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

ДЪРЖАВНАТА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА (ДКСИ), в качеството си на държавен орган, осъществяващ политиката на Република България за защита на класифицираната информация, който организира, осъществява, координира и контролира дейността по защита на тази информация и на компетентен орган по прилагането и контрола по изпълнението на международните договори за взаимна защита и обмен на класифицирана информация, на основание чл. 10, ал. 1, т. 4 от Закона за защита на класифицираната информация (ЗЗКИ), т. 48 от Приложение IV на Решение на Съвета относно правилата за сигурност за защита на класифицираната информация на ЕС (2013/488/ЕС), изменено с Решение на Съвета от 14.04.2014 г., параграф 13.6 от Приложение "F" към Документ на НАТО C-M(2002)49/17.06.2002 г. и въз основа на **Решение на ДКСИ № 50-I-5.1/02.07.2015 г.**,изменено с **Решение на ДКСИ № 5-I-15/19.01.2016 г.** издава до задължените по ЗЗКИ субекти

ЗАДЪЛЖИТЕЛНИ УКАЗАНИЯ
за реда за провеждане на процедура по акредитиране на сигурността на точки на присъствие (Points of Presence – PoP) на комуникационни и информационни системи (Communication and Information Systems - CIS) на НАТО или на ЕС и национални автоматизирани информационни системи (АИС) или мрежи, предназначени за работа с класифицирана информация на НАТО, на ЕС или чуждестранна класифицирана информация, предоставена на Република България по силата на действащите международни договори за взаимна защита и обмен на класифицирана информация

ГЛАВА ПЪРВА
ОБЩИ ПОЛОЖЕНИЯ

1. Настоящите задължителни указания уреждат разпределението на дейностите и осъществяването на координация между отделните субекти във връзка с осъществяване на функциите им по отношение на акредитиране на сигурността на точки на присъствие на комуникационни и информационни системи (PoP на CIS) на НАТО или на ЕС и национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО, на ЕС или чуждестранна класифицирана информация, предоставена на Република

България по силата на действащите международни договори за взаимна защита и обмен на класифицирана информация.

ГЛАВА ВТОРА
КОМПЕТЕНТНИ ОРГАНИ

2. Национални органи, изпълняващи функции по сигурността на класифицираната информация на ЕС (КИЕС), са следните ведомства:

Орган по осигуреност на информацията *Information Assurance Authority (IAA)*	ДКСИ и ДАНС
Орган по ТЕМПЕСТ *TEMPEST Authority (TA)*	ДАНС
Орган за криптографско одобрение *Crypto Approval Authority (CAA)*	ДАНС
Орган за разпределение на криптографски материали *Crypto Distribution Authority (CDA)*	ДАНС
Орган по акредитиране на сигурността *Security Accreditation Authority (SAA)*	ДКСИ

3. Функциите на органа по осигуреност на информацията (IAA) се разпределят както следва:

3.1. На ДКСИ

3.1.1. Разработване на политики и насоки за сигурност за осигуреност на информацията (ОИ) и наблюдение на тяхната ефективност и целесъобразност.

3.1.2. Гарантиране, че избраните за защита на КИЕС мерки за ОИ съответстват на политиките, уреждащи тяхната пригодност и избор.

3.1.3. Координиране на обучението и повишаването на осведомеността относно ОИ.

3.2. На ДАНС:

3.2.1. Опазване и администриране на техническата информация, свързана с криптографските продукти.

3.2.2. Гарантиране, че криптографските продукти се подбират в съответствие с политиките, уреждащи тяхната пригодност и избор.

3.3. На ДКСИ и ДАНС:

3.3.1. Консултиране с доставчика на системата, участниците в областта на сигурността и представители на ползвателите по отношение на политиките и насоките за сигурност за ОИ.

3.3.2. Гарантиране на наличието на подходящ експертен ресурс в състава на Комитета по сигурността, отговарящ за въпросите на ОИ.

4. За всяка CIS, предназначена за работа с класифицирана информация на ЕС, в организационните единици, по предложение на служителя по сигурността на информацията, се определя Оперативен орган по осигуреност на информацията (Information Assurance Operating Authority - IAOA).

5. Функциите на органите по сигурността са определени в Приложение IV на Решение на Съвета относно правилата за сигурност за защита на класифицираната информация на ЕС (2013/488/ЕС), изменено с Решение на Съвета от 14.04.2014 г.

6. Национални органи, изпълняващи функции по сигурността на класифицираната информация на НАТО, са следните ведомства:

Национален орган по комуникационна сигурност *National Communications Security Authority (NCSA)*	ДАНС
Орган по ТЕМПЕСТ *TEMPEST Authority (TA)*	ДАНС
Национален орган за разпределение на криптографски материали *National Distribution Authority (NDA)*	МО
Орган по акредитиране на сигурността *Security Approval or Accreditation Authority (SAA)*	ДКСИ

7. За всяка CIS, предназначена за работа с класифицирана информация на НАТО в организационната единица, по предложение на служителя по сигурността на информацията, се определя Оперативен орган за КИС (CIS Operating Authority).

8. Функциите на органите по сигурността са определени в Приложения „B“ и „F“ към Политиката на НАТО по сигурността (ENCLOSURE “B” и ENCLOSURE “F” to C-M(2002)49), Директивата на НАТО по управление на информационната сигурност за КИС (INFOSEC MANAGEMENT DIRECTIVE for CIS) и Директивата на НАТО по емисионна сигурност (Directive on Emission Security).

ГЛАВА ТРЕТА
ОРГАНИЗАЦИЯ И РАЗПРЕДЕЛЕНИЕ НА ДЕЙНОСТИТЕ

РАЗДЕЛ I

Акредитиране на сигурността на точки на присъствие на комуникационни и информационни системи на НАТО или ЕС

9. Организационната единица изпраща до ДКСИ заявление за акредитиране на изградена PoP на CIS на НАТО или ЕС по смисъла на чл. 13 от Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация (НЗОУСАИСМ).

10. След получаване на заявлението ДКСИ изпраща уведомление до организационната единица за условията и етапите за акредитиране.

11. Организационната единица изпраща до ДКСИ:

11.1. Изготвени от оперативния орган на РоР на CIS в ОЕ, съгласно стратегията за акредитация на системата, в електронен вид, за проверка:

11.1.1. Локализирани версии на документите по сигурността на РоР на CIS (SRMS, SSRS, SecOPs и др.) по образец на собственика на CIS.

11.1.2. Попълнен образец на декларация за съответствие (SoC) на РоР на CIS.

11.2. Съгласувани от ДАНС в качеството й на IAA и NCSA организационни правила и правила за техническа експлоатация на криптографското средство (Crypto plan), което се използва в РоР на CIS, ако се изисква в стратегията за акредитиране на системата.

11.3. Копие на заповед на ръководителя на ОЕ за определяне на служителите, които ще вземат участие в комисията за извършване на комплексна оценка на сигурността на РоР на CIS.

12. Със заповед на председателя на ДКСИ се определя междуведомствена комисия за комплексна оценка на сигурността на РоР на CIS по смисъла на чл. 16 от НЗОУСАИСМ, която е съставена от служители на ДКСИ и определените служители от организационната единица.

12.1. При необходимост в комисията по т. 12 се включват и експерти от ДАНС, в качеството й на IAA, NCSA и TA.

12.2. В случаите по т. 12.1 ДКСИ информира ДАНС за необходимостта от включване на съответните експерти, които се определят със заповед на председателя на ДАНС.

12.3. След приключване на работата си комисията съставя протокол (по един екземпляр за всяко ведомство, осигурило членове в комисията по т. 12.) за резултатите от извършената комплексна оценка на сигурността на РоР на CIS.

13. При положителна комплексна оценка на сигурността на РоР на CIS ДКСИ:

13.1. Утвърждава получените от организационната единица на хартиен носител в два екземпляра и одобрени от комисията за извършване на комплексна оценка, документи по сигурността на РоР на CIS.

13.2. Издава в три екземпляра Декларация за съответствие (SoC), с която потвърждава съответствието на приложените мерки по сигурността в РоР на CIS с изискванията на собственика на CIS.

13.3. Изпраща до организационната единица екземпляр № 1 от утвърдените документи по сигурността и екземпляр № 2 от издадената SoC.

13.4. Изпраща на хартиен носител екземпляр № 3 на издадената SoC до компетентния орган по акредитиране на системата.

13.5. В случай на необходимост ДКСИ, или по изключение организационната единица, съгласувано с ДКСИ, изпраща издадената SoC в електронен вид до компетентния орган по акредитиране на системата.

14. Най-малко 3 месеца преди изтичане на срока на валидност на издадената SoC организационната единица уведомява ДКСИ за необходимостта от преакредитация на PoP на CIS и описва настъпилите промени в средата за сигурност, ако има такива.

15. Редът за извършване на преакредитация на PoP на CIS се определя от ДКСИ, в съответствие с посочените от организационната единица по т. 14 промени.

РАЗДЕЛ II

Акредитиране на сигурността на национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО или ЕС

16. Организационната единица изпраща до ДКСИ заявление по смисъла на чл. 13 от НЗОУСАИСМ за започване на процедура по акредитиране на АИС или мрежата за работа с класифицирана информация на НАТО или ЕС.

17. След получаване на заявлението ДКСИ изпраща уведомление до организационната единица за условията и етапите за акредитиране.

18. При необходимост организационната единица заявява в ДАНС, в качеството й на ТА, извършване на зониране на помещения и оборудване.

19. При необходимост от използване на криптографски средства в АИС или мрежата организационната единица консултира и съгласува с ДАНС, в качеството й на ОКС, IAA и NCSA, всички аспекти на криптографската сигурност.

20. В случай на избор на криптографско средство, одобрено от компетентен орган на НАТО или ЕС, организационната единица получава от производителя и предоставя в ДАНС необходимите документи по отношение на сигурността за въвеждане в експлоатация и работа с избраното криптографско средство.

21. Организационната единица изпраща до ДКСИ:

21.1. Изготвените от органа по развитие и експлоатация (ОРЕ) в организационната единица документи по сигурността на АИС или мрежата, в електронен вид, за проверка:

21.1.1. Анализ на риска на АИС или мрежата (за АИС или мрежи, предназначени за работа с класифицирана информация с ниво на класификация „СЕКРЕТНО“ или по-високо), който след съгласуване с ДКСИ се утвърждава от ръководителя на организационната единица.

21.1.2. Специфични изисквания за сигурност (СИС) на АИС или мрежата.

21.1.3. Процедури за сигурност (ПС) на АИС или мрежата.

21.2. Съгласувани от ДАНС в качеството й на IAA и NCSA организационни правила и правила за техническа експлоатация на криптографското средство, когато в АИС или мрежата се използва такова.

21.3. Копие на заповед на ръководителя на организационната единица, с която се определят служителите, които ще вземат участие в комисията за извършване на комплексна оценка на сигурността на АИС или мрежата.

22. Със заповед на председателя на ДКСИ, в която са включени и определените служители на организационната единица, се назначава междуведомствена комисия за извършване на комплексна оценка на сигурността на АИС или мрежата.

22.1. При необходимост в комисията по т. 22 се включват и експерти от ДАНС, в качеството й на ОКС, IAA, NCSA и ТА.

22.2. В случаите по т. 22.1 ДКСИ информира ДАНС за необходимостта от включване на съответните експерти, които се определят със заповед на председателя на ДАНС.

22.3. След приключване на работата си, комисията съставя протокол (по един екземпляр за всяко ведомство, осигурило членове в комисията по т. 22) за резултатите от извършената комплексна оценка на сигурността на АИС или мрежата.

23. При положителна комплексна оценка на сигурността на АИС или мрежата ДКСИ:

23.1. Утвърждава получените от организационната единица на хартиен носител в два екземпляра и одобрени от комисията за извършване на комплексна оценка СИС и ПС на АИС или мрежата.

23.2. Издава сертификат за сигурност на АИС или мрежата по образец съгласно Приложение № 1 или Приложение № 2 със срок на валидност не по-дълъг от 3 години.

23.3. Издава в два екземпляра сертификационен отчет, който е неразделна част от сертификата по т. 23.2.

23.4. Изпраща до организационната единица екземпляр № 1 от утвърдените СИС и ПС на АИС или мрежата, издадения по т. 23.2 сертификат за сигурност на АИС или мрежата и екземпляр № 2 от сертификационния отчет към него.

24. Най-малко 3 месеца преди изтичане на срока на валидност на издадения сертификат за сигурност на АИС или мрежата организационната единица уведомява ДКСИ за необходимостта от преакредитация на АИС или

мрежата и описва настъпилите промени в средата за сигурност на АИС или мрежата, ако има такива.

25. Редът за извършване на преакредитация на АИС или мрежата се определя от ДКСИ в съответствие с посочените от организационната единица по т. 24 промени.

РАЗДЕЛ III

Акредитиране на сигурността на национални АИС или мрежи, предназначени за работа с национална класифицирана информация и класифицирана информация на НАТО или ЕС

26. Организационната единица изпраща заявление за започване на процедура по акредитиране на АИС или мрежата за работа с национална класифицирана информация до Органа по акредитиране на сигурността (ОАС) – СДИС-ДАНС по реда на чл. 13 от НЗОУСАИСМ.

27. След получен сертификат за сигурност на АИС или мрежата по чл. 14, т. 2 от ЗЗКИ, организационната единица изпраща до ДКСИ заявление за започване на процедура по акредитиране на АИС или мрежата за работа с класифицирана информация на НАТО или ЕС.

28. ДКСИ изпраща искане до ОАС за информация относно валидността на издадения на АИС или мрежата сертификат по т. 27.

29. След получаване от ДАНС на потвърждение на валидността на издадения на АИС или мрежата сертификат по т. 27, ДКСИ изпраща уведомление до организационната единица за условията и етапите за акредитиране.

30. Организационната единица изпраща до ДКСИ:

30.1. Утвърдените от ОАС документи по сигурността на АИС или мрежата, издадения от ОАС сертификат за сигурност на АИС или мрежата и сертификационния отчет към него, както и утвърдените от ОКС организационни правила и правила за техническа експлоатация на криптографското средство, когато в АИС или мрежата се използва такова за класифицирана информация с ниво на класификация до „ПОВЕРИТЕЛНО“ за запознаване и временно ползване.

30.2. Правила относно организацията на работа с класифицирана информация на НАТО или ЕС по всички видове сигурност и други допълнителни документи, касаещи сигурността на АИС или мрежата при

работата с класифицирана информация на НАТО или ЕС, посочени в уведомлението, в електронен вид за проверка.

30.3. Копие на заповед на ръководителя на организационната единица, с която се определят служителите, които ще вземат участие в комисията за извършване на комплексна оценка на сигурността на АИС или мрежата по отношение на работата с класифицирана информация на НАТО или ЕС.

31. За извършване на комплексна оценка на сигурността на заявената АИС или по отношение на работата с класифицирана информация на НАТО или ЕС се прилагат условията и реда на т. 22 от Раздел II, Глава трета от настоящите задължителни указания .

32. При положителна комплексна оценка на сигурността на АИС или мрежата ДКСИ:

32.1. Утвърждава получените от организационната единица на хартиен носител в два екземпляра и одобрени от комисията за извършване на комплексна оценка правила относно организацията на работа с класифицирана информация на НАТО или ЕС по всички видове сигурност на АИС или мрежата.

32.2. Издава сертификат за сигурност на АИС или мрежата по образец съгласно Приложение № 1 или Приложение № 2 със срок на валидност не по-дълъг от 3 години.

32.3. Издава в два екземпляра сертификационен отчет, който е неразделна част от сертификата по т. 32.2.

32.4. Изпраща до организационната единица екземпляр № 1 от утвърдените правила относно организацията на работа с класифицирана информация на НАТО или ЕС по всички видове сигурност на АИС или мрежата, издадения по т. 32.2 сертификат за сигурност на АИС или мрежата и екземпляр № 2 от сертификационния отчет към него.

33. Най-малко 3 месеца преди изтичане срока на валидност на издадения сертификат за сигурност на АИС или мрежата организационната единица уведомява ДКСИ за необходимостта от преакредитация на АИС или мрежата и описва настъпилите промени в средата за сигурност на АИС или мрежата, ако има такива.

34. Редът за извършване на преакредитация на АИС или мрежата се определя от ДКСИ, в съответствие с посочените от организационната единица по т. 33 промени.

РАЗДЕЛ IV

Акредитиране на сигурността на национални АИС или мрежи за двустранен или многостранен обмен на класифицирана информация с друга държава или международна организация, с която Република България има влязъл в сила международен договор за взаимна защита и обмен на класифицирана информация

35. Преди изграждане на АИС или мрежа за двустранен или многостранен обмен на класифицирана информация с друга държава или международна организация, с които Република България има влязъл в сила международен договор за взаимна защита и обмен на класифицирана информация, организационната единица е длъжна да уведоми ДКСИ за предстоящото изграждане на същата и да подаде заявление по смисъла на чл. 13 от НЗОУСАИСМ за започване на процедура по акредитиране на АИС или мрежата за работа с чуждестранна класифицирана информация.

36. Организационната единица е длъжна да предостави на ДКСИ всички документи, изготвени от организатора на АИС или мрежата, касаещи:

36.1. Техническата реализация и специфичните изисквания по сигурността на АИС или мрежата.

36.2. Разпределението на задълженията и отговорностите по сигурността за АИС или мрежата.

37. ДКСИ, в качеството й на държавен орган, който осъществява политиката на Република България за защита на класифицираната информация, е компетентен орган по прилагането и контрола по изпълнението на международните договори за взаимна защита и обмен на класифицирана информация.

37.1. Класифицираната информация, обменяна в АИС или мрежа по настоящия раздел, се счита за класифицирана информация, предназначена за двустранен/многостранен обмен (вж. § 2 от ДР.).

38. Процедурите по акредитиране и издаване на сертификат за сигурност на АИС или мрежата по този раздел (Приложение № 3) се определят за всеки конкретен случай съгласно съответния международен договор, освен ако могат да се приложат по аналогия процедурите, посочени в другите раздели на настоящите указания, когато съответният международен договор не предвижда други правила и изисквания.

РАЗДЕЛ V

Акредитиране на сигурността на взаимна свързаност на национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО или ЕС, към точки на присъствие на комуникационни и информационни системи на НАТО или ЕС

39. Организационната единица уведомява ДКСИ за необходимостта от изграждането на взаимна свързаност на акредитирана по реда на раздел II на Глава трета от настоящите указания АИС или мрежа, предназначена за работа с класифицирана информация на НАТО или ЕС, към точки на присъствие на комуникационни и информационни системи (PoP на CIS) на НАТО или ЕС.

40. ДКСИ оказва съдействие на организационната единица в проучването на възможността и условията за изграждане на заявената взаимна свързаност.

41. Организационната единица изпраща до ДКСИ:

41.1. Получени от организатора на CIS на НАТО или ЕС документи по сигурността на връзката на електронен носител.

41.2. Изготвени от ОРЕ в организационната единица в електронен вид, за проверка, следните документи по сигурността на АИС или мрежата:

41.2.1. Попълнен образец на SoC/Code of connection на АИС или мрежата.

41.2.2. Актуализирани, в съответствие с изисквания на собственика на CIS на НАТО или ЕС, Специфични изисквания за сигурност и Процедури за сигурност на АИС или мрежата.

41.3. Съгласувани от ДАНС, в качеството й на IAA и NCSA организационни правила и правила за техническа експлоатация на криптографското средство, когато в АИС или мрежата се използва такова.

41.4. Копие на заповед на ръководителя на организационната единица, с която се определят служителите, които ще вземат участие в комисията за извършване на комплексна оценка на сигурността на взаимната връзка.

42. Със заповед на председателя на ДКСИ се определя междуведомствена комисия за комплексна оценка на сигурността на взаимната връзка, която е съставена от служители на ДКСИ и определените служители на организационната единица.

42.1. При необходимост в комисията по чл. 42 се включват и експерти от ДАНС, в качеството й на IAA, NCSA.

42.2. В случаите по т. 42.1 ДКСИ информира ДАНС за необходимостта от включване на съответните експерти, които се определят със заповед на председателя на ДАНС.

42.3. След приключване на работата си комисията съставя протокол за резултатите от извършената комплексна оценка на сигурността на взаимната

връзка (по един екземпляр от протокола за всяко ведомство, осигурило членове в комисията по т. 42).

43. При положителна комплексна оценка на сигурността на взаимната връзка ДКСИ:

43.1. Утвърждава получените от организационната единица на хартиен носител в два екземпляра, актуализирани в съответствие с изисквания на собственика на CIS на НАТО или ЕС, документи по сигурността на АИС или мрежата.

43.2. Издава в три екземпляра одобрения от комисията по т. 42 SoC/Code of connection, с което потвърждава съответствието на приложените мерки по сигурността в АИС или мрежата с изискванията на собственика на CIS.

43.3. Изпраща до организационната единица екземпляр № 1 от утвърдените документи по сигурността и екземпляр № 2 от издадения SoC/Code of connection на АИС или мрежата.

43.4. Изпраща на хартиен носител екземпляр № 3 на издадения SoC/Code of connection до компетентния орган по акредитиране на CIS на НАТО или ЕС.

43.5. В случай на необходимост ДКСИ, или по изключение организационната единица, съгласувано с ДКСИ, изпраща издадения SoC/Code of connection на АИС или мрежата до компетентния орган по акредитиране на CIS на НАТО или ЕС в електронен вид.

44. Най-малко 3 месеца преди изтичане на срока на валидност на издадения SoC/Code of connection организационната единица уведомява ДКСИ за необходимостта от преакредитация на взаимната връзка на АИС или мрежата и описва настъпилите промени в средата за сигурност, ако има такива.

45. Редът за извършване на преакредитация на взаимната връзка на АИС или мрежата се определя от ДКСИ, в съответствие с посочените от организационната единица по т. 44 промени.

РАЗДЕЛ VI

Издаване на сертификат за определен срок на национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО или ЕС или за двустранен или многостранен обмен на класифицирана информация с друга държава или международна организация, с които Република България има влязъл в сила международен договор за взаимна защита и обмен на класифицирана информация

46. В случаите по раздели II, III и IV на Глава трета от настоящите задължителни указания ДКСИ може да издаде сертификат за сигурност за определен период на АИС или мрежа, когато за изпълнението на важни за

държавата задачи е необходимо тя да бъде въведена в експлоатация преди да бъде завършен процесът на нейното акредитиране.

47. Сертификатът по т. 46 съдържа:

47.1. Ниво на класификация на информацията, която ще бъде създавана, съхранявана, обработвана и пренасяна в АИС или мрежата.

47.2. Задължителните условия за сигурност, които трябва да се спазват при експлоатацията на АИС или мрежата в периода на действие на сертификата.

47.3. Условия за окончателно акредитиране на АИС или мрежата.

47.4. Срок на валидност на сертификата (не по-дълъг от 1 година).

48. В случаите по раздел III на Глава трета от настоящите задължителни указания сертификатът по т. 46 се издава след издаване от ОАС на сертификат за работа с национална класифицирана информация.

РАЗДЕЛ VII

Отнемане / Прекратяване на сертификат на национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО или ЕС или за двустранен или многостранен обмен на класифицирана информация с друга държава или международна организация, с която Република България има влязъл в сила международен договор за взаимна защита и обмен на класифицирана информация

49. За отнемане / прекратяване на сертификат на национални АИС или мрежи, предназначени за работа с класифицирана информация на НАТО или ЕС или за двустранен или многостранен обмен на класифицирана информация с друга държава или международна организация, с които Република България има влязъл в сила международен договор за взаимна защита и обмен на класифицирана информация се прилага редът, предвиден в Глава шеста от НЗОУСАИСМ.

РАЗДЕЛ VIII

Индустриална сигурност

50. Когато по реда на индустриалната сигурност от кандидата за изпълнител се изисква наличие на АИС или мрежа, предназначена за работа с класифицирана информация на НАТО, на ЕС или на чуждестранна класифицирана информация, предоставена на Република България по силата на действащите международни договори за взаимна защита и обмен на

класифицирана информация, заявлението за нейното акредитиране се изпраща до ДКСИ чрез организационната единица – възложител и акредитирането се извършва по реда на тези задължителни указания.

51. ДКСИ изпраща уведомлението за откриване на процедура по акредитиране на АИС или мрежата до организационната единица – кандидат за изпълнител чрез организационната единица – възложител.

52. При положителна комплексна оценка на сигурността на АИС или мрежата, ДКСИ издава съответния сертификат за сигурност на АИС или мрежата със срок на валидност не по-дълъг от 3 години.

53. ДКСИ изпраща сертификата на организационната единица-кандидат за изпълнител и едновременно с това уведомява възложителя за неговото издаване.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. „Комуникационна информационна система“ (Communication and information system – CIS) е всяка система, даваща възможност за работа с класифицирана информация в електронна форма. Една CIS обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси.

§2. По отношение на защитата на класифицираната информация, предназначена за двустранен или многостранен обмен, обменяна по реда на Глава трета, Раздел IV от настоящите задължителни указания, приложимото право е съответният влязъл в сила международен договор или принципите, нормите и процедурите на международната организация за защита на класифицирана информация.

§3. ДКСИ води регистър на сертифицираните АИС или мрежи, предназначени за работа с класифицирана информация на НАТО, на ЕС или на чуждестранна класифицирана информация.

§4. Легенда на съкращенията на чуждите думи и изрази:

PoP	Point of Presence *Точка на присъствие*
CIS	Communication and Information System *Комуникационна и информационна система*

SRMS	System Risk Management Statement *Декларация за управление на риска на системата*
SSRS	System-specific Security Requirements Statement *Специфични изисквания за сигурност на системата*
SecOPs	Security Operating Procedures *Процедури за сигурност*
SoC	Statement Of Compliance *Декларация за съответствие*
SAR	Security Accreditation Report *Акредитационен доклад*
NOS	National Security Authority *Национален орган по сигурността*
SAA	Security Accreditation Authority *Орган по акредитиране на сигурността*
IAA	Information Assurance Authority *Орган по осигуреност на информацията*
CAA	Crypto Approval Authority *Орган за криптографско одобрение*
CDA	Crypto Distribution Authority Орган за разпределение на криптографски материали
TA	TEMPEST Authority *Орган по ТЕМПЕСТ*
NCSA	National Communications Security Authority *Национален орган по комуникационна сигурност*
NDA	National Distribution Authority *Национален орган за разпределение на криптографски материали*

Настоящите задължителни указания подлежат на незабавно изпълнение.

Приложение № 1

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА

1505 СОФИЯ, ул.”Черковна” № 90

тел.: +3592 9333 600; факс: +3592 987 3750; e-mail: dksi@government.bg

СЕРТИФИКАТ ЗА СИГУРНОСТ НА АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ИЛИ МРЕЖА

№ Е - ……..

Държавната комисия по сигурността на информацията в качеството ѝ на национален орган по акредитиране на сигурността на АИС или мрежи, в които се създава, обработва, съхранява и пренася чуждестранна класифицирана информация и на основание т. 48 от Приложение IV на Решение на Съвета относно правилата за сигурност за защита на класифицираната информация на ЕС (2013/488/ЕС), изменено с Решение на Съвета от 14.04.2014 г., съгласно свое решение № …… издава настоящия сертификат за сигурност на

……..,

изградена за нуждите на

……

Настоящият сертификат удостоверява, че в посочената по-горе АИС „……” може да се създава, обработва, съхранява и пренася класифицирана информация на Европейския съюз с ниво на класификация за сигурност

……..включително,

със срок на валидност до …….

ПРЕДСЕДАТЕЛ НА ДКСИ

…….

…….

гр. София, ___.___.____ г.

Приложение № 2

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
1505 СОФИЯ, ул.”Черковна” № 90
тел.: +3592 9333 600; факс: +3592 987 3750; e-mail: dksi@government.bg

СЕРТИФИКАТ ЗА СИГУРНОСТ НА АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ИЛИ МРЕЖА

№ Н - ……..

Държавната комисия по сигурността на информацията в качеството й на национален орган по акредитиране на сигурността на АИС или мрежи, в които се създава, обработва, съхранява и пренася чуждестранна класифицирана информация и на основание параграф 13.6 от Приложение "F" към Документ на НАТО C-M(2002)49/17.06.2002 г., съгласно свое решение № …… издава настоящия сертификат за сигурност на

……..,

изградена за нуждите на

……

Настоящият сертификат удостоверява, че в посочената по-горе АИС „.……” може да се създава, обработва, съхранява и пренася класифицирана информация на НАТО с ниво на класификация за сигурност

……..включително,

със срок на валидност до …….

ПРЕДСЕДАТЕЛ НА ДКСИ

……

……

гр. София, ___.___.____ г.

Приложение № 3

ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
1505 СОФИЯ, ул.”Черковна” № 90
тел.: +3592 9333 600; факс: +3592 987 3750; e-mail: dksi@government.bg

СЕРТИФИКАТ ЗА СИГУРНОСТ НА АВТОМАТИЗИРАНА ИНФОРМАЦИОННА СИСТЕМА ИЛИ МРЕЖА

№ Ч - ……..

Държавната комисия по сигурността на информацията в качеството ѝ на национален орган по акредитиране на сигурността на АИС или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация, предназначена за двустранен/многостранен обмен и на основание ……(изписва се споразумението/договора)……., съгласно свое решение № …… издава настоящия сертификат за сигурност на

……..,

изградена за нуждите на

……

Настоящият сертификат удостоверява, че в посочената по-горе АИС „……” може да се създава, обработва, съхранява и пренася класифицирана информация, предназначена за двустранен/многостранен обмен с ниво на класификация за сигурност, еквивалентно на

……..включително,

със срок на валидност до …….

ПРЕДСЕДАТЕЛ НА ДКСИ

……

……

гр. София, ___.___.____ г.