изпълнението на предвидените мерки за сигурност;

3. на основание чл. 90, ал. 2 от Закона за защита на класифицираната информация (ЗЗКИ) ОАС утвърждава документите по чл. 29, ал. 1, т. 2 и 3.

(2) Проверките по ал. 1, т. 1 и 2 се извършват от комисия с председател - представител на ОАС, и членове - представители на ОАС и на организационната единица. При необходимост може да се привличат специалисти по видовете сигурност.

(3) Комплексната оценка по ал. 1 може да не включва проверки по т. 2 за АИС или мрежи, в които се създава, обработва, съхранява или пренася само класифицирана информация, представляваща служебна тайна.

(4) Комисията по ал. 2 се назначава със заповед на ръководителите на ОАС и на организационната единица.

Чл. 17. В случай на установени несъответствия при проверките по чл. 16, ал. 1, т. 1 и 2 ОАС изисква от заявителя да ги отстрани.

Чл. 18. (1) (Изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) При положителна комплексна оценка ОАС издава сертификат за сигурност на АИС или мрежата по чл. 14, т.

2 ЗЗКИ съгласно приложение № 1.

(2) Сертификатът по ал. 1 може да се издава и за обособени подсистеми на АИС или мрежи по реда на тази глава.

Чл. 19. Сертификатът съдържа:

1. идентификация на сертификата;
2. правното основание за издаването на сертификата;
3. идентификация на АИС или мрежата;
4. идентификация на заявителя;
5. нивата на класификация за сигурност на информацията, която ще бъде създавана, обработвана, съхранявана и пренасяна в АИС или мрежата;
6. (изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) срок на валидност на сертификата:

а) "Строго секретно" – 3 години;

б) "Секретно" – 4 години;

в) "Поверително" – 5 години;

г) "За служебно ползване" – без срок;

7. дата и място на издаването;
8. подпис и печат.

Чл. 20. (1) За резултатите от оценката по чл. 16 ОАС изготвя сертификационен отчет, който е неразделна част на сертификата.

(2) Сертификационният отчет съдържа:

1. общо описание на АИС или мрежата;
2. заключения от комплексната оценка;
3. опис на документите за сигурност, представени при акредитирането;
4. (изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) видовете изменения на АИС или мрежата, които изискват извършване на допълнително акредитиране.

(3) Сертификационният отчет по ал. 2 се класифицира с ниво на класификация, еднакво с най-високото ниво на класификация на информацията в АИС или мрежата.

Чл. 21. (1) В случай че за изпълнението на важни за държавата задачи е необходимо АИС или мрежа да бъде въведена в експлоатация, преди да бъде завършен процесът на акредитиране и издаване на сертификат, ОАС може да издаде сертификат за сигурност на АИС или мрежата за определен период.

(2) Сертификатът по ал. 1 се издава след съгласуване с ДКСИ.

(3) Сертификатът по ал. 1 съдържа:

1. ниво на класификация на информацията, която ще бъде създавана, съхранявана, обработвана и пренасяна в АИС или мрежата;
2. задължителните условия за сигурност, които трябва да се спазват при експлоатацията на АИС или мрежата в периода на действие на сертификата;
3. условия за окончателно акредитиране на АИС или мрежата;
4. срок на валидност на сертификата.

Чл. 22. (1) (Доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Когато АИС или мрежата обхваща повече от една организационна единица, между тях се сключва споразумение, определящо коя организационна единица е организатор на АИС или

мрежата и разпределението на отговорностите по сигурността за съставните части на АИС или мрежата. В органите на държавната власт и на местното самоуправление, в които са обособени повече от една организационна единица, вместо споразумение може да се издаде заповед на ръководителя на ведомството или на органа на местното самоуправление.

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

(3) Споразумението по ал. 1 се прилага към заявлението по чл. 13 от организатора на АИС или мрежата.

(4) Всяка организационна единица носи отговорност за акредитирането на частта от АИС или мрежата, която е в нейна отговорност по споразумението по ал. 1.

(5) (Нова - ДВ, бр. 57 от 2009 г.) Организационните единици по чл. 4 и 5 от 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. 23. (1) За всяка акредитирана АИС или мрежа ОАС поддържа акредитационно дело, което съдържа:

1. преписката по акредитирането и допълнителните акредитирания;
2. вторите екземпляри на сертификата и сертификационния отчет по чл. 20;
3. отчетите за допълнителните акредитирания по чл. 28, ал. 1, т. 3.

(2) Документите по сигурността се съхраняват в организационната единица.

Чл. 24. (1) Органът по акредитиране на сигурността води регистър на сертифицираните АИС или мрежи. За всяка сертифицирана АИС или мрежа в регистъра се вписват:

1. данните от сертификата;
2. регистрационните номера на заявленията по чл. 13 и 25;
3. регистрационните номера на документите по сигурността, представени при акредитирането и при допълнителните акредитирания;
4. регистрационните номера на сертификационния отчет по чл. 20 и допълнителните отчети по чл. 28, ал. 1, т. 3;
5. регистрационните номера на документите, съдържащи изменения на специфичните изисквания за сигурност и процедурите за сигурност, утвърдени от ОАС.

(2) (Изм. - ДВ, бр. 44 от 2008 г.) 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. 25. (1) При необходимост от промени по чл. 20, ал. 2, т. 4 в АИС или мрежата 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 промените, които налагат допълнителното акредитиране;

2. очаквано влияние на промените върху сигурността на АИС или мрежата;

3. етапите и сроковете за извършване на промените.

Чл. 26. (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 и етапите за допълнително акредитиране.

Чл. 27. В съответствие с етапите за допълнително акредитиране за извършване на оценка на промените и влиянието им върху сигурността на АИС или мрежата заявителят представя на ОАС:

1. измененията в специфичните изисквания за сигурност и процедурите за сигурност на АИС или мрежата;

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

3. при поискване - документи по сигурността, утвърдени от ОАС.

Чл. 28. (Изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) (1) Органът по акредитиране на сигурността на АИС или мрежи:

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 комисията по чл. 16, ал. 2. При необходимост може да бъдат привличани специалисти по видовете сигурност.

(3) Проверките по ал. 1, т. 1 може да не бъдат извършвани за АИС или мрежи, в които се създава, обработва, съхранява или пренася класифицирана информация, представляваща служебна тайна.

(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 АИС или мрежата;

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

Глава четвърта
ДОКУМЕНТИ ПО СИГУРНОСТТА, НЕОБХОДИМИ ЗА АКРЕДИТИРАНЕ

Раздел I
Видове документи

Чл. 29. (1) Задължителните документи по сигурността, необходими за извършване на акредитирането, са:

1. анализът на риска за сигурността на АИС или мрежата;

2. специфичните изисквания за сигурност на АИС или мрежата в организационната единица;

3. процедурите за сигурност, изготвени на основата на СИС.

(2) Документите по сигурността по ал. 1 се класифицират с ниво на класификация, съответстващо на най-високото ниво на класификация на информацията, която се обработва в АИС или мрежата.

(3) За АИС или мрежи, с които се обработва информация с ниво на класификация за сигурност до "Поверително" (включително), анализ на риска не се изисква.

Раздел II
Анализ на риска

Чл. 30. Анализът на риска за сигурността на АИС или мрежата е процес, при който се установяват заплахите и уязвимите места на АИС или мрежата, вероятността за осъществяване на заплахите при конкретните ресурси и работна среда и се оценяват последствията при тяхното реализиране.

Чл. 31. Анализът на риска цели:

1. определяне на необходимите мерки за сигурност;

2. ефективно комбиниране на видовете мерки за сигурност;

3. правилна оценка на остатъчния риск.

Чл. 32. Анализът на риска се извършва периодично с оглед отчитането на:

1. новопоявили се уязвимости и/или заплахи към АИС или мрежата;

2. промени в ресурсите на АИС или мрежата и/или в нивото на класификация за сигурност на информацията.

Чл. 33. (1) За анализ на риска и определяне на адекватни мерки за противодействие в организационната единица се сформира екип от специалисти по физическа, персонална, документална, компютърна, комуникационна и криптографска сигурност и по защита от електромагнитни излъчвания.

(2) В екипа по ал. 1 могат да се привличат и представители на проектантите.

(3) За сложни АИС или мрежи при възможност се използват автоматизирани средства за оценка на риска.

Чл. 34. (1) Възможните резултати от анализа на всеки конкретен риск са:

1. елиминиране на риска - целта е цялостно елиминиране на реална или потенциална уязвимост на АИС или мрежата чрез пълно прилагане на мерки за сигурност;

2. предотвратяване загубата на физически и информационни ресурси - целта е 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 информационни ресурси - целта е прилагане на мерки за сигурност, ограничаващи загубите до приемливо ниво;

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

(2) Резултатите от анализа на риска се оформят в документа по чл. 38, т. 2.

Чл. 35. За условия на експлоатация на АИС или мрежа, които не са свързани с конкретна глобална среда за сигурност (например мобилни, полеви и други условия), при анализа на риска се оценяват и рисковете, свързани със средата, в която АИС или мрежата ще бъде ползвана.

Раздел III
Специфични изисквания за сигурност

Чл. 36. (1) За всяка АИС или мрежа, в която се създава, обработва, съхранява и пренася класифицирана информация, се изготвят специфични изисквания за сигурност (СИС) съгласно чл. 90, ал. 2 ЗЗКИ.

(2) Специфичните изисквания за сигурност се формулират по време на най-ранния стадий от проектирането на системата и се детайлизират и развиват в процеса на разработване и изпълнение на проекта на АИС или мрежата. Степента на детайлизация зависи от сложността на системата или мрежата, от режима на сигурност, в който се експлоатира, и от нивото на класификация на обработваната информация.

(3) В своя завършен вид СИС определят как се постига, управлява и контролира сигурността на АИС или мрежата.

Чл. 37. В отделните етапи на разработка и експлоатация на АИС или мрежата СИС изпълняват различни функции:

1. в етапа на планиране СИС представляват схематично описание на глобалната и локалната среда за сигурност, в които ще се експлоатира системата, с постепенна детайлизация на изискванията за сигурност;

2. в етапа на разработка или доставка се детайлизират техническите аспекти на СИС, което спомага за правилната спецификация на системата или мрежата;

3. преди комплексната оценка СИС са в завършен вид и са основа за формулиране на процедурите за сигурност;

4. в етапа на експлоатация СИС определят границите на отговорност на ОРЕ и на останалия състав, действащ в локалната и глобалната среда за сигурност;

5. в етапа на прекратяване на експлоатацията СИС се ползват за определяне на действията, които трябва да се предприемат с цел запазване сигурността на информацията.

Чл. 38. Специфичните изисквания за сигурност в завършен вид съдържат:

1. подробно описание на АИС или мрежата по отношение на формата на представяне и нивото на класификация на информацията; групите потребители според нивото на достъп и начина на взаимодействие със системата; физическата среда за работа; функционалните елементи, включително архитектура, интерфейси и външни връзки;

2. (доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) описание на специфичните заплахи, уязвимостите на АИС или мрежата, режима за сигурност при експлоатация на системата, изискванията към физическата и техническата среда, а в случаите по чл. 77 – резултатите от изготвения анализ на риска и предложените заместващи мерки;

3. описание на глобалната, локалната и електронната среда за сигурност на АИС или мрежата;

4. подробно описание на мерките за сигурност относно:

а) контрола на достъпа, включително физическия, и определяне автентичността на потребителите;

б) отчетността на действията на отделните потребители и възможностите за проверка на валидността на тези действия;

в) предотвратяване на възможността за нерегламентиран достъп до информация, включително при повторно използване обектите на системата;

г) съхраняване интегритета на информацията;

д) осигуряване достъпност на информацията;

е) пренасянето на информацията;

ж) други специфични рискове;

5. управление на сигурността, включително при прилагане на разработените процедури по сигурността, конфигурационния контрол, поддръжката, разработването на документи по сигурността, обучението, случаите, в които се налага допълнително акредитиране;

6. описание на мерките за сигурност при критични ситуации;

7. описание на мерките за сигурност при прекратяване на експлоатацията на АИС или мрежата.

Чл. 39. При необходимост от по-детайлно разработване на отделни аспекти на сигурността по чл. 1, ал. 2, т. 3, букви "г" - "ж" ОАС може да изисква допълнителни СИС за тези аспекти.

Раздел IV
Процедури за сигурност на АИС или мрежи

Чл. 40. (1) Процедурите за сигурност са подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на утвърдените мерки за сигурност на АИС или мрежата.

(2) Процедурите за сигурност са правилата за сигурност по чл. 90, ал. 3 ЗЗКИ.

Чл. 41. Процедурите за сигурност съдържат следните раздели:

1. организация на сигурността;
2. персонална сигурност;
3. физическа сигурност;
4. документална сигурност;
5. компютърна сигурност;
6. комуникационна сигурност;
7. сигурност при осигуряването със средства за АИС или мрежата;
8. действия при критични по отношение на сигурността ситуации;
9. управление на конфигурацията;
10. отговорности и задължения на потребителите.

Глава пета
ОБЩИ ИЗИСКВАНИЯ ЗА СИГУРНОСТ НА АИС ИЛИ МРЕЖИ

Раздел I

Сигурност на АИС или мрежи

Чл. 42. (1) Сигурността на АИС или мрежа, в която се създава, обработва, съхранява или пренася класифицирана информация, 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, създавана, обработвана, съхранявана или пренасяна в АИС или мрежата.

Раздел II
Физическа сигурност

Чл. 43. (1) Зоните, в които са разположени ресурсите на АИС или мрежата, където се създава, обработва, съхранява или пренася класифицирана информация или в които е възможен достъп до такава информация, се определят като зони за сигурност съгласно наредбата по чл. 78 ЗЗКИ.

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

Чл. 44. (1) В рамките на зоните за сигурност по чл. 43, ал. 1 се определят места за: компютърно и комуникационно оборудване; въвеждане и извеждане на документи във и от системата; център за управление на АИС или мрежата; работа с криптографски средства и ключове; библиотеки за компютърни носители на класифицирана информация и др.

(2) За критичните от гледна точка на сигурността места по ал. 1 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.

Чл. 45. За условия на експлоатация на АИС или мрежа, които не са свързани с конкретна глобална среда за сигурност (например мобилни, полеви и други условия), се изготвят специфични изисквания за физическа сигурност.

Раздел III
Персонална сигурност

Чл. 46. (1) Потребителите на АИС или мрежата трябва да имат разрешение за достъп до най-високото ниво на класификация за сигурност на информацията, с която имат право да работят в АИС или мрежата.

(2) Системният персонал на АИС или мрежата, както и лицата, участващи в проектирането и изграждането на системата за сигурност на АИС или мрежата, трябва да имат разрешение за достъп до най-високото ниво на класификация на информацията в АИС или мрежата.

Чл. 47. (1) Системният персонал и потребителите на АИС или мрежата преминават обучение по сигурността на АИС или мрежата.

(2) Обучението по ал. 1 се организира и провежда от ОРЕ за различните категории служители (системни администратори, администратори по сигурността, развойни звена,

технически и обслужващ персонал).

(3) При успешно завършило обучение лицата по ал. 1 се допускат до работа в АИС или мрежата.

Чл. 48. Правомощията на персонала, работещ в АИС или мрежа, се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на АИС или мрежата.

Раздел IV
Документална сигурност

Чл. 49. (1) Всички документи, съдържащи класифицирана информация, които се създават, обработват, съхраняват и/или пренасят в АИС или мрежи, се идентифицират, маркират и контролират по подходящи начини.

(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 АИС или мрежата.

(4) Документите по ал. 1 не се регистрират в регистратурата по чл. 51, ал. 1 от Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ).

Чл. 50. Извеждането на документи, съдържащи класифицирана информация, от сертифицирани АИС или мрежи се извършва:

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

2. в зоните за сигурност по чл. 43, ал. 1.

Чл. 51. Пренос на документи, съдържащи класифицирана информация, от една АИС или мрежа към друга се извършва само ако получателят е АИС или мрежа, сертифицирана за ниво на класификация на информацията, същото или по-високо от нивото на класификация на пренасяните документи.

Чл. 52. (1) Материалните носители на класифицирана информация, използвани в АИС или мрежи, се маркират, регистрират се в регистратурата по чл. 51, ал. 1 ППЗЗКИ и се съхраняват по начин, съответстващ на грифа за сигурност 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.

Чл. 53. Съхраняването и периодичният контрол на носителите по чл. 52, ал. 2 се извършват в съответствие с утвърдените процедури за сигурност на АИС или мрежата.

Чл. 54. (1) Информацията и материалите, осигуряващи достъп до ресурсите на АИС или мрежата, се защитават с мерки, съответни на мерките за най-високото ниво на класификация на информацията, за която дават достъп.

(2) Информацията и материалите по ал. 1, които вече не се използват за осигуряване на достъп до ресурсите на АИС или мрежата, се унищожават в съответствие с правилата в експлоатационната документация по сигурността и по начин, недопускащ възстановяване на информацията.

Чл. 55. (1) Преносими компютърни устройства, използвани за създаване, обработване и съхраняване на класифицирана информация, се разглеждат като носители на такава информация.

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

Раздел V
Комуникационна и криптографска сигурност, защита от паразитни електромагнитни излъчвания, които могат да доведат до компрометиране на сигурността на АИС или мрежата
(Загл. изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.)

Чл. 56. (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, защита от излъчвания и защита при пренасяне на информацията.

Чл. 57. Комуникационните системи за пренос на класифицирана информация 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.

Чл. 58. В АИС или мрежи се прилагат само криптографски средства, одобрени по реда на наредбата по чл. 85 ЗЗКИ.

Чл. 59. (1) Класифицирана информация се пренася по комуникационни системи извън зоните за сигурност на АИС или мрежи, когато е защитена с криптографски средства.

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

Чл. 60. (1) Автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и/или пренася класифицирана информация с ниво на класификация "Поверително" и по-високо, трябва да са осигурени срещу паразитни електромагнитни излъчвания, които могат да доведат до нерегламентиран достъп до информацията.

(2) Мерките за защита от електромагнитни излъчвания съответстват на най-високото ниво на класификация на информацията в АИС или мрежата.

Раздел VI
Минимални изисквания за компютърна сигурност

Чл. 61. Компютърната сигурност представлява система от мерки за сигурност, прилагани с цел осигуряване на конфиденциалност, интегритет и достъпност на класифицираната информация в АИС или мрежата. Тези мерки за сигурност се реализират чрез възможностите на техническите и програмните средства на компютърните системи и на специализирани средства.

Чл. 62. (1) Минималните изисквания за компютърна сигурност на АИС или мрежа включват:

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

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

3. непрекъснат запис на събития, свързани със сигурността на АИС или мрежата (одитни записи); записват се всички действия, свързани с контрола на достъпа, включително неуспешни опити за достъп, създаване или разрушаване на обекти или действия на оторизирани субекти, влияещи на сигурността на информационната система;

4. възможност за изучаване на одитните записи и установяване на свързаните със сигурността действия на отделните субекти на АИС или мрежа;

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

6. 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. 63. Автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и/или пренася класифицирана информация, се експлоатират в един или няколко от следните режими за сигурност:

1. "С общ достъп";

2. "С общо ниво";

3. "С много нива".

Чл. 64. (1) При работа на АИС или мрежа в режим за сигурност "С общ достъп":

1. всички потребители имат разрешение за достъп до най-високото ниво на класификация на информацията, която се създава, обработва, съхранява или пренася в АИС или мрежата;

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

(2) Компютърната сигурност за АИС или мрежа 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 АИС или мрежата.

(3) При работа на АИС или мрежа в режим за сигурност "С общ достъп" цялата информация, създавана, обработвана, съхранявана или пренасяна в АИС или мрежата, 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 АИС или мрежа в режим за сигурност "С общо ниво":

1. всички потребители имат разрешение за достъп до най-високото ниво на

класификация на информацията, създавана, обработвана, съхранявана или пренасяна в АИС или мрежата;

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

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

(3) При работа на АИС или мрежа в режим за сигурност "С общо ниво" цялата информация, която се създава, обработва, съхранява или пренася в АИС или мрежата, се защитава като информация с най-високо ниво на класификация, освен ако е налице гарантиран механизъм за разпознаване нивото на класификация на информацията.

Чл. 66. (1) При работа на АИС или мрежа 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 АИС или мрежа по ал. 1 се осигурява с минималните изисквания за компютърна сигурност и прилагане на задължителен контрол на достъп на субектите до обектите на АИС или мрежата.

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

1. присвояване на атрибут за сигурност на всеки субект и обект на АИС или мрежата; 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 АИС или мрежата за присвояване и изменение на атрибутите за сигурност на субектите на АИС или мрежата по реда, установен в документите по сигурността на АИС или мрежата;

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 АИС или мрежата 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 АИС или мрежи

Чл. 67. (1) Експлоатацията и развитието на сертифицирана АИС или мрежа 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 АИС или мрежи, служителят и администраторът по сигурността на АИС или мрежата в рамките на своите отговорности контролират и оценяват всички промени в глобалната, локалната и електронната среда за сигурност на АИС или мрежата и съвместно предлагат изменение на мерките и процедурите за сигурност.

(3) Когато промените по ал. 2 не налагат изменение на СИС, изменението на мерките и процедурите за сигурност се извършва с документ, утвърден от ръководителя на организационната единица, който става част от документите по сигурността на АИС или мрежата.

(4) Когато промените по ал. 2 налагат изменение на СИС, променените СИС и описанието на промените по ал. 2 се представят за утвърждаване от ОАС, който в срок 15 работни дни след представяне на необходимите документи ги утвърждава или прави мотивиран отказ. Промените по ал. 2 не се извършват преди утвърждаването на промените в СИС.

(5) Когато промените по ал. 2 налагат допълнително акредитиране за сигурност на АИС или мрежата, се разкрива процедура по реда на глава трета, раздел II.

(6) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) Най-малко 6 месеца преди изтичане срока на валидност на издадения сертификат за сигурност на АИС или мрежата в случаите, когато е необходимо да се продължи експлоатирането й, заявителят подава до ОАС на АИС или мрежи заявление за ново акредитиране по реда на глава трета, раздел I.

(7) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В случаите по ал. 6, когато не са настъпили промени в глобалната, локалната и електронната среда за сигурност на АИС или мрежата, проверката по чл. 16, ал. 1, т. 2 може да не бъде извършвана.

Чл. 68. По време на експлоатацията и развитието на АИС или мрежата:

1. се извършва проверка на програмни средства и преносими носители на информация за наличието на вредни програмни средства, преди те да бъдат използвани в АИС или мрежата;

2. се извършва резервиране на системната и класифицираната информация, като резервните копия се съхраняват по начин, недопускащ нерегламентиран достъп до тях;

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

4. се извършва внедряване на нови технически и програмни средства или на техни версии само след оценка и тестване за сигурност от ОРЕ или след одобряване от ОАС, когато е необходимо допълнително акредитиране на АИС или мрежата;

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

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

7. се извършва повторно одобряване за електромагнитни излъчвания на преминали ремонт технически средства;

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

Чл. 69. (1) Преносими компютърни устройства, съдържащи класифицирана информация, могат да бъдат свързвани към АИС или мрежа само ако тя е сертифицирана за ниво на класификация на информацията, съответстващо на маркировката на устройствата.

(2) Служителят по сигурността на информацията на организационната единица дава разрешение за свързването по ал. 1.

(3) Преносими компютърни устройства могат да работят в места с осигурени мерки за физическа сигурност, съответстващи на нивото на класификация на информацията, съдържаща се в тях.

Раздел IX
Сигурност на АИС или мрежи, в които се създава, обработва, съхранява или пренася информация с класификационно ниво "Строго секретно"

Чл. 70. Класифицирана информация с класификационно ниво "Строго секретно" се създава, обработва и съхранява във:

1. автоматизирани информационни системи, изградени на базата на самостоятелни, несвързани в мрежа компютърни устройства, защитени от паразитни електромагнитни излъчвания, или

2. автоматизирани информационни системи или мрежи, изградени в зони за сигурност, които са защитени от паразитни електромагнитни излъчвания.

Чл. 71. Класифицирана информация с ниво на класификация "Строго секретно" не се пренася по комуникационни системи извън зоните по чл. 70, т. 2.

Чл. 72. Класифицирана информация с класификационно ниво "Строго секретно" не се обработва с преносими компютърни устройства.

Чл. 73. Автоматизирани информационни системи или мрежи, 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. 74. Автоматизирани информационни системи или мрежи, съхраняващи и обработващи информация с ниво на класификация "Строго секретно", не могат да бъдат свързвани с други АИС и мрежи.

Чл. 75. Криптографски методи и средства за защита на информация с ниво на класификация "Строго секретно" могат да се използват само за защита при съхраняване на информацията с цел прилагане на принципа "необходимост да се знае".

Чл. 76. (1) Носителите за многократен запис на информация, използвани за съхраняване на информация с ниво на класификация "Строго секретно", се водят в отделен регистър.

(2) Върху носителите за многократен запис с ниво на класификация "Строго секретно" не може да се записва информация с по-ниско ниво на класификация.

(3) При изтичане на експлоатационния период на носителите за многократен запис с ниво на класификация "Строго секретно" те не се декласифицират, а се унищожават.

(4) Повредените компютърни носители с ниво на класификация "Строго секретно" не се ремонтират, а се унищожават по реда на чл. 141 ППЗЗКИ.

Раздел X
Възможност за заместване на мерките за компютърна сигурност, комуникационна сигурност и защита от паразитни електромагнитни излъчвания, които могат да доведат до компрометиране на сигурността на АИС или мрежата
(Загл. изм. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.)

Чл. 77. (1) (Доп. – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) В случай на прекомерни разходи за осъществяване на някои мерки за компютърна сигурност, комуникационна сигурност и защита от паразитни електромагнитни излъчвания, които могат да доведат до компрометиране на сигурността на АИС или мрежата, те могат да се заместят с мерки от другите видове сигурност на АИС или мрежа.

(2) (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) 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) (Предишна ал. 2 – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) 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
(Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.)
РЕД ЗА ОТНЕМАНЕ И ПРЕКРАТЯВАНЕ НА СЕРТИФИКАТИ ЗА СИГУРНОСТ НА АИС ИЛИ МРЕЖИ

Чл. 78. (Нов – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) (1) Отнемането на сертификата по чл. 94а ЗЗКИ се извършва с акт по образец съгласно приложение № 2.

(2) Органът по акредитиране на сигурността на АИС или мрежи уведомява съответната организационна единица, като изпраща екземпляр от отнемането на сертификата за сигурност на АИС или мрежата.

(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 АИС или мрежа.

Чл. 79. (Нов – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) (1) При наличие на основание по чл. 94б, т. 1 ЗЗКИ за прекратяване действието на издаден сертификат по чл. 14, т. 2 ЗЗКИ, ОАС прекратява действието на сертификата за сигурност на АИС или мрежата с акт по образец съгласно приложение № 3 не по-късно от датата на изтичане срока на сертификата и уведомява писмено ръководителя на организационната единица, като изпраща екземпляр от него. След получаване на акта за прекратяване на сертификата за сигурност на АИС или мрежата ръководителят на организационната единица незабавно предприема мерки за прекратяване на дейността по създаване, обработване, съхраняване и пренасяне на класифицирана информация в тази АИС или мрежа.

(2) При наличие на основание по чл. 94б, т. 2, 3 и 4 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 АИС или мрежата;

2. в случаите на промяна нивото на класификация по чл. 94б, т. 2 ЗЗКИ заявителят подава и заявление за започване на процедура по акредитиране по чл. 13;

3. органът по акредитиране на сигурността на АИС или мрежи 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 АИС или мрежи уведомява заявителя, като изпраща екземпляр от акта за прекратяване действието на сертификата за сигурност.

(5) В случаите по ал. 2, т. 2, когато нивото на класификация на АИС или мрежата се променя към по-ниско и не са настъпили промени в глобалната, локалната и електронната среда за сигурност на АИС или мрежата, проверката по чл. 16, ал. 1, т. 2 не се извършва.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на наредбата:

1. "Автоматизирана информационна система" (АИС) е съвкупност от технически и програмни средства, методи, процедури и персонал, организирани за осъществяване на функции по създаването, съхраняването, обработването, ползването и обмена на класифицирана информация в границите на системата. Границите на системата се определят от ОРЕ. Автоматизираната информационна система може да бъде изградена и на основата на една или повече отделни работни станции, несвързани в мрежа, които са в отговорността на ОРЕ.

2. "Автоматизирана информационна мрежа" (или само "мрежа") е съвкупност от технически и програмни средства, методи и ако е необходимо, персонал и процедури, организирани за осъществяване обмен на данни (информация) между две или повече АИС или в рамките на една АИС.

3. "Комуникационна система" е съвкупност от взаимносвързани комуникационни средства, криптографски средства и среда за разпространение на сигнала, предоставящи комуникационен ресурс на АИС или мрежата.

4. "Заплаха към АИС или мрежа" е възможност за случаен или целенасочен нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежата.

5. "Уязвимост на АИС или мрежа" 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 АИС или мрежата. Уязвимостта може да бъде пропуск или да се дължи на недостатъчно ефективен надзор, недобра комплектуваност и устойчивост на работата на АИС или мрежата или на неефективна физическа защита. Уязвимостта може да бъде от техническо, програмно, технологично или процедурно естество.

6. "Риск за АИС или мрежа" е възможността определена заплаха да използва уязвимите места на АИС или мрежата и да компрометира в определена степен нейната сигурност.

7. "Ресурси на АИС или мрежа" са използваните в нея технически и програмни средства и техните характеристики, потребителската и системната информация на АИС или мрежата.

8. "Обект на АИС или мрежа" (или само "обект") е пасивен елемент на АИС или мрежата, който съдържа или приема информация.

9. "Субект на АИС или мрежа" (или само "субект") е активен елемент на АИС или мрежата (лице, процес или устройство), който осъществява обмен на информация между обектите или изменение в състоянието на системата или мрежата.

10. "Атрибути за сигурност" са уникални характеристики на обектите и субектите, използвани от механизмите за сигурност при осигуряване 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".

11. "Механизъм за сигурност" е реализиране на мярка за сигурност в АИС или мрежата чрез технически и програмни средства.

12. "Идентификация на субекта" е разпознаване на субекта от механизмите за сигурност на АИС или мрежата.

13. "Автентификация на субекта" е процес на проверка от механизмите за сигурност на АИС или мрежата на идентичността на субекта.

14. "Оторизация на субекта" е даване на определени права на субекта за изпълнение на определени действия с ресурсите на АИС или мрежата.

15. "Конфиденциалност на информацията" е характеристика на класифицираната информация в АИС или мрежата, която изисква защитата й от разкриване от неоторизиран субект.

16. "Интегритет на информацията" е характеристика на информацията в АИС или мрежата, която изисква защитата й от промяна от неоторизиран субект.

17. "Достъпност на информацията" е характеристика на информацията в АИС или мрежата, която изисква осигуряване на гарантиран и своевременен достъп на оторизираните субекти до нея.

18. "Компрометиране на сигурността на АИС или мрежата" е пълна или частична загуба на конфиденциалност, интегритет или достъпност на информацията в АИС или мрежа.

19. "Одитен запис" е запис за събитие, което има отношение към сигурността на АИС или мрежата.

20. "Глобална среда за сигурност на АИС или мрежата" е средата, в която е разположена АИС или мрежата 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.

21. "Локална среда за сигурност на АИС или мрежата" е средата, в която е разположена АИС или мрежата и в която са приложени мерки за физическа, персонална и документална сигурност, които са в отговорността на ОРЕ.

22. "Електронна среда за сигурност на АИС или мрежата" е съвкупността от мерките за сигурност от областта на компютърната, комуникационната и криптографската сигурност и на защитата от електромагнитни излъчвания, които са приложени в самата АИС или мрежа и са в отговорността на ОРЕ.

23. "Системен персонал" са служителите, на които е възложена отговорността за експлоатацията, развитието, управлението или сигурността на АИС или мрежата.

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

25. (Нова – ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.) "Администратор на АИС или мрежи" е лице, изпълняващо функциите по системно, приложно, мрежово или друго администриране в системата или мрежата.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. (1) Автоматизираните информационни системи или мрежи, в които към момента на влизането в сила на наредбата се създава, обработва, съхранява и пренася класифицирана информация, се считат за сертифицирани за срок 18 месеца.

(2) В срок един месец от влизането в сила на наредбата ръководителите на организационните единици уведомяват писмено ОАС кои АИС или мрежи ще се считат за сертифицирани съгласно ал. 1.

(3) Заявление за акредитиране на АИС или мрежи по ал. 2 се подава не по-късно от 12 месеца от влизането в сила на наредбата.

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

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ към Постановление № 308 на Министерския съвет от 17 декември 2009 г. за изменение и допълнение на Правилника за прилагане на Закона за Държавна агенция "Национална сигурност"

(ДВ, бр. 101 от 2009 г., в сила от 18.12.2009 г.)

.....

§ 50. Навсякъде в Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, приета с Постановление № 99 на Министерския съвет от 2003 г. (обн., ДВ, бр. 46 от 2003 г.; изм. и доп., бр. 44 от 2008 г. и бр. 57 от 2009 г.) думите "Главна дирекция "Технически операции" се заменят със "специализирана дирекция "Технически операции".

.....

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

към Постановление № 280 на Министерския съвет от 12 декември 2013 г. за изменение и допълнение на Наредбата за задължителните общи условия за сигурност на

автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация

(ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г.)

§ 21. Сроковете по чл. 19, т. 6 за действащите сертификати за сигурност на АИС или мрежи започват да текат от датата на влизане в сила на постановлението.

.....

ПОСТАНОВЛЕНИЕ № 110 на Министерския съвет
от 10 май 2014 г. за изменение на Наредбата
за задължителните общи условия за сигурност
на автоматизираните информационни системи или мрежи,
в които се създава, обработва, съхранява и пренася
класифицирана информация

(ДВ, бр. 41 от 2014 г., в сила от 16.05.2014 г.)

§ 1. Навсякъде в наредбата и в приложенията към нея думите "специализирана дирекция "Технически операции" се заменят със "специализирана дирекция "Информационна сигурност".

Преходни и заключителни разпоредби

§ 2. Издадените от специализирана дирекция "Технически операции" сертификати за сигурност на автоматизирани информационни системи или мрежи запазват действието си.

.....

Приложение № 1

към чл. 18, ал. 1
(Изм. - ДВ, бр. 44 от 2008 г., бр. 108 от 2013 г.,
в сила от 17.12.2013 г.,
бр. 41 от 2014 г.,
в сила от 16.05.2014 г.)

ДЪРЖАВНА АГЕНЦИЯ „НАЦИОНАЛНА СИГУРНОСТ”

СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ "ИНФОРМАЦИОННА СИГУРНОСТ"

СЕРТИФИКАТ ЗА СИГУРНОСТ

НА

АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ИЛИ МРЕЖА

№ .....

На основание чл. 14, т. 2 от Закона за защита на класифицираната информация и чл. 3, ал. 2, т. 5 от Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи (АИС) или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, и резултатите от извършена комплексна оценка

Специализирана дирекция "Информационна сигурност" издава настоящия сертификат за сигурност на

.....,

(наименование на АИС или мрежа)

изградена за нуждите на .....

.....

(наименование на организационната единица - заявител)

Настоящият сертификат удостоверява

че в посочената по-горе .....

(АИС или мрежа)

може да се създава, обработва, съхранява и пренася класифицирана информация 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. 78, ал. 1
(Ново - ДВ, бр. 108 от 2013 г.,
в сила от 17.12.2013 г.,
изм., бр. 41 от 2014 г.,
в сила от 16.05.2014 г.)

ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ"
СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ "ИНФОРМАЦИОННА СИГУРНОСТ"
ОТНЕМАНЕ НА СЕРТИФИКАТ ЗА СИГУРНОСТ НА АИС ИЛИ МРЕЖА
№ .....

На основание чл. 94а от Закона за защита на класифицираната информация и чл. 78, ал. 1 от Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи (АИС) или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, поради констатирани системни нарушения на изискванията за сигурност на класифицираната информация, създавана, обработвана, съхранявана и пренасяна в АИС или мрежа,

Специализирана дирекция "Информационна сигурност" на Държавна агенция "Национална сигурност" отнема издаден сертификат за сигурност
№ .....
на .....
.....,
(наименование на АИС или мрежа)

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 или на упълномощен представител на организационната единица.

..... Подпис: .....
(дата на издаване) Печат:
..... (.....)
(място на издаване) *(фамилия)*

Приложение № 3

към чл. 79, ал. 1
(Ново - ДВ, бр. 108 от 2013 г., в сила от 17.12.2013 г., изм., бр. 41 от 2014 г., в сила от 16.05.2014 г.)

ДЪРЖАВНА АГЕНЦИЯ "НАЦИОНАЛНА СИГУРНОСТ"
СПЕЦИАЛИЗИРАНА ДИРЕКЦИЯ "ИНФОРМАЦИОННА СИГУРНОСТ"
ПРЕКРАТЯВАНЕ НА СЕРТИФИКАТ ЗА СИГУРНОСТ НА АИС ИЛИ МРЕЖА
№ .....

На основание чл. 94б, т. ... от Закона за защита на класифицираната информация и чл. 79, ал. 1 от Наредбата за задължителните общи условия за сигурност на автоматизираните информационни системи (АИС) или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, поради ... *(изтичане срока на действие на сертификат за сигурност на АИС/М; премахване или промяна на нивото на класификация на информацията, която се създава, обработва, съхранява и пренася в АИС/М; прекратяване експлоатацията на АИС/М; закриване на организационната единица без правоприемник)*
Специализирана дирекция "Информационна сигурност" на Държавна агенция "Национална сигурност" прекратява действието на издаден сертификат за сигурност №.....
на .....
.....,
(наименование на АИС или мрежа)
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 или на упълномощен представител на организационната единица.

..... Подпис: .....

(дата на издаване)
.....
(място на издаване)

Печат:
(.....)
(фамилия)