НАРЕДБА за криптографската сигурност на класифицираната информация

Приета с ПМС № 263 от 11.11.2003 г., обн., ДВ, бр. 102 от 21.11.2003 г., изм., бр. 44 от 9.05.2008 г., доп., бр. 57 от 24.07.2009 г., изм., бр. 5 от 19.01.2010 г., бр. 27 от 5.04.2016 г., в сила от 5.04.2016 г., изм. и доп., бр. 35 от 10.05.2016 г., в сила от 10.05.2016 г., бр. 21 от 13.03.2020 г., в сила от 13.03.2020 г.

Сборник закони - АПИС, кн. 12/2003 г., стр. 235

Библиотека закони - АПИС, т. 1, р. 6, № 601

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. С наредбата се определят:

1. органите за криптографска сигурност на класифицираната информация в Република България;

2. условията и редът за:

а) (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) използване на криптографски методи и средства за защита на класифицирана информация; производство, маркиране, съхраняване, разпределяне, пренасяне, използване и унищожаване на криптографски материали и на криптографски средства за защита на класифицирана информация;

б) издаване на разрешения и удостоверения за работа с криптографски средства;

в) (изм. и доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) одобрение на криптографски средства за защита на класифицирана информация;

г) (нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) контрол по използване на криптографски методи и средства за защита на класифицирана информация.

Глава втора
ОРГАНИ ЗА КРИПТОГРАФСКА СИГУРНОСТ

Раздел I
Държавна комисия по сигурността на информацията

Чл. 2. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Държавната комисия по

сигурността на информацията осъществява общо ръководство и контрол на дейностите по криптографска сигурност.

Раздел II
Орган по криптографската сигурност на Република България

Чл. 3. (Изм. - ДВ, бр. 44 от 2008 г.) Орган по криптографската сигурност на Република България (ОКС) по смисъла на наредбата е Държавна агенция "Национална сигурност".

Чл. 4. Органът по криптографската сигурност на Република България:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) прилага националната политика за криптографска сигурност в съответствие със Закона за защита на класифицираната информация (ЗЗКИ), тази наредба и другите подзаконови актове по защитата на класифицираната информация;

2. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) дава указания и задължителни предписания по всички аспекти на криптографската сигурност;

3. (изм. и доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) извършва одобрение на криптографски методи и средства за защита на класифицираната информация и периодичен анализ за установяване на тяхната способност да защитават класифицирана информация;

3а. (нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) проектира и разработва изцяло или отделни елементи от криптографски методи и средства;

4. участва в извършването на комплексна оценка на сигурността на криптографските мрежи и в одобряването на въвеждането им в експлоатация;

5. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) произвежда и разпределя ключови материали за криптографските мрежи на Република България;

6. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) извършва одобрение на системи за управление на криптографски ключове (СУКК) и одобрява въвеждането им в експлоатация и периодичен анализ за установяване на тяхната способност за защита на класифицираната информация;

7. координира и контролира използването, производството и вноса на средства за криптографска защита на класифицирана информация;

8. провежда обучение в областта на криптографската сигурност и издава разрешения за работа с криптографски средства;

9. осъществява методическо ръководство на дейността на служителите по криптографската сигурност;

10. разрешава и контролира провеждането на обучение по криптографска сигурност от други организационни единици;

11. изготвя писмени становища при компрометиране на криптографската сигурност;

12. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) води регистри на одобрените криптографски средства и мрежи, поекземплярно проверените криптографски средства и разрешенията за работа с криптографски средства;

13. (отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

Раздел III
Служител по криптографската сигурност

Чл. 5. (1) Във всяка организационна единица, в която се експлоатират или се предвижда да се въвеждат в експлоатация криптографски средства за защита на класифицираната информация, с писмена заповед на нейния ръководител се определя служител по криптографската сигурност.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Служителят по криптографската сигурност е служител от организационната единица.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При необходимост могат да бъдат определени повече от един служител по криптографската сигурност.

(4) Задълженията на служител по криптографската сигурност могат да се изпълняват и от служителя по сигурността на информацията.

Чл. 6. Служителят по криптографската сигурност е лице, което е получило разрешение за работа с криптографски средства.

Чл. 7. Служителят по криптографската сигурност:

1. създава необходимата организация и осъществява общо ръководство и контрол на криптографската защита на класифицираната информация в организационната единица;

2. организира изготвянето на необходимите документи за изпълнение на процедурите по наредбата;

3. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) организира изготвянето на криптоплановете в организационната единица, които се утвърждават от ОКС;

4. организира и осъществява подготовката на администраторите по криптографската

сигурност и на потребителите на криптографски средства, като:

а) прави предложения пред служителя по сигурността на информацията за възлагане на функции по чл. 8 и 11;

б) изготвя конкретните им функционални задължения, свързани с криптографската сигурност;

в) организира или извършва обучението им;

г) издава удостоверения за работа с криптографски средства;

д) води на отчет, отнема и прекратява действието на издадените удостоверения;

5. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) организира процедурата по снабдяване и водене на отчет на криптографските средства и криптографските материали в организационната единица;

6. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) организира съхраняването, пренасянето и контрола на криптографските средства, криптографските материали и друга документация, свързана с криптографската сигурност в организационната единица;

7. организира унищожаване на снетите от експлоатация криптографски средства;

8. участва в установяване на обстоятелствата, свързани с компрометиране на криптографската сигурност, и докладва за резултатите на служителя по сигурността на информацията в организационната единица, който уведомява ОКС;

9. (нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) организира инвентаризация на използваните в организационната единица криптографски средства и криптографски материали и изготвя обобщен отчет по чл. 36, ал. 6.

Раздел IV
Администратор по криптографската сигурност

Чл. 8. (1) Ръководителят на организационната единица въз основа на предложение на служителя по сигурността на информацията с писмена заповед възлага функции на администратор по криптографската сигурност.

(2) За всяка криптографска мрежа се определя администратор по криптографската сигурност.

Чл. 9. Администраторът по криптографската сигурност е служител от организационната единица, който е получил удостоверение за работа с криптографски средства.

Чл. 10. (1) Администраторът по криптографската сигурност:

1. организира въвеждането в експлоатация на криптографската мрежа;

2. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) контролира спазването на правилата за експлоатация на криптографските средства и криптоплана от потребителите на криптографски средства и периодично ги информира за техните задължения във връзка с криптографската сигурност;

3. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) осигурява снабдяването с криптографски материали, необходими за работа на криптографската мрежа;

4. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) експлоатира системи за управление на криптографски ключове при наличие на такива системи;

5. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) контролира съхраняването, използването и унищожаването на криптографските материали;

6. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) извършва периодична инвентаризация на използваните в подчинената му криптографска мрежа криптографски средства и криптографски материали, за резултатите от която представя отчет на служителя по криптографската сигурност;

7. извършва проверка за целостта на защитната опаковка на ключовите материали при получаването им, при инвентаризацията им и преди тяхното предаване и/или използване;

8. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) разработва и предлага на служителя по криптографската сигурност изменения и допълнения на криптоплана;

9. следи за правилното функциониране на криптографските средства и за извършването на регламентираните профилактични дейности и проверки;

10. при установяване на неизправна работа на криптографските средства организира своевременното им изваждане от експлоатация и техния ремонт;

11. (отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.);

12. участва заедно със служителя по криптографската сигурност в установяването на обстоятелствата, свързани с компрометиране на криптографската сигурност.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Функциите по ал. 1 могат да бъдат възложени или разпределени на няколко служители по чл. 9. Разпределянето на функциите се описва в криптоплана по чл. 19, ал. 1, т. 5.

Раздел V
Потребител на криптографски средства

Чл. 11. Ръководителят на организационната единица въз основа на предложение от служителя по сигурността на информацията с писмена заповед възлага функции на потребители на криптографски средства.

Чл. 12. Потребител на криптографски средства е служител от организационната единица, който е получил удостоверение за работа с криптографски средства.

Чл. 13. Потребителят на криптографски средства:

1. обработва класифицирана информация с криптографски средства;

2. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) експлоатира криптографските средства при спазване на криптоплана;

3. информира администратора по криптографската сигурност за всеки случай на неизправна работа на криптографските средства и компрометиране на криптографската сигурност.

Глава трета
ИЗПОЛЗВАНЕ НА КРИПТОГРАФСКИ СРЕДСТВА

Раздел I
Въвеждане в експлоатация на криптографски мрежи

Чл. 14. (1) (Изм. - ДВ, бр. 44 от 2008 г.) За защита на класифицираната информация се прилагат само криптографски средства, предварително одобрени и регистрирани от ОКС по чл. 86 ЗЗКИ.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При наличие на одобрени криптографски средства от внос и на произведени в Република България, удовлетворяващи в еднаква степен качествените и функционалните изисквания към тях за конкретното приложение, организационните единици закупуват и прилагат криптографските средства, произведени в Република България.

(3) За защита на класифицираната информация в задграничните представителства на Република България се използват само криптографски средства, произведени в Република България.

(4) За защита на класифицираната информация, обменяна с други държави или международни организации, с които Република България има влезли в сила международни договори за защита на класифицирана информация, могат да се използват криптографски средства, одобрени от страната организатор на криптографската мрежа, в съответствие с двустранните договорености по сигурността или българското законодателство.

Чл. 15. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) Ръководителят на организационната единица взема решение за необходимостта от използване на криптографски средства за защита на класифицираната информация в организационната единица и изпраща писмено запитване до ОКС за наличието на одобрени криптографски средства. В запитването се посочват качествените и функционалните показатели на средствата, от които организационната единица има нужда.

(2) В срок до 15 работни дни от получаването на запитването ОКС отговаря писмено за наличието на одобрени средства по ал. 1. В писмения отговор се посочват нивото на класифицирана информация, за което са одобрени, предназначението, версията и производителят им.

(3) Процедура по възлагане на обществена поръчка за доставка на криптографски средства може да започне след получаването на писмения отговор по ал. 2 за одобрени криптографски средства.

(4) След приключването на процедурата за доставка на криптографски средства по ал. 3 ръководителят на организационната единица уведомява писмено ОКС за броя и идентификационните номера на доставените криптографски средства.

Чл. 16. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) За използването на криптографски средства ръководителят на организационната единица изпраща заявление до ОКС, което съдържа:

1. идентификационни данни на криптографските средства, които ще се организират в криптографската мрежа;

2. нивото за сигурност на класифицираната информация, която ще бъде защитавана;

3. наименование на криптографската мрежа и наименование на комуникационната и информационната система (КИС), ако криптографската мрежа се предвижда да е част от такава система, включително връзка с други системи;

4. описание на мерките за физическа сигурност на криптографските средства;

5. описание на предвиждания брой криптографски средства, които ще се използват в криптографска мрежа, на предвижданата организация на използването им, както и на физическото им местоположение.

(2) В случаите, когато криптографската мрежа е част от КИС, заявлението по ал. 1 се подава на етап, определен от органа по акредитиране на сигурността (ОАС) на КИС в уведомлението по чл. 16 от Наредбата за сигурността на комуникационните и информационните системи.

Чл. 17. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В срок до 15 работни дни от получаване на заявлението ОКС дава или отказва съгласие за използване на криптографските средства по чл. 16, за което уведомява писмено организационната

единица.

(2) Отказът по ал. 1 съдържа условията за даване на съгласие.

Чл. 18. (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

Чл. 19. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) За въвеждане в експлоатация на криптографски мрежи за защита на класифицираната информация е необходимо предварително да са налице:

1. одобрени и поекземплярно проверени от ОКС криптографски средства;

2. администратор по криптографската сигурност и при необходимост потребители на криптографски средства в организационната единица;

3. документ, удостоверяващ изпълнението на нормативните изисквания за физическа и документална сигурност, съответстващи на нивото за сигурност на криптографските средства и на защитаваната класифицирана информация;

4. изпълнени условия за експлоатация на криптографските средства, определени в техните сертификати за одобрение, и условията за валидност към сертификатите;

5. изготвен в организационната единица и утвърден от ръководителя на ОКС или от упълномощено от него длъжностно лице криптоплан, включващ:

а) организационни правила и правила за техническа експлоатация в областта на криптографската сигурност;

б) план за действие при критични ситуации.

(2) В срок до 24 месеца от получаването на съгласието по чл. 17, ал. 1 организационната единица – заявител, уведомява писмено ОКС за изпълнението на изискванията на ал. 1.

(3) Органът по криптографската сигурност на Република България прекратява процедурата по чл. 16 в случаите, когато не е спазен срокът по ал. 2.

Чл. 20. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) Въвеждането в експлоатация на криптографски средства в криптографска мрежа се одобрява с решение на комисия след проверка на изпълнението на изискванията по чл. 19, а когато са част от КИС – след издаване на сертификат за сигурност на КИС по чл. 20 от Наредбата за сигурността на комуникационните и информационните системи.

(2) Комисията по ал. 1 се съставя от представители на ОКС и служител по криптографската сигурност на организационната единица – заявител по чл. 16. Комисията се назначава със заповед на ръководителите на ОКС и на организационната единица – заявител по чл. 16.

(3) При проверката по ал. 1 ОКС може да определи допълнителни изисквания по отношение на сигурността, които трябва да бъдат изпълнени преди издаването на решението.

(4) За криптографските мрежи, предназначени за защита на класифицирана информация с ниво на класификация "За служебно ползване", проверката по ал. 1 може да се извършва по документи.

(5) В случай че след издаване на решението по ал. 1 има промяна в условията по чл. 19, ал. 1, т. 1, 3 и 4, ръководителят на организационна единица – заявител, подава допълнение към заявлението по чл. 16, в което се посочват настъпилите промени и предприетите мерки за изпълнението на изискванията на чл. 19, ал. 1, т. 1, 3 и 4.

(6) След подаване на допълнението по ал. 5 ОКС може да изиска извършване на повторна проверка на изпълнението на изискванията по чл. 19.

Чл. 21. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Решението по чл. 20, ал. 1 съдържа описание на изпълнението на изискванията по чл. 19, както следва:

1. идентификация на одобрените криптографски средства, включително маркировката по чл. 72, ал. 1, т. 5 на поекземплярно проверените криптографски средства или техни модули;

2. нивото за сигурност на класифицираната информация, която може да бъде защитавана с одобрените криптографски средства;

3. задължителните условия за експлоатация, при които е гарантирана защитата на класифицираната информация от съответното ниво за сигурност;

4. физическото разположение на криптографските средства по места и предприетите мерки по физическа и документална сигурност.

(2) Решението по ал. 1 и документите по чл. 19 и 20 се съхраняват в делата по чл. 22, ал. 1.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Екземпляр от решението по ал. 1 се изпраща на организационната единица, експлоатираща криптографските средства в мрежа, или на организатора по чл. 23. В случаите, когато криптографската мрежа е част от КИС, решението се изпраща след издаване на сертификат за КИС.

Чл. 22. (1) Органът по криптографската сигурност на Република България води регистър и дела на материалите, свързани с процеса на използване на криптографските средства.

(2) В делата по ал. 1 се съхраняват и документите по чл. 16 и 17.

Чл. 23. (1) (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г., изм., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Когато криптографска мрежа обхваща повече от една организационна единица, между тях се сключва споразумение, определящо коя организационна единица е организатор на мрежата. В органите на държавната власт, в които са обособени повече от една организационни единици, вместо споразумение може да се издаде заповед на съответния компетентен орган на държавната власт.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Организаторът отговаря за разпределението на необходимите криптографски материали в мрежата, а дейностите по поекземплярната проверка, разпределението и ремонта на използваните криптографски средства се организират съгласно споразумението или заповедта по ал. 1.

(3) (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Споразумението или заповедта по ал. 1 се прилага към заявлението по чл. 16 от организатора на криптографската мрежа.

(4) (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Всяка организационна единица изпълнява изискванията по чл. 19 спрямо частта от мрежата, която е в нейна отговорност по споразумението или заповедта по ал. 1.

(5) (Нова - ДВ, бр. 57 от 2009 г., изм., бр. 21 от 2020 г., в сила от 13.03.2020 г.) 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. 24. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Криптографските средства и ключовите материали са с ниво на класификация не по-ниско от нивото на класификация на информацията, за което е одобрено криптографското средство.

Чл. 25. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Класифицирана информация от КИС се пренася по комуникационни системи по реда на Наредбата за сигурността на комуникационните и информационните системи.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Пренасяне по комуникационни системи на класифицирана информация, защитена с криптографски средства, се допуска за ниво на класификация до "Секретно" включително.

(3) Класифицирана информация с ниво за сигурност "Строго секретно" може да се защитава с криптографски средства с ниво за сигурност "Секретно" само в съвкупност с мерки от останалите видове сигурност, съответстващи на ниво за сигурност "Строго секретно".

Раздел II
Експлоатация на криптографски средства

Чл. 26. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Експлоатацията на криптографските средства и на криптографските ключове се извършва в съответствие с правилата за работа с тях и криптоплана по чл. 19, ал. 1, т. 5.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Всички промени в криптоплана по ал. 1 се утвърждават от ОКС.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Експлоатацията по ал. 1 се извършва след издаване на решение по чл. 20, а когато криптографската мрежа е част от КИС – и след издаване на сертификат за сигурност на КИС по реда на Наредбата за сигурността на комуникационните и информационните системи.

Чл. 27. (1) Криптографските средства се експлоатират в условия с осигурени мерки за физическа и документална сигурност, съответстващи на нивото за сигурност на криптографските средства и на класифицираната информация, която ще бъде защитавана.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Експлоатация на новозакупени екземпляри криптографски средства се допуска само след поекземплярната им проверка от ОКС.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Криптографските средства се съхраняват и пренасят с незаредени криптографски ключове.

Чл. 28. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Преди първоначалното използване на ключови материали се извършва проверка на целостта на защитната им опаковка и при съмнения за компрометиране се уведомява служителят по криптографската сигурност.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) По време на експлоатация на криптографските средства ключовите материали се съхраняват по начин, недопускащ нерегламентиран достъп до тях.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Ключовите материали се унищожават след отпадане на необходимостта от тяхното използване по реда, предвиден в криптоплана по чл. 19, ал. 1, т. 5.

Чл. 29. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При необходимост от ремонт на криптографско средство администраторът по криптографската сигурност предприема необходимите действия за недопускане на нерегламентиран достъп до класифицирана информация и ключови материали, съхранявани в предаваното за ремонт средство.

(2) Служителят по криптографската сигурност уведомява писмено ОКС за идентификационните номера на подлежащите на ремонт криптографски средства.

(3) Органът по криптографската сигурност може да изиска повредените

криптографски средства преди изпращането им за ремонт.

(4) Ремонтът се извършва на територията на Република България.

(5) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) След ремонта, преди въвеждане в експлоатация, криптографското средство подлежи на проверка от ОКС за съответствие на криптографската функционалност и конфигурационен контрол.

(6) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Администраторите по криптографската сигурност водят подробен отчет на профилактиките и ремонтите на криптографски средства в криптографската мрежа, за която отговарят.

Чл. 30. При възникване на непоправими повреди криптографските средства се унищожават по реда на чл. 33.

Раздел III
Прекратяване на експлоатацията на криптографски средства

Чл. 31. (1) (Предишен текст на чл. 31 – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Прекратяване на експлоатацията на криптографски средства се извършва:

1. при отпадане на необходимостта от използване на криптографските средства в организационната единица, за което писмено се уведомява ОКС;

2. при установяване на неспособност на експлоатираните криптографски средства да осигуряват необходимото ниво на защита на класифицираната информация, което се удостоверява от ОКС;

3. (нова – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) при компрометиране на криптографската сигурност след издадено писмено становище по чл. 4, т. 11.

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При прекратяване на експлоатацията на криптографски средства в криптографска мрежа по ал. 1, т. 1 заявителят по чл. 16 писмено уведомява ОКС.

Чл. 32. (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) При прекратяване на експлоатацията на криптографските средства по чл. 31 служителят по криптографската сигурност организира съхраняването на тези средства, на ключовите материали за работа с тях и на съпътстващата ги експлоатационна документация или те се унищожават по реда на чл. 33.

Чл. 33. (1) Унищожаването на криптографските средства се извършва от комисия, назначена с писмена заповед на ръководителя на организационната единица.

(2) В комисията по ал. 1 задължително се включват служителят по криптографската сигурност и администратор по криптографската сигурност.

(3) (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Комисията унищожава и всички неизползвани криптографски ключове, предназначени за средствата по ал. 1, както и съпътстващата ги експлоатационна документация.

(4) (Изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Унищожаването на криптографските средства и ключовите материали се извършва по начин, недопускащ компрометиране на криптографската сигурност.

(5) (Изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) За унищожаването по ал. 3 се изготвя протокол.

(6) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В срок до 12 месеца от унищожаването в ОКС се изпраща списък на унищожените средства и материалите по ал. 3.

(7) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) След унищожаване на всички криптографски средства и материали от конкретна криптографска мрежа и анализ на списъка по чл. 33, ал. 6 ОКС прекратява експлоатацията на криптографската мрежа, като уведомява писмено ръководителя на организационната единица – заявител по чл. 16.

Раздел IV
Производство, маркиране, съхраняване, разпределяне, пренасяне и използване на ключови материали
(Загл. изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.)

Чл. 34. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Производството и разпределянето на ключови материали за криптографските мрежи на Република България се извършва от ОКС или от организационните единици при условията на чл. 35 и 36.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Ключовите материали се обозначават с име, пореден номер, екземплярен номер и ниво за сигурност на информацията, съдържаща се в тях, и допълнителна маркировка "КРИПТО". Когато са в обща защитна опаковка, отделните елементи на ключовия материал могат да не съдържат всички обозначения от опаковката.

Чл. 35. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В организационните единици могат да се експлоатират системи за управление на криптографски ключове (СУКК) при следните условия:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) системата за управление на криптографски ключове да е одобрена от ОКС;

2. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) системата за управление на криптографски ключове да бъде обособена в зона за сигурност и да са осигурени мерките за физическа и документална сигурност за ниво на класификация не по-ниско от нивото на класификация на произвежданите криптографски ключове, което се удостоверява със съответния документ;

3. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) да са изпълнени условията за експлоатация на СУКК, определени в нейния сертификат за одобрение;

4. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) да има служител или администратор по криптографската сигурност, обучен за работа със СУКК от ОКС или от доставчика.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Въвеждането в експлоатация на СУКК се извършва по реда на чл. 20 с решение на комисия след проверка на изпълнението на изискванията по ал. 1, а когато са част от КИС – след издаване на сертификат за сигурност на КИС по чл. 20 от Наредбата за сигурността на комуникационните и информационните системи.

(3) (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

Чл. 36. (1) (Изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Съхраняването и разпределянето на криптографските материали се извършват в криптографска регистратура, която е част от регистратурата на организационната единица по чл. 51, ал. 1 от Правилника за прилагане на Закона за защита на класифицираната информация (ППЗЗКИ), или в отделна регистратура, създадена на основание чл. 51, ал. 3 от същия правилник. Криптографската регистратура трябва да бъде обособена в зона за сигурност.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Ръководителят на организационната единица определя служител - завеждащ криптографската регистратура, и негов заместник, които трябва да притежават удостоверение по чл. 54. Завеждащият криптографската регистратура води на отчет, съхранява и разпределя криптографските материали. В негово отсъствие тези функции се изпълняват от заместника. Завеждащият криптографската регистратура (в негово отсъствие - заместникът) е отговорен за опазването от нерегламентиран достъп на криптографските материали в криптографската регистратура.

(3) (Изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) В регистратурите по чл. 51, ал. 1 ППЗЗКИ криптографските материали се съхраняват в отделни каси.

(4) (Изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Отчитането на криптографските материали се извършва в отделни регистри.

(5) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Пренасянето на криптографските материали се извършва по реда за пренасяне на материали, съдържащи класифицирана информация, регламентиран в ППЗЗКИ. Подателят поставя върху

вътрешната опаковка на пакетите надпис: "Да се отвори от завеждащия криптографската регистратура!". Получателят на материалите потвърждава писмено получаването и сигнализира за открити несъответствия в опаковката или съдържанието на пакетите, ако са констатирани такива. Потвърдителните писма се съхраняват за периода на съхраняване на съпроводителните писма на криптографските материали.

(6) (Изм. и доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Служителят по криптографската сигурност организира периодично, но най-малко веднъж годишно, както и при смяна на завеждащия криптографската регистратура инвентаризация на използваните в организационната единица криптографски средства и криптографски материали. За резултатите от инвентаризацията служителят по криптографската сигурност изготвя обобщен отчет, който предоставя на служителя по сигурността на информацията. Обобщеният отчет е с класификационно ниво за сигурност не по-ниско от "Поверително". Копие на обобщения отчет се изпраща на ОКС.

Раздел V
Контрол по използването на криптографските средства

Чл. 37. (1) Контролът по използването на криптографските средства се осъществява от ОКС и от служителите и администраторите по криптографската сигурност.

(2) (Изм. – ДВ, бр. 27 от 2016 г., в сила от 5.04.2016 г., доп., бр. 21 от 2020 г., в сила от 13.03.2020 г.) В Държавна агенция "Разузнаване" и в служба "Военна информация" към министъра на отбраната ОКС осъществява контрола по ал. 1 чрез техните структури по сигурността, с изключение на случаите по чл. 43, ал. 5.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) На контрол подлежат организацията, начинът и условията на използване, съхраняване и унищожаване на криптографските средства и криптографските материали.

(4) Контролът се осъществява чрез проверки от ОКС в организационните единици.

Чл. 38. (1) Преди извършване на проверката по чл. 37, ал. 4 ОКС писмено уведомява ръководителя на организационната единица.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Проверката се извършва от комисия, съставена от служители на ОКС, определени със заповед на неговия ръководител. В службите по чл. 37, ал. 2 проверката се извършва от комисия, съставена от служители от съответните структури по сигурността, с изключение на случаите по чл. 43, ал. 5.

(3) Комисията извършва проверката съвместно със служителя по криптографската сигурност и други служители от административното звено по сигурността на организационната единица.

(4) При осъществяване на проверката комисията има право на достъп до обекти,

помещения и материали, свързани с криптографската сигурност.

(5) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Редът за достъпа по ал. 4 се определя със заповед на ръководителя на организационната единица.

(6) За резултатите от проверката се съставя протокол в два екземпляра - един за ОКС и един за организационната единица.

(7) В случай на констатирани нарушения използването на криптографските средства се прекратява до отстраняването им, което се посочва в протокола по ал. 6.

Чл. 39. Служителите и администраторите по криптографската сигурност осъществяват текущ контрол по използването на криптографските средства в съответствие с възложените им с наредбата и от ръководителя на организационната единица функции.

Раздел VI
Използване на криптографските средства в сложни условия

Чл. 40. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За въвеждане в експлоатация на криптографски мрежи в сложни условия организационните единици изготвят криптоплан, съответстващ на изискванията по чл. 19.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Криптопланът по ал. 1 се утвърждава от ръководителя на ОКС или от упълномощено от него длъжностно лице.

Чл. 41. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Въвеждането в експлоатация на криптографски мрежи, действащи в сложни условия, се извършва въз основа на заповед на ръководителя на организационната единица или на упълномощено от него длъжностно лице и под контрола на служителя по криптографската сигурност на организационната единица.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В заповедта по ал. 1 се изписва периодът, за който се въвежда в експлоатация криптографската мрежа. Копие от заповедта се изпраща в ОКС.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За периода, през който криптографската мрежа не е въведена в експлоатация, криптографските средства и криптографските материали се съхраняват по реда на криптоплана.

(4) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Когато действащата в сложни условия криптографска мрежа е част от КИС, заповедта за въвеждане на мрежата в експлоатация се издава след получаване на сертификат за сигурност на КИС по реда на Наредбата за сигурността на комуникационните и информационните системи.

Раздел VII
Действия при компрометиране на криптографската сигурност

Чл. 42. (1) При съмнения за компрометиране или при компрометиране на криптографската сигурност служителят по сигурността на информацията в организационната единица:

1. взема мерки за предотвратяване или ограничаване на вредните последствия;

2. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) незабавно информира ОКС и организационната единица – организатор на криптографската мрежа, ако събитието се е случило в различна от нея организационна единица.

(2) Информацията по ал. 1, т. 2 е с ниво на класификация не по-ниско от нивото на класификация на криптографското средство.

Чл. 43. (1) По предложение на служителя по сигурността на информацията ръководителят на организационната единица назначава комисия за установяване на обстоятелствата, свързани с компрометирането на криптографската сигурност.

(2) В комисията по ал. 1 задължително се включват служителят и администраторът по криптографската сигурност.

(3) Резултатите от работата на комисията се отразяват в протокол, който включва всички установени обстоятелства и заключения.

(4) Протоколът по ал. 3 се предоставя на ръководителя на организационната единица, а копие от него се изпраща в ОКС.

(5) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Органът по криптографската сигурност може да извърши отделна проверка по случая, ако установените в протокола по ал. 3 обстоятелства го налагат. Проверката се извършва по реда на чл. 37 и 38.

Чл. 44. (1) Въз основа на протокола по чл. 43, ал. 3 ОКС изготвя писмено становище, което се изпраща до ДКСИ и до организационната единица.

(2) В случай че компрометирането на криптографската сигурност засяга криптографски мрежи, в които се обработва информация на други държави или международни организации, те се информират в съответствие с двустранните договорености по сигурността.

Чл. 44а. (Нов – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) При съмнение за или установяване на нерегламентиран достъп до информация за криптографско средство за защита на класифицирана информация в процес на разработка в Република България

разработчикът по чл. 83 незабавно информира ОКС.

(2) В случаите по ал. 1 ОКС определя необходимите мерки за минимизиране на възможните вредни последици от това събитие и контролира изпълнението им.

Глава четвърта
ИЗДАВАНЕ НА РАЗРЕШЕНИЯ И УДОСТОВЕРЕНИЯ ЗА РАБОТА С КРИПТОГРАФСКИ СРЕДСТВА И ОБУЧЕНИЕ ПО КРИПТОГРАФСКА СИГУРНОСТ

Раздел I
Разрешения за работа с криптографски средства

Чл. 45. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Разрешение за работа с криптографски средства се издава от ОКС на служител в организационната единица, определен да изпълнява задълженията на служител по криптографската сигурност:

1. на когото е извършено проучване по чл. 46, т. 3 ЗЗКИ и е издадено разрешение за достъп до класифицирана информация с ниво на класификация "Строго секретно";

2. който е преминал успешно обучение по чл. 88, ал. 1 ЗЗКИ в ОКС и има издадено свидетелство по чл. 66;

3. на когото не е отнето разрешението за работа с криптографски средства.

Чл. 46. (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За обучение и издаване на разрешение по чл. 45 ръководителят на организационната единица подава заявление до ръководителя на ОКС, в което се посочват:

1. трите имена и единният граждански номер на служителя по чл. 45;

2. организационната единица, в която работи служителят;

3. номерът и датата на разрешението за достъп до класифицирана информация с ниво на класификация "Строго секретно", както и органът, който го е издал;

4. (отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

Чл. 47. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Разрешението за работа с криптографски средства се издава от ръководителя на ОКС или от упълномощено от него длъжностно лице след преминато успешно обучение по чл. 88, ал. 1 от ЗЗКИ в ОКС.

(2) Разрешението по ал. 1 се издава в два екземпляра.

(3) Екземпляр от разрешението по ал. 1 се изпраща на ръководителя на организационната единица.

Чл. 48. Разрешението за работа с криптографски средства съдържа:

1. регистрационен номер;

2. правното основание за издаване на разрешението;

3. органа, издал документа;

4. име, презиме, фамилия и единен граждански номер на лицето, на което се издава;

5. организационната единица, в която лицето работи;

6. срока на валидност на разрешението;

7. дата и място на издаването;

8. подпис и печат.

Чл. 49. (1) Разрешението за работа с криптографски средства се издава за срок 5 години.

(2) Не по-късно от 3 месеца преди изтичане на срока на разрешението по ал. 1 ръководителят на организационната единица започва процедура по реда на чл. 46 за издаване на ново разрешение.

Чл. 50. (1) Органът по криптографската сигурност отнема разрешението за работа с криптографски средства по писмено предложение на служителя по сигурността на информацията, когато:

1. лицето е извършило нарушение, което е довело до компрометиране на криптографската сигурност;

2. лицето е извършило системни нарушения, които са създали опасност от компрометиране на криптографската сигурност;

3. е отнето разрешението за достъп до класифицирана информация с ниво на класификация "Строго секретно".

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В случаите по ал. 1, т. 1 ОКС може да отнеме разрешението за работа с криптографски средства без писмено предложение на служителя по сигурността на информацията.

(3) (Предишна ал. 2 – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Отнемането на разрешението се извършва с писмен акт.

Чл. 51. (1) Органът по криптографската сигурност прекратява действието на разрешението за работа с криптографски средства по писмено предложение на служителя по сигурността на информацията при:

1. изтичане на неговия срок на валидност;

2. прекратяване на действието на разрешението за достъп до класифицирана информация с ниво на класификация "Строго секретно";

3. преустановяване изпълнението на задълженията на служител по криптографската сигурност.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Прекратяването на разрешението се извършва с писмен акт, с изключение на случаите по ал. 1, т. 1.

Чл. 52. (1) Органът по криптографската сигурност писмено уведомява ръководителя на организационната единица за отнемането или прекратяването на действието на разрешението за работа с криптографски средства.

(2) След уведомлението по ал. 1 организационната единица връща разрешението за работа с криптографски средства в ОКС.

Чл. 53. Органът по криптографската сигурност води регистър на издадените разрешения за работа с криптографски средства и съхранява съпровождащата ги преписка.

Раздел II
Удостоверение за работа с криптографски средства

Чл. 54. (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Удостоверение за работа с криптографски средства, наричано по-нататък "удостоверение", се издава на служител в организационната единица, определен да изпълнява задълженията на администратор по криптографската сигурност, завеждащ криптографска регистратура, или потребител на криптографски средства:

1. на когото е извършено проучване и е издадено разрешение за достъп до класифицирана информация с ниво на класификация:

а) (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) за администратор по криптографската сигурност и завеждащ криптографска регистратура - не по-ниско от нивото на класификация на криптографските средства и ключовите материали, с които ще работи, в зависимост от броя на обслужваните криптографски мрежи, но не по-ниско от "Поверително";

б) за потребител на криптографското средство - съответстващо на нивото на класификация на информацията, до която ще има достъп по силата на служебните си задължения;

2. (изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) който има издадено свидетелство по реда на тази наредба за успешно преминато обучение по чл. 62 и документ, издаден по чл. 64, ал. 2, ако обучението по чл. 62, т. 2 е извършено от доставчици или производители на криптографски средства;

3. на когото не е отнето удостоверението за работа с криптографски средства.

Чл. 55. (1) Удостоверението за работа с криптографски средства се издава от служителя по криптографската сигурност по образец съгласно приложение № 1.

(2) Съхраняването на удостоверението по ал. 1 се организира от служителя по криптографската сигурност.

Чл. 56. (1) Удостоверението за работа с криптографски средства съдържа:

1. регистрационен номер;

2. правното основание за издаването;

3. органа, издал документа;

4. име, презиме, фамилия и единен граждански номер на лицето, на което се издава;

5. функции, които изпълнява лицето във връзка с криптографската сигурност;

6. наименование на криптографската мрежа, в която лицето изпълнява функциите;

7. организационната единица, в която работи лицето;

8. криптографското средство, за което се издава, или правото за работа с криптографски материали, когато удостоверението е на завеждащ криптографска регистратура;

9. срок на валидност на удостоверението;

10. дата и място на издаването;

11. подпис и печат.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Екземпляр от удостоверението на администраторите по криптографската сигурност и завеждащите криптографска регистратура се изпраща в ОКС.

(3) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Органът по криптографската сигурност води регистър на издадените удостоверения за работа с криптографски средства на администраторите по криптографската сигурност и завеждащите криптографска регистратура.

Чл. 57. (1) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Удостоверението за работа с криптографски средства се издава за срок до 5 години.

(2) Преди изтичането на срока на удостоверението служителите преминават курс на обучение за издаване на ново удостоверение.

Чл. 58. (1) Служителят по криптографската сигурност отнема удостоверението за работа с криптографски средства, когато:

1. лицето е извършило нарушение, което е довело до компрометиране на криптографската сигурност;

2. лицето е извършило системни нарушения, които са създали опасност от компрометиране на криптографската сигурност;

3. е отнето разрешението за достъп до класифицирана информация.

(2) Отнемането на удостоверението се извършва с писмен акт съгласно приложение № 2.

Чл. 59. (1) Служителят по криптографската сигурност прекратява действието на удостоверението за работа с криптографски средства при:

1. изтичане на неговия срок на валидност;

2. прекратяване действието на разрешението за достъп до класифицирана информация;

3. преустановяване изпълнението на задълженията на администратор по криптографската сигурност или потребител на криптографски средства.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Прекратяването на удостоверението се извършва с писмен акт съгласно приложение № 3, с изключение на случаите по ал. 1, т. 1.

Чл. 60. Служителят по криптографската сигурност уведомява писмено ОКС за прекратените или отнетите удостоверения на администраторите по криптографската сигурност.

Чл. 61. Служителят по криптографската сигурност води регистър на удостоверенията за работа с криптографски средства.

Раздел III
Обучение по криптографска сигурност

Чл. 62. Обучението по криптографска сигурност включва:

1. обучение по организационните принципи и правила за криптографска сигурност;

2. обучение за работа с конкретни криптографски средства.

Чл. 63. Обучението по чл. 62, т. 1 се извършва от:

1. органа по криптографската сигурност - на служителите по криптографската сигурност;

2. органа по криптографската сигурност или от служителите по криптографската сигурност - на администраторите по криптографската сигурност;

3. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) служителите или администраторите по криптографската сигурност - на други администратори по криптографската сигурност, на завеждащите криптографска регистратура и на потребителите на криптографски средства.

Чл. 64. (1) (Предишен текст на чл. 64 - ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Обучението по чл. 62, т. 2 се извършва от:

1. доставчици или производители на криптографски средства;

2. служители на ОКС, служители и администратори по криптографската сигурност, на които доставчикът или производителят е дал право да провеждат обучение.

(2) (Нова – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) На служителите от организационните единици, преминали успешно обучение по ал. 1, т. 1, доставчиците или производителите на криптографски средства издават документ, в който се посочва:

1. видът на криптографското средство, за което е проведено обучението;

2. правото за провеждане на обучение, ако такова е дадено.

Чл. 65. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Обучението по криптографска сигурност се провежда с откъсване от работа в съгласувани с организационната единица срокове.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Органът по криптографската сигурност и служителите от организационните единици, на които им е дадено право да провеждат обучение, извършват периодично допълнително обучение по криптографска

сигурност.

Чл. 66. (1) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Служителите и администраторите по криптографската сигурност, успешно преминали обучението в ОКС, получават свидетелство, издадено от ръководителя на ОКС или упълномощено от него длъжностно лице.

(2) В свидетелството по ал. 1 се отбелязва правото за провеждане на обучение, ако такова е дадено.

(3) Свидетелството по ал. 1 се издава за срок не по-дълъг от 5 години.

Чл. 67. (1) Администраторите по криптографската сигурност и потребителите на криптографски средства, успешно преминали обучението в организационната единица, получават свидетелство съгласно приложение № 4.

(2) В свидетелството по ал. 1 за администраторите по криптографската сигурност се отбелязва правото за провеждане на обучение, ако такова е дадено.

(3) Свидетелството по ал. 1 се издава за срок не по-дълъг от 5 години.

(4) Към свидетелството могат да се приложат данни за оценките, получени при обучението.

Чл. 68. (1) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Обучение на администратори по криптографската сигурност на завеждащите криптографска регистратура и на потребители на криптографски средства се извършва в организационната единица при наличие на:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) помещения с осигурени мерки за физическа и документална сигурност, удостоверени със съответния документ, удостоверяващ изпълнението на нормативните изисквания за физическа и документална сигурност, съответстващи на нивото за сигурност на криптографските средства;

2. оборудване, средства и учебни материали, необходими за провеждане на обучението;

3. утвърдени от ОКС програми за обучение;

4. (изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) служители по криптографската сигурност, получили право да провеждат обучение по чл. 62, т. 1 или 2;

5. (изм. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) администратори по криптографската сигурност, получили право да провеждат обучение по чл. 62.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При наличие на условията по ал. 1 ръководителят на ОКС или упълномощено от него длъжностно лице издава

разрешение за провеждане на обучение във връзка с чл. 88, ал. 3 ЗЗКИ.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В органите на държавната власт, в които са обособени повече от една организационни единици, може да се създават учебни центрове за провеждане на обучението по ал. 1.

(4) Контролът върху условията и процеса на обучение се извършва от ОКС по реда на чл. 37 и 38.

Глава пета
ОДОБРЕНИЕ ЗА ПРИЛАГАНЕ НА КРИПТОГРАФСКИ СРЕДСТВА

Раздел I
Общи условия и ред за одобрение на криптографски средства

Чл. 69. Одобрение на криптографско средство за защита на класифицирана информация може да иска:

1. лице, което е регистрирано по Търговския закон на Република България и е с над 50 на сто българско участие;

2. организационна единица, ако тя е производител на криптографското средство.

Чл. 70. (1) (Предишен текст на чл. 70 – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Лицето или организационната единица по чл. 69, наричани по-нататък "заявителя", подава до ръководителя на ОКС заявление за одобрение на криптографско средство за защита на класифицирана информация, наричано по-нататък "одобрение".

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Одобрение може да бъде искано и извършено само за средство с напълно приключил етап на разработка и функционални изпитания, от което има произведени образци в напълно завършен вид.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Системата за управление на криптографски ключове за криптографско средство, когато не е неразделна част от него, а е обособена самостоятелно, се одобрява:

1. отделно като криптографско средство и се открива процедура по нейното одобрение преди или едновременно с процедурата по одобрението на криптографското средство, което ще я ползва;

2. като задължително условие за одобрението на криптографското средство, което ще я ползва.

Чл. 71. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Процедура за одобрение се открива с подаване на заявлението по чл. 70, което съдържа:

1. име и седалище на заявителя и адрес за кореспонденция;

2. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) название и пълно типово означение на криптографското средство, включително версиите на софтуера и фърмуера;

3. предназначение на криптографското средство и ниво на сигурност, за което ще се използва;

4. име и седалище на производителя и адрес за кореспонденция.

(2) Към заявлението се прилагат и:

1. пълна документация (включително блокови, електрически, монтажни схеми, изходен код на програмите) на криптографското средство, която съдържа изчерпателна информация, позволяваща проверката на:

а) (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) използваните криптографски алгоритми, начините за тяхното прилагане (инициализация, режими на работа, формати на входящите и изходящите данни и др.);

б) криптографските ключове, начините за генерирането им, включително тестовете за проверка на качествата на случайните поредици, начините и форматите за разпределянето, съхраняването и защитата им;

в) техническия контрол на достъпа до криптографското средство;

г) блокировките и сигнализацията при неизправна работа на криптографското средство или неправилна работа с него;

д) (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) мерките по защита от компрометиращи електромагнитни излъчвания и филтриране на захранващите линии, както и информация за всички входни и изходни интерфейси (описание на сигналите – аналогови и цифрови, минимална и максимална скорост на предаване);

е) (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) пълно описание на начините за използването му (включително изходни кодове на програми), ако то е част от КИС;

ж) (нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) мерките за безвъзвратно унищожаване на криптографските алгоритми и ключови материали при неоторизиран достъп;

з) (нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) форматите на входящите и изходящите данни, обменяни през комуникационната среда;

2. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) описание на възможни методи за извършване на проверките по т. 1 и при наличност – резултати от извършени тестове и анализи в процеса на разработка и производство;

3. инструкции за експлоатация, изисквания за сигурност при експлоатацията и при генериране и управление на криптографските ключове;

4. необходимият брой действащи образци от криптографското средство, включително ключови и други материали, необходими за експлоатация на средството, както и средство за генериране на ключове, ако е обособено отделно;

5. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) документи, удостоверяващи изпълнението на изискванията за безопасност и за опазване на околната среда, техническите параметри и електромагнитната съвместимост на криптографското средство и други стандарти;

6. писмена декларация на заявителя, че:

а) в криптографското средство не са реализирани допълнителни функции, неописани в предоставената документация;

б) ще осигури пълно съответствие на функционалните и техническите параметри с тези на предоставените по т. 4 образци на криптографското средство;

в) ще осигури гаранционно и следгаранционно обслужване на територията на Република България при изпълнени мерки за индустриална сигурност, съответстващи на нивото на класификация за сигурност на криптографското средство.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Когато заявлението е подадено от лице по чл. 69, т. 1, към него се прилагат и:

1. удостоверения за липса на вписано обстоятелство или обявен акт в търговския регистър и регистъра на ЮЛНЦ за производство по ликвидация и за производство по несъстоятелност;

2. удостоверение за актуално състояние на регистрирано в търговския регистър и регистъра на ЮЛНЦ лице/копие от регистрационно удостоверение на вписано в регистър БУЛСТАТ лице;

3. декларация, че при настъпване на промяна в обстоятелствата по т. 1 и 2 и по чл. 69, т. 1 заявителят уведомява писмено ОКС за промяната в двуседмичен срок от настъпването ѝ.

(4) Материалите по ал. 2, т. 1 - 5 могат да бъдат предоставени на ОКС и от производителя.

(5) Материалите по ал. 2 се предоставят на български или английски език за криптографски средства от внос и на български език за криптографски средства, произведени в Република България.

(6) В процеса на одобрение ОКС може да изиска допълнителна информация и технически средства, необходими за неговото провеждане.

(7) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Когато заявлението не отговаря на изискванията на ал. 1 или не съдържа някое от приложенията към него по ал. 2 – 5, заявителят се уведомява писмено да отстрани пропуските. Ако пропуските не бъдат отстранени в тримесечен срок от датата на уведомяването, процедурата за одобрение се прекратява.

(8) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За криптографско средство, разработено и произведено от ОКС, не се подава заявление по чл. 70, като такова се одобрява по реда на чл. 72, ал. 1.

Чл. 72. (1) (Предишен текст на чл. 72 – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В процеса на одобрение ОКС извършва:

1. проверка на пълнотата на подаденото заявление и на приложената документация;

2. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) проверка на функционалността на предадените образци от криптографското средство;

3. аналитични, програмни и технически криптографски проверки;

4. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) оценка на защитата от компрометиращи електромагнитни излъчвания;

5. маркировка чрез стикери, пломби, печати и други на поекземплярно проверените криптографски средства или техни модули.

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Всички проверки в процеса на одобрение се извършват в помещенията на ОКС.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При обективна невъзможност част от проверките да се осъществят в помещенията на ОКС те могат да бъдат извършени в помещенията на производителя на криптографското средство за сметка на заявителя по чл. 69.

Чл. 73. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За всяко одобрено криптографско средство ОКС издава сертификат за одобрение.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) При наличие на обособена система за управление на криптографски ключове за нея се издава отделен сертификат за одобрение.

(3) В случай на неодобрение на криптографското средство ОКС уведомява писмено заявителя.

Чл. 74. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Сертификатът за одобрение съдържа:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) номер на сертификата;

2. (доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г., изм., бр. 21 от 2020 г., в сила от 13.03.2020 г.) идентификация на криптографското средство, за което се издава, включително версиите на софтуера и фърмуера, които се използват;

3. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) идентификация на притежателя на сертификата;

4. идентификация на производителя на криптографското средство;

5. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) ниво на класификация на информацията, за което е одобрено криптографското средство;

6. дата и място на издаването;

7. подпис на ръководителя на ОКС или на упълномощено от него длъжностно лице и печат.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Към сертификата за одобрение се прилагат условията за валидност, които съдържат:

1. условия за експлоатация на криптографското средство;

2. ограничения за валидността на свидетелството, ако има такива.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) След извършване на анализ по чл. 4, т. 3 и 6 ОКС може да внася промени в условията за валидност към сертификата, като:

1. промените се отразяват чрез издаване на нови условия за валидност към вече издаден сертификат за одобрение;

2. органът по криптографска сигурност определя срок, в който старите условия за валидност остават в действие, след което влизат в сила новите условия за валидност.

(4) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В случаите по ал. 3 ОКС незабавно информира писмено притежателя на сертификата за одобрение и организационните единици, в които се експлоатира криптографското средство.

(5) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В едномесечен срок от изтичането на срока по ал. 3, т. 2 притежателят на сертификата за одобрение е длъжен да върне на ОКС старите условия за валидност.

Чл. 75. (1) Органът по криптографската сигурност води регистър на одобрените криптографски средства и дела с материалите, свързани с процеса на одобрение.

(2) (Доп. – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) Делата по ал. 1 се съхраняват за срок, не по-малък от 5 години, след снемане от експлоатация на криптографското средство.

Чл. 76. След одобрение на криптографското средство ОКС:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) връща на заявителя системата за управление на криптографските ключове, ако такава е била приложена за целите на проверките в процеса на одобрение и същата не е част от одобреното средство;

2. съхранява образец от криптографското средство като еталон до прекратяване на експлоатацията му;

3. (нова – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) съхранява образец от всяко друго обособено устройство, необходимо за функционирането на криптографското средство, като еталон до прекратяване на експлоатацията му.

Чл. 77. При неодобрение на криптографското средство ОКС връща средствата и материалите по чл. 71, ал. 2, т. 4.

Чл. 78. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Валидността на сертификата по чл. 73, ал. 1 се прекратява при:

1. установяване от ОКС на неспособност на одобреното криптографско средство да осигури нивото на защита на класифицираната информация, за което е одобрено. В този случай ОКС може да издаде сертификат за по-ниско ниво на класификация на информацията, без да се подава заявление за одобрение;

2. настъпване на обстоятелство, неотговарящо на изискванията по чл. 69, т. 1.

(2) (Изм. и доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В случаите по ал. 1 ОКС уведомява организационните единици, в които се експлоатира криптографското средство, и притежателя на сертификата за одобрение и му предоставя новия сертификат, ако такъв е издаден.

Чл. 79. (1) (Предишен текст на чл. 79 – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Модификациите на криптографското средство подлежат на одобрение по реда на този раздел.

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Обновяване на софтуер и/или

фърмуер, използван в одобрено криптографско средство, се извършва при условия и по ред, определени от ОКС за всеки конкретен случай. Допуска се обновяване без последващо одобрение само и единствено ако обновяването не води до промяна на криптографските характеристики на средството и не намалява сигурността.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Размножаване на софтуер и/или фърмуер, който е част от одобрено криптографско средство, може да се извършва само при условия и по ред, определени от ОКС за всеки конкретен случай.

Раздел II
Допълнителни условия за одобрение на криптографски средства от внос

Чл. 80. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) (1) Криптографски средства от внос могат да се одобряват за защита на класифицирана информация с ниво на класификация до:

1. "Поверително" включително;

2. "Секретно" включително, в случай че са произведени в държава, с която има влязъл в сила международен договор, по който Република България е страна, за защита на класифицирана информация, и са одобрени за защита на нейна информация със съответно или по-високо ниво на класификация.

(2) Криптографски средства, предназначени за защита на информация с ниво на класификация "Поверително" и по-високо, могат да се одобряват само ако криптографският алгоритъм за защита на поверителността на данните е реализиран в хардуерен криптомодул и е предвидена възможност за модификацията му без участие на фирмата производител. Одобрените криптографски средства се експлоатират само с модифициран от ОКС криптографски алгоритъм.

Чл. 81. (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

Чл. 82. В случай че заявителят разполага със сертификати или други подобни документи, издадени за криптографското средство, той прилага копие от тях към заявлението по чл. 70.

Раздел III
Допълнителни условия за одобрение на криптографски средства, които се проектират и произвеждат в Република България

Чл. 83. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Преди разработка на

криптографско средство за защита на класифицирана информация разработчикът писмено уведомява ОКС.

(2) (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Към уведомлението разработчикът прилага:

1. (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) основание за разработката; работни название и типово означение на криптографското средство – предмет на разработката; описание на функционалните характеристики на криптографското средство, включително предвижданото ниво на класификация на информацията, която ще защитава; описание на предвижданата среда на работа и условия на експлоатация на криптографското средство;

2. (доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) пълна информация за възложителя на разработката и условията на договора по възлагане, ако има такъв, списък на служителите, участващи в разработката, и идентификационните данни на техните разрешения за достъп до класифицирана информация с ниво на класификация, съответно на заявеното по т. 1;

3. идентификационните данни на удостоверението за сигурност по чл. 96, ал. 1 ЗЗКИ - за лицата по чл. 69, т. 1.

Чл. 84. В случай че разработката се възлага от организационна единица, заданието предварително се съгласува с ОКС.

Чл. 85. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Органът по криптографската сигурност въз основа на уведомлението по чл. 83 предоставя на разработчика задължителни изисквания за криптографска сигурност, на които трябва да отговаря криптографското средство.

Чл. 86. (1) (Предишен текст на чл. 86, изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) По време на разработката ОКС обменя информация с разработчика и при необходимост поставя допълнителни изисквания към криптографското средство.

(2) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Предвидените за използване криптографски алгоритми и начините за тяхното прилагане се одобряват задължително от ОКС.

(3) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Критично важни параметри и криптографски алгоритми се залагат в криптографското средство при условия и по ред, определени от ОКС за всеки конкретен случай.

(4) (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Органът по криптографската сигурност на Република България предоставя изисквания и техническа информация, свързана с разработката, единствено на лицата по чл. 83, ал. 3, т. 2 при спазване на

принципа "необходимост да се знае".

Чл. 87. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) След приключване на разработката разработчикът уведомява писмено за това ОКС, като декларира съответствието на крайния резултат с изискванията на ОКС.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Освен приложенията по чл. 71 лицето по чл. 69, т. 1 прилага към заявлението за одобрение по чл. 70 писмена декларация за възможността да осигури цялостното производство на модулите, реализиращи криптографските функции на територията на Република България.

(3) Одобрението се извършва по реда на раздел I.

Чл. 88. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В случай че в процеса на одобрение се открият недостатъци в криптографските и функционалните характеристики на одобряваното средство, ОКС преценява при какви условия тяхното отстраняване е допустимо в рамките на текущата процедура по одобрение. Органът по криптографската сигурност на Република България писмено информира заявителя за решението си и в случай че промените са допустими, определя срок, в който недостатъците трябва да бъдат отстранени.

(2) (Доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) В случай че отстраняването на установени недостатъци не е допустимо в рамките на текущата процедура по одобрение или заявителят не отстрани недостатъците в указания срок, ОКС прекратява процеса на одобрение.

Чл. 89. Органът по криптографската сигурност осъществява контрол върху процеса на разработка и производство на криптографски средства.

Чл. 90. (1) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Разработчикът няма право да предоставя на други физически или юридически лица информация за предоставени от ОКС в процеса на разработка криптографски алгоритми и модули.

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Разработчикът няма право да прилага предоставени от ОКС в процеса на разработка криптографски алгоритми и модули или техни разновидности във вариантите на криптографското средство, които не са предназначени за защита на класифицирана информация на Република България или на държави и организации, с които Република България има влязъл в сила международен договор за защита на класифицирана информация.

(3) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) Износът на криптографско средство се извършва след становище от ОКС.

(4) (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. (1) (Изм. - ДВ, бр. 5 от 2010 г., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Планирането, организацията, изграждането, ръководството и контролът на криптографската сигурност на Върховното главно командване за военно време се възлагат на Министерството на отбраната (МО) и на дирекция "Комуникационни и информационни системи" на Министерството на вътрешните работи (МВР).

(2) (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) За изпълнение на функциите и задачите по ал. 1 ръководителите на министерствата и ведомствата изготвят необходимите документи за криптографските мрежи на Върховното главно командване, които се съгласуват с МО.

(3) (Изм. - ДВ, бр. 5 от 2010 г., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Комуникациите за държавно управление от пунктовете на Върховното главно командване и пунктовете за управление на министерствата и ведомствата се планират съвместно от МО и дирекция "Комуникационни и информационни системи" – МВР. Ръководството, организацията, експлоатацията и контролът на комуникациите се осъществяват от дирекция "Комуникационни и информационни системи" – МВР.

(4) (Изм. - ДВ, бр. 5 от 2010 г., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Защитата с криптографски средства на комуникационните и информационните системи, необходими за държавното ръководство, министерствата и ведомствата, се организира, осъществява и експлоатира от дирекция "Комуникационни и информационни системи" - МВР.

(5) (Изм. - ДВ, бр. 5 от 2010 г., бр. 21 от 2020 г., в сила от 13.03.2020 г.) Защитата с криптографски средства на комуникационните и информационните системи за пунктовете за управление на министерствата и ведомствата се планира съвместно от МО и дирекция "Комуникационни и информационни системи" - МВР. Ръководството, организацията и експлоатацията им се осъществяват от дирекция "Комуникационни и информационни системи" - МВР.

§ 2. (Отм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.).

§ 2а. (Нов – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) На криптографските средства и криптографските материали се поставя допълнителна маркировка "КРИПТО".

§ 3. По смисъла на наредбата:

1. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографска защита" е прилагането на криптографски методи и средства с цел защита на свойствата на класифицираната информация, свързани с контрола на достъпа до нея, като поверителност, цялост и други, при нейното обработване, съхраняване, пренасяне и използване.

1а. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографска трансформация" е обработка на информация с цел нейната защита от неоторизиран достъп.

1б. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографски алгоритъм" е

параметризирана фамилия криптографски трансформации.

1в. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографски ключ" е параметърът на криптографския алгоритъм, определящ еднозначно криптографската трансформация и подлежащ на периодична смяна.

1г. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Шифър" е еквивалентно понятие на "криптографски алгоритъм".

1д. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографски метод" е метод за защита на класифицирана информация чрез криптографска трансформация.

2. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографско средство" е средство, предназначено за защита на класифицирана информация чрез комбинация от криптографски методи, или средство за управление на криптографски ключове.

2а. (Нова – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Управление на криптографски ключове" е всяка дейност, свързана с осигуряването на пълната функционалност и защита на криптографските ключове през целия им жизнен цикъл, в това число тяхното генериране, запис, маркиране, съхранение, разпределение, пренос, използване и унищожение.

3. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Ключови материали" са криптографски ключове, пароли, инициализиращи стойности и други, свързани с криптографската защита параметри, записани на различни материални носители.

4. "Криптографска мрежа" е съвкупност от съвместими, одобрени криптографски средства с общо администриране на ключовите материали, осигуряваща криптографска защита на обменяната класифицирана информация.

5. "Компрометиране на криптографската сигурност" е събитие, което създава условия за или е довело до нерегламентиран достъп до криптографските средства и ключови материали или до обработваната с тях класифицирана информация. Такива събития могат да бъдат:

а) (изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) криптографски: нерегламентиран достъп до самите криптографски средства или ключови материали, включително до информация за криптографско средство за защита на класифицирана информация в процес на разработка в Република България; неизправна работа на криптографското средство; неправилна работа с криптографското средство или с ключовите материали (нарушена опаковка, дефектен, подменен или повторно използван ключов материал, използване на криптографския ключ извън разрешения период, неразрешено използване на собствено изработени ключове, смяна на поредността на ключовете и др.); използване на криптографското средство от неоторизиран персонал; използване на незащитени комуникационни канали за детайлно изясняване на повреда на криптографско средство; неоторизирана модификация на криптографското средство;

б) персонални: действия или обстоятелства, свързани с лица, получили разрешение или удостоверение за работа с криптографски средства, които биха изложили на опасност криптографската сигурност (измяна, саботаж, разгласяване на информация, свързана с криптографските средства и ключовите материали);

в) физически: кражба, загубване, неправилно транспортиране (грешен получател или използване на непозволени транспортни канали за разпределяне, неправилно пакетиране или нарушена опаковка на пакета); неправилно унищожаване, позволяващо възстановяване на ключовата информация, неконтролирано съхраняване с възможност за неоторизиран достъп до ключов материал; съхраняване на ключови материали или средства, описани като унищожени; необясними повреди или премахване на защитната опаковка на криптографския ключ; опити за извличане на ключ от криптографското средство (активиране на защитни блокировки, неоторизирано изтриване на ключовете).

6. "Кодови пособия" са криптографски средства на хартиен носител, осигуряващи преобразуване на класифицираната информация с помощта на таблични заместания.

7. (Изм. и доп. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Критична ситуация" е ситуация, настъпила в резултат на всяко събитие, което може да доведе или е довело до компрометиране на криптографската сигурност.

8. (Изм. – ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Сложни условия" са специфични условия на експлоатация на криптографските мрежи, създаващи повишен риск за криптографската сигурност и/или затрудняващи прилагането на всички необходими мерки за сигурност.

9. (Нова – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г., изм., бр. 21 от 2020 г., в сила от 13.03.2020 г.) "Криптографски материали" са ключовите материали и други материали, свързани с криптографската функционалност и нейното прилагане.

10. (Нова – ДВ, бр. 35 от 2016 г., в сила от 10.05.2016 г.) "КРИПТО" е допълнителна маркировка в добавка към нивото на класификацията за сигурност, която се поставя с цел спазване и контрол на прилаганите мерки за сигурност, разписани в тази наредба.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 4. (1) Криптографски средства и криптографски мрежи, които към момента на влизане в сила на наредбата се ползват за защита на класифицирана информация, се считат за одобрени за срок 24 месеца, след което подлежат на одобрение по реда на наредбата.

(2) В срок два месеца от влизането в сила на наредбата ръководителите на организационните единици уведомяват писмено ОКС за експлоатираните криптографски мрежи и за типа и броя на криптографски средства в тях.

(3) Заявления за въвеждане в експлоатация на криптографските мрежи по ал. 2 и за одобрение на криптографските средства по ал. 2 се подават не по-късно от 6 месеца от

влизането в сила на наредбата.

§ 5. (1) Издадените преди влизането в сила на наредбата допуски до шифрова работа са валидни до издаване на разрешения и удостоверения за работа с криптографски средства за срок не по-дълъг от 24 месеца от влизането в сила на наредбата.

(2) В срок два месеца от изтичането на срока по ал. 1 издадените допуски до шифрова работа се връщат в ОКС.

§ 6. В срок две години от влизането в сила на наредбата ОКС организира и осигурява изпълнението на чл. 14, ал. 3.

§ 7. Наредбата се приема на основание чл. 85 от Закона за защита на класифицираната информация.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

към Постановление № 41 на Министерския съвет от 9 март 2020 г. за изменение и

допълнение на Наредбата за криптографската сигурност на класифицираната информация

(ДВ, бр. 21 от 2020 г., в сила от 13.03.2020 г.)

§ 70. Издадените свидетелства за одобрение на криптографски средства, утвърдените организационни правила и правила за техническа експлоатация на криптографските мрежи и минимални изисквания за криптографска сигурност, издадени преди влизането в сила на настоящото постановление, запазват действието си.

.....

Приложение № 1
към чл. 55, ал. 1
(Изм. и доп. – ДВ, бр. 21 от 2020 г.,
в сила от 13.03.2020 г.)

Поверително!

(след попълване)

УДОСТОВЕРЕНИЕ
ЗА
РАБОТА С КРИПТОГРАФСКИ СРЕДСТВА
№ ....., екз. № .....

На основание чл. 7, т. 4, буква "г" и чл. 55, ал. 1 от Наредбата за криптографската сигурност на класифицираната информация (НКСКИ)
.....
(орган, издал документа)
издава

на .....,
(трите имена на лицето)
ЕГН .....,
изпълняващ функции по чл. ..... от НКСКИ
(чл. 10, 13 или чл. 36, ал. 2)
като .....
(администратор, потребител)
на/в .....,
(наименование на криптографската мрежа, ако функциите, които се изпълняват, са по чл. 10 или 13)
в .....,
(организационна единица)
удостоверение за работа с .....
(посочва се криптографското средство
.....
или правото за работа с криптографски материали)
Удостоверението е валидно до .....

..... Подпис: .....

(дата на издаване)

Печат:

.....

(.....)

(място на издаване)

(фамилия)

Приложение № 2
към чл. 58, ал. 2

ОТНЕМАНЕ
НА УДОСТОВЕРЕНИЕ
ЗА
РАБОТА С КРИПТОГРАФСКИ СРЕДСТВА
№ ....., екз. № .....

На основание чл. 7, т. 4, буква "д" и чл. 58, ал. 1, т. .... от Наредбата за криптографската сигурност на класифицираната информация
.....
(орган, издал документа)
отнема
удостоверение за работа с криптографски средства № ...../....., издадено на .....,
(трите имена на лицето)
ЕГН .....,
от .....,
(организационна единица)

..... Подпис: .....

(дата на издаване) Печат:

..... (.....)

(място на издаване) (фамилия)

Приложение № 3
към чл. 59, ал. 2

ПРЕКРАТЯВАНЕ

НА УДОСТОВЕРЕНИЕ
ЗА
РАБОТА С КРИПТОГРАФСКИ СРЕДСТВА
№ ....., екз. № .....

На основание чл. 7, т. 4, буква "д" и чл. 59, ал. 1, т. .... от Наредбата за криптографската сигурност на класифицираната информация
.....
(орган, издал документа)
прекратява действието
на удостоверение за работа с криптографски средства № ...../.....,
издадено на .....,
(трите имена на лицето)
ЕГН .....,
от .....,
(организационна единица)

..... Подпис:.....

(дата на издаване) Печат:

..... (.....)

(място на издаване) (фамилия)

Приложение № 4
към чл. 67, ал. 1
(Доп. – ДВ, бр. 21 от 2020 г.,
в сила от 13.03.2020 г.)

Поверително!

(след попълване)

СВИДЕТЕЛСТВО
ЗА ОБУЧЕНИЕ
ПО КРИПТОГРАФСКА СИГУРНОСТ
№ .....

На основание чл. 63, т. .... от Наредбата за криптографската сигурност на класифицираната информация .....
.....
(орган, издал документа)
издава настоящото свидетелство
на .....,
(трите имена на лицето)
ЕГН .....,
.....,

(длъжност)

в .....,

(организационна единица)

в уверение на това, че същият е преминал успешно курс на обучение по криптографска сигурност.

Обучението е проведено от

.....

(орган, провел обучението)

Притежателят на настоящото свидетелство има право:

1. да изпълнява функциите на

.....

(администратор, завеждащ криптографска регистратура и потребител)

2. да работи с криптографско средство

.....

(тип на криптографското средство)

3. да провежда обучение по/за (само за администратор)

.....

(област, в която има право да провежда обучение)

Свидетелството е валидно до .....

Подпис на лицето: .....

..... Подпис: .....

(дата на издаване) Печат:

..... (.....)

(място на издаване) (фамилия)