ДЪРЖАВНА КОМИСИЯ ПО СИГУРНОСТТА НА ИНФОРМАЦИЯТА
1202 СОФИЯ, ул. „Козлодуй” № 4
тел.: +3592 9333 600; факс: +3592 9873 750; e-mail: dksi@dksi.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, който организира, контролира и отговаря за изпълнението на задълженията за защита на класифицираната информация, съдържащи се в международни договори, по които Република България е страна, и на основание чл. 9, т. 6 и т.16, чл. 10, ал. 1, т. 4 от ЗЗКИ, въз основа на Решение на ДКСИ № 44-I-15/16.06.2022 г., издава до задължените по ЗЗКИ субекти

ЗАДЪЛЖИТЕЛНИ УКАЗАНИЯ

за реда за провеждане на процедурата по акредитиране на комуникационните и информационните системи за работа с класифицирана информация на ЕС и/или на НАТО

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Предмет и обхват

1. Настоящите задължителни указания регламентират правилата и изискванията, свързани с провеждането на процедурата по акредитиране на комуникационните и информационните системи (КИС) за работа с класифицирана информация на ЕС и/или НАТО.

2. Документът се отнася за всички КИС, в които се създава, обработва, ползва, съхранява или обменя класифицирана информация на ЕС и/или на НАТО.

Цел

3. Целта на настоящите задължителни указания е изпълнението на задълженията за защита на класифицираната информация, съдържащи се в международни договори, по които Република България е страна – в частност Споразуменията с държавите-членки на Европейския съюз и на Северноатлантическия договор.

Принципи

4. По отношение на обменяната или предоставената на Република България класифицирана информация от страна на международна организация, чийто член е Република България, се прилагат принципите, нормите и процедурите за защита на класифицирана информация, действащи в рамките на тази международна организация (чл. 116 ЗЗКИ).

5. Всички КИС, предназначени за работа с класифицирана информация на НАТО и ЕС, преминават през процедура по акредитиране. Целта е да се гарантира, че са изпълнени всички необходими мерки за сигурност и е постигнато достатъчно високо ниво на защита на КИС и на информацията в нея.

Глава втора
КОМПЕТЕНТНИ ОРГАНИ

6. Национални органи, които изпълняват функции по сигурността на класифицираната информация на ЕС (КИЕС) в електронна форма:

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

6.1. ДКСИ извършва акредитирането на точките на присъствие на КИС на ЕС и взаимната свързаност на национални КИС с тях.

6.2. ДАНС извършва акредитирането на националните КИС за работа с класифицирана информация на ЕС.

6.3. 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 19.12.2019 г. (Правила за сигурност на Съвета на ЕС)

6.4. За всяка КИС, предназначена за работа с КИЕС, в организационните единици по предложение на служителя по сигурността на информацията се определя оперативен орган по осигуреност на информацията (Information Assurance Operational Authority - IAOA)

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

Национален орган по сигурността на КИС *National CIS Security Authority (NCSA)*	ДАНС
Национален орган по TEMPEST *TEMPEST Authority (TA)*	ДАНС
Национален орган за разпределение на криптографски материали *National Distribution Authority (NDA)*	МО
Органи по акредитиране на сигурността *Security Approval or Accreditation Authority (SAA)*	ДКСИ, ДАНС

7.1. ДКСИ извършва акредитирането на точките на присъствие на КИС на НАТО и взаимната свързаност на национални КИС с тях.

7.2. ДАНС извършва акредитирането на националните КИС за работа с класифицирана информация на НАТО.

7.3. За всяка КИС, 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 Operational Authority).

7.4. Функциите на органите по сигурността са определени в Приложение „F" към Политиката за сигурност на НАТО C-M(2002)49, Директивата на НАТО за управление на сигурността на КИС AC/35-D/2005 и Директивата на НАТО за сигурност по отношение на компрометиращите електромагнитни излъчвания AC/322-D(2019)0021.

Глава трета

ОРГАНИЗАЦИЯ И РАЗПРЕДЕЛЕНИЕ НА ДЕЙНОСТИТЕ ПО АКРЕДИТИРАНЕ НА КОМУНИКАЦИОННИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ ЗА РАБОТА С КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС И/ИЛИ НАТО

Раздел I

Акредитиране на точки на присъствие (ТнП) на комуникационните и информационните системи на ЕС или НАТО за Република България

8. Организационната единица изпраща до ДКСИ заявление за започване на процедура по акредитиране на ТнП на КИС на ЕС или на НАТО.

8.1. Заявлението се изготвя от оперативния орган по осигуреност на информацията на КИС (за КИЕС) или оперативния орган на системата (за КИ на НАТО), съгласува се със служителя по сигурността на информацията и се подписва от ръководителя на ОЕ.

8.2. В заявлението се посочват общи сведения за конкретната ТнП на КИС, които включват:

- описание и предназначение на КИС;
- режим за сигурност;
- форма на представяне и ниво на класификация на информацията;
- очакван брой и типове потребители;
- средата, в която ще се експлоатира ТнП на КИС;
- тип криптографски средства и описание на предвижданата организация на тяхното използване;
- връзки с други КИС и/или други системи;
- ръководителя на оперативния орган на КИС в ОЕ.

9. След получаване на заявлението ДКСИ изпраща писмо до организационната единица, съдържащо уведомление за условията и етапите на акредитиране.

10. Организационната единица изпраща до ДКСИ:

10.1. Изготвени от оперативния орган на КИС в ОЕ в електронен вид, за преглед и одобрение:

- локализирани версии на документи по сигурността на ТнП на КИС по образец на собственика на системата;
- попълнен образец на документ за съответствие на ТнП на КИС;
- заповед/и за определяне на органи по сигурността и възлагане на функции съгласно изискванията на организатора на КИС;
- криптоплан за използваното криптографско средство, ако това се изисква за ТнП на КИС.

10.2. Проект на криптоплана за използваното криптографско средство в ТнП на КИС се изпраща до ДАНС (в качеството й на IAA и NCSA) заедно с одобрения от организатора на КИС криптоплан или друг подобен документ.

Окончателният документ се съгласува от ДАНС и се утвърждава от ДКСИ.

10.3. Копие на заповедта на ръководителя на ОЕ за определяне на служителите, които ще вземат участие в комисията за извършване на проверка на сигурността на ТнП на КИС, включваща проверки на изпълнението на мерките за сигурност, посочени в документите по сигурността.

11. Със заповед на председателя на ДКСИ се определя междуведомствена комисия за извършване на проверка на сигурността на ТнП на КИС. Комисията е

съставена от служители на ДКСИ и определените служители от организационната единица.

11.1. При необходимост в комисията по т. 11 се включват и експерти от ДАНС, в качеството й на IAA, NCSA и TA.

11.2. В случаите по т. 11.1 ДКСИ информира ДАНС за необходимостта от включване на съответните експерти, които се определят със заповед на председателя на ДАНС.

12. След приключване на работата си комисията съставя протокол (по един екземпляр за всяко ведомство, осигурило членове в комисията по т. 11) за резултатите от извършената проверка на ТнП на КИС.

13. При положителен резултат от извършената от комисията по т. 11 проверка на сигурността ДКСИ:

13.1. Утвърждава получените от организационната единица в два екземпляра на хартиен носител документи за сигурност на ТнП на КИС, одобрени от комисията по т. 11.

13.2. Утвърждава документа за съответствие, с което потвърждава съответствието на приложените мерки по сигурността в ТнП на КИС с изискванията на собственика на системата.

13.3. Изпраща до организационната единица утвърдените документи по сигурността и екземпляр от издадения документ по т. 13.2.

13.4. Утвърденият от ДКСИ документ за съответствие се изпраща до компетентния орган по акредитиране на КИС на ЕС или на НАТО от организационната единица или ДКСИ.

14. Най-малко 6 месеца преди изтичане на срока на валидност на утвърдения документ за съответствие организационната единица уведомява ДКСИ за необходимостта от преакредитиране на ТнП и описва настъпилите промени в средата за сигурност, ако има такива.

15. Редът за извършване на преакредитиране на ТнП на КИС се определя от ДКСИ, в съответствие с посочените от организационната единица по т. 14 промени.

Раздел II

Акредитиране на КИС за работа с национална класифицирана информация и класифицирана информация на ЕС и/или НАТО

Акридитирането се извършва в съответствие с националното законодателство. В случаите, когато нормативната уредба на ЕС и/или НАТО предвижда различен от националното законодателство ред за акредитиране и/или различни изисквания за защита на КИ, ОАС посочва в уведомлението по чл. 16 от Наредбата за сигурността на КИС на комуникационните и информационните системи (НСКИС) или последващата кореспонденция конкретните ред, условия и изисквания за акредитиране на КИС.

16. Акредитирането на КИС за работа с национална класифицирана информация и класифицирана информация на ЕС и/или на НАТО може да се извършва паралелно в рамките на една процедура по акредитиране от ОАС (Специализирана дирекция „Информационна сигурност“ на ДАНС) по реда на глава трета от НСКИС.

17. ОЕ в този случай изготвя един комплект документи по сигурността (СИС и ПС), съдържащи изискванията и правилата за работа с национална класифицирана информация и такава на ЕС и/или НАТО, което ще се счита за изпълнение на изискванията на чл. 17, т. 1 от НСКИС за стартираните на процедури по акредитиране на КИС.

18. ОАС издава отделен сертификат за сигурност за класифицирана информация на ЕС или на НАТО, чийто срок е съобразен със съответните изисквания, но не по-дълъг от срока на валидност на сертификата за сигурност на КИС за национална КИ. За всеки издаден сетификат на КИС за работа с класифицирана информация на ЕС или НАТО ОАС писмено уведомява ДКСИ в едномесечен срок.

19. При изтичане срока на валидност на сертификат за сигурност на КИС за класифицирана информация на ЕС и/или НАТО и когато ОЕ декларира, че няма настъпили промени в утвърдените документи по сигурността и изпълнението на мерките и процедурите за сигурност, ОАС издава нов сертификат за сигурност по реда на глава трета, раздел I от НСКИС за съответната класифицирана информация със срок на валидност не по-дълъг от срока на валидност на сертификата за сигурност за национална класифицирана информация.

20. В случай че възникне необходимост за работа с класифицирана информация на ЕС и/или НАТО в периода на валидност на сертификата за сигурност за национална класифицирана информация, ОЕ стартира процедура по допълнително акредитиране, като подава заявление по чл. 28 от НСКИС. В него се включват и данните по чл. 15, ал. 3 на НСКИС по отношение на класифицираната информация на ЕС и/или НАТО.

21. С подаване на заявлението за допълнително акредитиране ОАС стартира процедура по акредитиране на КИС за класифицирана информация на ЕС и/или НАТО.

22. На органите по сигурността на КИС, определени по реда на националното законодателство, могат да се възлагат и функции по сигурността според нормативните изисквания на ЕС и НАТО. Функциите на ОРЕ следва да бъдат съобразени с тези на Information Assurance Operational Authority (IAOA) и/или на CIS Operational Authority (CISOA).

23. При премахване или промяна на нивото на класификация на информацията за един от типовете КИ, за които е сертифицирана КИС, прекратяването на съответния сертификат се извършва по реда на чл. 95 от НСКИС.

24. При наличие на междусистемна връзка се прилагат по-рестриктивните изисквания от приложимите законодателства. В изпълнение на изискването на чл. 77 от НСКИС, споразумението се сключва между Ръководителя на ОЕ, в която се експлоатира КИС и собственика на другата КИС.

25. При използване на криптографски мрежи, предназначени за защита на национална КИ, както и на КИ на ЕС и/или НАТО с криптографско средство, одобрено от ОКС – ДАНС се извършват дейностите и процедурите за криптографско одобрение по реда на НКСКИ за въвеждането им в експлоатация.

Раздел III

Акредитиране на национални КИС за работа с класифицирана информация на ЕС и/или на НАТО

Акредитирането на национални КИС за работа с класифицирана информация на ЕС и/или на НАТО се извършва съгласно националното законодателство.

В случаите, когато съществуват различни изисквания за защита на класифицирана информация на ЕС, ОАС посочва в уведомлението по чл. 16 от НСКИС или последващата кореспонденция конкретните ред, условия и изисквания за акредитиране на КИС.

Акредитирането на национални КИС за работа с класифицирана информация на НАТО се извършва по реда на националното законодателство и при спазване на изискванията на NATO Security Policy - Enclosure "F", Primary Directive on CIS Security, Management Directive on CIS Security и придружаващите ги директиви, ръководства и стандарти по отношение на КИ на НАТО.

26. По отношение на класифицираната информация на ЕС или на НАТО следва да бъдат определени длъжностни лица по сигурността на КИС съгласно НСКИС.

27. На органите по сигурността на КИС, определени по реда на националното законодателство, със заповед на РОЕ съгласувано със ССИ могат да се възлагат и функции по сигурността, определени по изискванията на ЕС или на НАТО, като функциите на ОРЕ следва да бъдат съобразени с тези на:

- Information Assurance Operational Authority – за класифицирана информация на ЕС, съгласно Правилата за сигурност на Съвета на ЕС (2013/488/EU);
- CIS Operational Authority – за класифицирана информация на НАТО, съгласно Management Directive on CIS Security (AC/35-D/2005-REV3/12.10.2015).

28. При междусистемна връзка се прилагат по-рестриктивните изисквания от приложимите нормативни документи. В изпълнение на изискването на чл. 77 от НСКИС, споразумението се сключва между Ръководителя на ОЕ, в която се експлоатира КИС и собственика на другата КИС.

29. За защита на класифицираната информация на НАТО в КИС се използват продукти от NATO Information Assurance Product Catalogue (https://www.ia.nato.int/niapc).

30. При използване на криптографски мрежи, предназначени за защита на КИ на ЕС и/или НАТО с криптографско средство, съответно одобрено от ЕС и/или НАТО в ОКС – ДАНС се предоставя:

- писмена информация по отношение на типа криптографско средство (КС) и описание на предвижданата организация на неговото използване;
- необходимите документи по отношение на криптографската сигурност, включително за инсталиране и експлоатиране на криптографското средство, администриране на ключовите материали, и условията при които следва да се извършват тези дейности.

31. ОЕ изготвя криптоплан за сигурността на криптографските средства и материали по отношение на тяхното транспортиране, инсталиране, администриране, експлоатация, съхранение, ремонт и предвидените действия при критични ситуации. Криптопланът се утвърждава от ОКС – ДАНС.

32. Проверките, които се изискват по правилата на НАТО по време на експлоатация на КИС, се извършват по реда на чл. 12 от ЗЗКИ.

33. Издаденият от ОАС сертификат за работа с класифицирана информация на ЕС и/или на НАТО е с валидност до 3 години. За издаването му ОАС уведомява ДКСИ в едномесечен срок.

Раздел IV

Акредитиране на сигурността на взаимна свързаност между национални КИС и точки на присъствие на КИС на ЕС или НАТО

Извършва се съгласно изискванията на организатора на КИС на ЕС и/или НАТО и документите: NATO Security Policy - Enclosure "F", Primary Directive on CIS Security, Management Directive on CIS Security и придружаващите ги директиви, ръководства и стандарти по отношение на класифицираната информация на НАТО и изискванията на Правилата за сигурност на Съвета на ЕС (2013/488/EU).

34. Организационната единица уведомява ДКСИ за необходимостта от взаимна свързаност между национална КИС и ТнП на КИС на ЕС или НАТО. Задължително условие е КИС предварително да бъде акредитирана от ОАС за работа с класифицирана информация на ЕС или НАТО със съответното ниво на класификация.

35. ДКСИ оказва съдействие на организационната единица в проучването на възможността и условията за изграждане на заявената взаимна свързаност. За тази свързаност не е необходимо да се подписва споразумение с организаторите на КИС на ЕС и/или НАТО.

36. Организационната единица изпраща до ДКСИ:

- Получени от организатора на КИС на ЕС или НАТО документи по сигурността на взаимната свързаност в електронна форма.
- Изготвените от оперативния орган на КИС в организационната единица документи по сигурността на КИС за запознаване:

- Издаден от ОАС валиден сертификат за сигурност на съответната КИС;
- Актуализирани специфични изисквания за сигурност и процедури за сигурност на КИС в съответствие с изискванията на организатора за взаимна свързаност на КИС на ЕС или НАТО;
- Утвърден криптоплан на криптографското средство, когато в КИС се използва такова;
- Копие на заповед на ръководителя на организационната единица, с която се определят служителите, които ще вземат участие в проверките, свързани със сигурността на междусистемната връзка;
- Попълнен образец на документ за съответствие на изискванията за сигурност на взаимната свързаност на КИС в електронен вид.

37. Със заповед на председателя на ДКСИ се определя междуведомствена комисия за извършване на проверка на сигурността на взаимната свързаност, която е съставена от служители на ДКСИ и определените служители на организационната единица.

37.1. При необходимост в комисията по чл. 37 се включват и експерти от ДАНС, в качеството й на IAA и NCSA.

37.2. В случаите по т. 37.1 ДКСИ информира ДАНС за необходимостта от включване на съответните експерти, които се определят със заповед на председателя на ДАНС.

37.3. След приключване на работата си комисията съставя протокол за резултатите от извършената проверка на сигурността на взаимната свързаност (по един екземпляр от протокола за всяко ведомство, осигурило членове в комисията по т. 37).

38. При положителен резултат от проверката на сигурността на взаимната свързаност ДКСИ:

38.1. Утвърждава одобрения от комисията документ за съответствие на изискванията за сигурност, с което потвърждава, че приложените мерки по сигурността за взаимната свързаност отговарят на изискванията на собственика на КИС на ЕС и/или НАТО.

38.2. Изпраща до организационната единица екземпляр от издадения по т. 38.1 документ за съответствие на изискванията за сигурност на взаимната свързаност.

39. Утвърденият от ДКСИ документ за съответствие се изпраща до компетентния орган по акредитиране на системата от Организационната единица или ДКСИ.

40. Най-малко 6 месеца преди изтичане на срока на валидност на издадения документ за съответствие на изискванията за сигурност на взаимната свързаност организационната единица уведомява ДКСИ за необходимостта от ново акредитиране и описва настъпилите промени в средите за сигурност, ако има такива.

41. Редът за извършване на ново акредитиране на взаимната свързаност на КИС се определя от ДКСИ, в съответствие с посочените от организационната единица по т. 40 промени.

Глава четвърта

ДЕЙНОСТИ ВЪВ ВРЪЗКА С ИЗПЪЛНЕНИЕ НА ИЗИСКВАНИЯТА ЗА КРИПТОГРАФСКАТА СИГУРНОСТ

Раздел I

Възлагане на функции по криптографската сигурност на класифицирана информация на ЕС и/или НАТО

42. В организационните единици, в които функционират ТнП на КИС за класифицирана информация на ЕС и/или НАТО, се възлагат функции на органи по криптографската сигурност, съгласно изискванията на организатора на КИС на ЕС и НАТО.

43. В криптографски мрежи по смисъла на Наредбата за криптографската сигурност на класифицираната информация, които се използват за защита на класифицирана информация на ЕС или НАТО, органите и функциите по криптографската сигурност се определят в съответствие със същата наредба.

44. При необходимост, в криптоплана могат да се разписват допълнителни роли и функции, в зависимост от организацията на криптографската мрежа.

45. На органите по криптографската сигурност, определени по реда на националното законодателство, могат да се възлагат и функции по сигурността, определени от изискванията на ЕС и на НАТО, ако е необходимо.

Раздел II

При използване на криптографски средства в национални КИС за работа с класифицирана информация на ЕС и/или НАТО ОЕ съгласува с ДАНС, в качеството ѝ на ОКС, всички аспекти на криптографската сигурност.

Използване на криптографски средства в национални КИС за работа класифицирана информация на ЕС и/или на НАТО

46. За защита на класифицирана информация на ЕС и/или НАТО могат да се използват криптографски средства:

- одобрени от компетентен орган по криптографско одобрение на ЕС или НАТО;
- одобрени от ОКС за защита на национална класифицирана информация, в случай на използването им за защита на класифицирана информация на ЕС или НАТО до ниво CONFIDENTIEL UE/EU CONFIDENTIAL и NATO CONFIDENTIAL включително.

47. Ръководителят на ОЕ взема решение за необходимостта от използване на криптографски средства за защита на класифицираа информация на ЕС и/или НАТО в ОЕ като се консултира с ОКС за наличието на подходящи за конкретната системна реализация криптографски средства или за други аспекти на криптографската сигурност.

ДОПЪЛНИТЕЛНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Точка на присъствие е обособена част от КИС на ЕС или НАТО, функционираща на територията на Република България в граници и по правила, определени от организатора на системата.

§ 2. Редът по чл. 23 от Наредбата за сигурността на КИС не се прилага при издаването на сертификат за сигурност на национални КИС за работа с класифицирана информация на ЕС и/или на НАТО.

§ 3. ДКСИ води регистър на сертифицираните КИС, предназначени за работа с класифицирана информация на НАТО и/или на ЕС, за което получава информация от ОАС два пъти годишно.

§ 4. Издадените от ДКСИ до влизането в сила на настоящите задължителни указания сертификати за сигурност на КИС се считат за валидни до изтичане на сроковете им.

§ 5. Настоящите задължителни указания влизат в сила след тяхното приемане.

Настоящите задължителни указания отменят Задължителните указания на ДКСИ за реда за провеждане на процедурата по акредитиране на комуникационните и информационните системи за работа с класифицирана информация на ЕС и/или на НАТО, приети с Решение на ДКСИ № 46 I-17/03.06.2021 г.