СИГУРНОСТ НА КОМУНИКАЦИОННИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ (КИС)

ДЕЙНОСТИ, СВЪРЗАНИ С КРИПТОГРАФСКАТА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Нормативна база, регламентираща защитата на класифицираната информация в КИС

- ЗЗКИ
- Правилник за прилагането на ЗЗКИ
- Наредба за сигурността на комуникационните и информационните системи
- Наредба за криптографската сигурност на класифицираната информация

Основни дефиниции за КИС и сигурност на КИС

Комуникационна и информационна система (КИС)

Съвкупност от технически (вкл. комуникационни средства, устройства за защита на границата, криптографски средства и среда за разпространение на сигнала в границите на системата) и програмни средства, методи, процедури и персонал, организирани за осъществяване на една или няколко от функциите по създаване, обработване, ползване, съхраняване и обмен на класифицирана информация в електронна форма.

Сигурност на КИС - Сигурността на КИС представлява система от принципи и мерки за защита от нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в КИС.

Органи по сигурността на КИС

На национално ниво:

- Държавна комисия по сигурността на информацията
- Орган по акредитиране на сигурността на КИС е Специализирана дирекция “Информационна сигурност“- ДАНС

В организационната единица:

- Служител по сигурността на КИС (СС на КИС)
- Орган по развитие и експлоатация на КИС (ОРЕ)
- Администратор по сигурността на КИС
- Администратор на КИС
- Потребители на КИС

Органи по сигурността на КИС на национално ниво

ДКСИ осъществява общ контрол по:

- **Защитата на КИ в КИС**
- **Процеса на акредитиране на КИС**

Органи по сигурността на КИС на национално ниво

ОАС

- *Дава препоръки и указания по сигурността на КИС;*
- *Препоръчва стандарти и средства, които могат да се използват в КИС за защита на КИ;*
- *Утвърждава документите по сигурността на КИС;*
- *Извършва комплексна оценка на сигурността на КИС;*
- *Издава сертификати за сигурност на КИС;*
- *Определя условията, при които следва да се извърши допълнително или ново акредитиране на КИС;*
- *Координира и контролира дейността по TEMPEST и определя контрамерките за защита на КИС от компрометиращи електромагнитни излъчвания (КЕМИ);*
- *Провежда обучение на служители по сигурността на КИС;*
- *Отнема и прекратява действието на сертификати за сигурност на КИС;*
- *Одобрява механизмите за защита на границата на КИС;*
- *Определя стандарти и списъци на одобрени продукти, които могат да се използват при избор на компоненти и устройства за защита на границата.*

Органи по сигурността на КИС в организационната единица

Служител по сигурността на КИС в ОЕ

- ***Създава необходимата организация и осъществява контрол на сигурността на КИС в ОЕ;***
- ***Координира изготвянето на документите по сигурността на КИС;***
- ***Съгласува изготвените документи по сигурността на КИС и ги предоставя на ССИ;***
- ***При случаи или съмнения за компрометиране сигурността на КИС:***
  - ***уведомява отговорните лица по сигурността на КИС в ОЕ;***
  - ***предприема действия за ограничаване или предотвратяване на вредите;***
  - ***участва в процеса по установяване и анализиране на обстоятелствата, свързани с компрометирането и докладва за резултатите на ССИ, който уведомява ОАС.***

Органи по сигурността на КИС в организационната единица

Орган по развитие и експлоатация на КИС в ОЕ

- ***Разработва и предлага изискванията за сигурност на КИС;***
- ***Изготвя документите по сигурността на всяка КИС;***
  Участва в подбора и тестването на техническите и програмни средства и механизмите за сигурност, използвани в КИС;
- ***Осигурява изпълнението на изискванията за акредитиране на КИС;***
  Определя мерките за сигурност и границите на отговорност при осъществяване на връзки с други КИС;
- ***Прави предложение за възлагане функции на администратор по сигурността на всяка КИС;***
- ***Организира и провежда обучение по сигурността на КИС;***
  Организира прилагането на одобрените мерки за сигурност в КИС;
- ***При междусистемна връзка на КИС извършва подбор на механизми за защита на границата.***

Органи по сигурността на КИС в организационната единица

Администратор по сигурността на КИС

(определя се за конкретна КИС)

Ясно разграничаване на задълженията на администратора по сигурността на КИС от администратора на КИС като не могат да се изпълняват от едно и също лице;

Участва в изготвянето и актуализирането на процедурите за сигурност на КИС;

Изготвя експлоатационни документи по сигурността на КИС на базата на утвърдените процедури за сигурност;

Изпълнява възложените му процедури по сигурност на КИС;
Предоставя на потребителите достъп до ресурсите на КИС в съответствие с предоставените им права;

Управлява, наблюдава и анализира одитните записи и осигурява тяхното резервиране и съхраняване в определените срокове;

Участва заедно със ССИ на КИС и ОРЕ в установяването на обстоятелствата по компрометирането на сигурността на КИС.

Органи по сигурността на КИС в организационната единица

Администратор

на КИС

(определя се за конкретна КИС)

- ***Лице с възложени функции и предоставени права по системно, приложно, мрежово и/или друго администриране в КИС;***
- ***Да притежава РДКИ до най-високото ниво на класификация за сигурност на информацията в КИС;***
- ***Да е преминало обучение в областта на сигурността на КИС;***
- ***Изпълнява задълженията, посочени в експлоатационните документи по сигурността на КИС;***
- ***Изпълнява указанията на администратора по сигурността на КИС, свързани със сигурността;***
- ***Уведомява администратора по сигурността на КИС за случаи или съмнения за компрометиране на сигурността ѝ.***

Органи по сигурността на КИС в организационната единица

Потребители в КИС

Да имат РДКИ до най-високо ниво на КИ, с която имат право да работят в КИС;

Да са преминали обучение в областта на сигурността на КИС;

Да имат предоставени права за достъп до ресурсите на КИС;

Да изпълняват задълженията, посочени в експлоатационните документи по сигурността на КИС, както и указанията на администратора по сигурността й;

Да уведомяват администратора по сигурността на КИС за случаи или съмнения за компрометиране на сигурността на КИС.

Акредитиране на КИС (1)
Условия и ред за акредитиране

1. В етапа на проектиране на КИС РОЕ подава до ОАС зявление за започване на процедура по акредитиране. Заявлението се изготвя от ОРЕ, съгласува се със ССИ и съдържа:

- Общи сведения за КИС, които включват:
  ниво на класификация, форма на представяне на информацията, очакван брой и типове потребители, среда на експлоатация и информация за планирано използване на криптографски средства;
- Общи сведения за връзки с други КИС и/или други системи, като: наименование на тези КИС; най-високо ниво на класификация на информацията в свързаните КИС; за всяка връзка – посока на обмен и нива на класификация на обменяната информация; предвиждани механизми за защита на границата; предвиждани информационни услуги, които ще се предоставят или ползват при междусистемната връзка с всяка от системите.
- Имената на ръководителя на ОРЕ и администратора по сигурността на КИС;
- Етапите и сроковете за изграждане на КИС.

Акредитиране на КИС (2)
Условия и ред за акредитиране

2. ОАС взема решение за откриване на процедура и уведомява писмено заявителя (в срок от 15 работни дни). В уведомлението се посочват сроковете за представяне на документите по сигурността съгласно чл. 32 от НСКИС, съобразени с етапите и сроковете за изграждане на КИС, условията, редът и етапите за акредитиране.

3. Заявителят изпраща до ОАС документите по сигурността на КИС съгласно чл. 32 от НСКИС и други документи, удостоверяващи изпълнението на отделните мерки за сигурност и сертификати за сигурност на отделни средства и подсистеми, ако има такива.

Акредитиране на КИС (3)
Условия и ред за акредитиране

4. Комплексна оценка на сигурността на КИС

Извършва се от комисия, назначена със съвместна заповед от ръководителите на ОАС и ОЕ.

Комисията:

- Проверява предоставените документи по сигурността;
- Проверява изпълнението на предвидените мерки за сигурност
- Изготвя протокол за резултатите от извършените проверки;

При установени несъответствия при проверките ОАС изисква от заявителя да ги отстрани.

Акредитиране на КИС (4)
Условия и ред за акредитиране

5. При положителна комплексна оценка ОАС издава сертификат за сигурност на КИС. Сертификат може да се издава и за обособени части на КИС.

Сертификатът съдържа: Идентификация на сертификата, правно основание за издаването му, идентификация на КИС, идентификация на заявителя, най-високо ниво на класификация за сигурност на информацията в КИС, срок на валидност, дата и място на издаване, подпис и печат.

6. Като неразделна част от сертификата, ОАС изготвя сертификационен отчет, съдържащ: общо описание на КИС; заключения от комплексната оценка; опис на представените документи по сигурността; видовете изменения, които изискват допълнително акредитиране; условията, изискващи повторна оценка на контрамерките по TEMPEST.

Сертификационният отчет се класифицира по реда на ЗЗКИ и ППЗЗКИ.

Акредитиране на КИС (5)
Условия и ред за акредитиране

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

8. Процедурата за издаване на такъв сертификат е описана в чл. 23 и чд. 24 от Наредбата за сигурността на КИС.

9. Когато КИС обхваща повече от една ОЕ, между тях се сключва споразумение, определящо коя ОЕ е организатор на КИС, границата на КИС и разпределението на отговорностите за съставните части на КИС, както и процеса за нейното акредитиране.

Документи по сигурността на КИС (1)

Документите по сигурността, необходими за извършване на акредитирането на всяка КИ съгласно чл. 32 от НСКИС, са:

1. Специфични изисквания за сигурност (СИС).
2. Процедури за сигурност, изготвени на основата на СИС.
3. При издаване на сертификат за сигурност за обособени части на КИС ОАС може да изиска допълнителни СИС и/или процедури за сигурност.

Документите по сигурността се класифицират по реда на ЗЗКИ и ППЗЗКИ.

Документи по сигурността на КИС (2) Специфични изисквания за сигурност (СИС)

- СИС се формулират по време на най-ранния стадий от проектирането на КИС и се детайлизират и развиват в процеса на разработване и изпълнение на проекта.
- При детайлизиране на изискванията ОРЕ взаимодейства с ОАС и съгласува с него прилаганите мерки за сигурност.
- СИС в завършен вид съдържат като отделни раздели: описание на конкретната КИС, описание на ГСС, ЛСС, ЕСС на КИС, **анализ на риска за сигурността на КИС**, мерките за сигурност; управление на сигурността при експлоатация на КИС, мерките за сигурност при критични ситуации и при прекратяване на експлоатацията на КИС, обособената част от КИС или междусистемна връзка.
- Документирането на а**нализа** на риска за сигурността на КИС се извършва в СИС, като описанието включва минимум приложената методология за анализ и оценка на резултатите от анализа.

Документи по сигурността на КИС (3) Процедури за сигурност (ПС)

- ПС са подробно описание на реда и отговорностите за изпълнение на дейностите при прилагането на утвърдените мерки за сигурност на КИС
- ПС съдържат раздели, свързани с:
  - Организация на сигурността;
  - Персонална, физическа, документална, компютърна, комуникационна сигурност, контрамерки по TEMPEST;
  - Действия при критични по отношение на сигурността ситуации;

При междусистемна връзка ПС на всяка КИС трябва да определят ред и отговорност за обмена на информация, свързана с инцидент със сигурността на КИС.

Общи изисквания за сигурност на КИС

Сигурността на КИС включва прилагане на балансирана система от мерки за сигурност в следните области:

1. Физическа сигурност;
2. Персонална сигурност;
3. Документална сигурност;
4. Комуникационна сигурност;
5. Криптографска сигурност,
6. Контрамерки по TEMPEST;
7. Компютърна сигурност;
8. Сигурност при свързване.

и с това се цели осигуряване на конфиденциалност, интегритет и достъпност на информацията в КИС.

Общи изисквания за сигурност на КИС
Физическа сигурност

- Ресурсите на КИС се разполагат в зони за сигурност клас I или клас II;
- Допуска се КИС, предназначени за работа с КИ, представляваща служебна тайна, да се разполагат в административни зони, като това не се отнася за критичното оборудване (сървъри, комуникационни и криптографски средства от комуникационна система, подсистеми за управление и друго оборудване, определено от анализа на риска).
- Зоните, в които са разположени ресурси на КИС, се защитават със съответни на най-високото ниво на класифицираната информация мерки, способи и средства за физическа сигурност.

За критичните от гледна точка на сигурността места се вземат допълнителни мерки.

Общи изисквания за сигурност на КИС
Персонална сигурност

- Потребителите в КИС трябва да имат РДКИ до най-високото ниво на класификация на информацията, с която имат право да работят в КИС.
- Служителите, на които е възложена дейността по развитието, управлението или сигурността на КИС, както и лицата, участващи в проектирането и изграждането на системата от мерки за сигурност на КИС, трябва да имат РДКИ до най-високото ниво на класификация на информацията в КИС.
- Правомощията им се определят така, че да не се допуска възможността едно лице да познава или контролира изцяло важните елементи от сигурността на конкретната КИС.
- Всички потребители преминават обучение по сигурността на КИС
- - Организира се от ОРЕ и се провежда за отделните категории служители съгласно чл. 46, ал. 2 от НСКИС;
- - Задължително за получаване достъп до КИС.

Общи изисквания за сигурност на КИС - Документална сигурност (1)

- Всички документи в КИС, съдържащи КИ, се идентифицират, маркират и контролират.
- Маркировката трябва да осигурява еднозначна информация за нивото на класификация при работа с тях.
- Начините за идентифициране, маркиране и контролиране се определят в документите по сигурността на конкретната КИС.
- Извеждането на документи, съдържащи КИ, от сертифицирани КИС, се извършва в съответствие с изискванията на ППЗЗКИ в зоните за сигурност.
- Пренос на документи, съдържащи КИ, от една КИС към друга се извършва само ако приемащата КИС е сертифицирана за ниво на класификация на информацията, същото или по-високо от нивото на пренасяните документи.

Общи изисквания за сигурност на КИС - Документална сигурност (2)

- Материалните носители за многократен запис на КИ, използвани в КИС, се маркират и регистрират в регистратурата.
- Регистрирането, маркирането, контролът и унищожаването на материалните носители за многократне запис на КИ се извършват по реда на ППЗЗКИ.
- Съхраняването и периодичният контрол на тези носители се извършват в съответствие с утвърдените процедури за сигурност на КИС.
- Материалите и записаната на хартиен носител информация (пароли, пин, кодове и др.), осигуряващи достъп до КИС или ресурси на КИС, се класифицират с ниво на класификация за сигурност на информацията, съответстващо на най-високото ниво на класификация на информацията, за която дават достъп. Унищожават се по реда, определен в документите по сигурността на КИС, а не по реда на ППЗЗКИ.
- Преносими компютърни устройства, предназначени за КИ, се маркират като носители на такава информация и се разглеждат като КИС или част от КИС. Пренасянето им извън зоните за сигурност се извършва по реда на ППЗЗКИ.

Общи изисквания за сигурност на КИС Комуникационна и криптографска сигурност, контрамерки по TEMPEST

- Комуникационната сигурност представлява система от мерки за защита на класифицираната информация при пренасяне по комуникационни системи;
- Класифицираната информация от КИС се пренася по комуникационни системи извън зоните за сигурност на КИС или административните зони, когато е защитена с одобрени криптографски средства;
- Форма на информация, получена след обработка на КИ с одобрени криптографски средства, не представлява КИ по смисъла на ЗЗКИ;
- КИС за класифицирана информация с ниво “Поверително” и по-високо трябва да са осигурени с контрамерки по TEMPEST.
- В КИС не се допуска безжичен пренос на КИ, освен в случаите, когато е защитена с одобрени криптографски средства.

Минимални изисквания за компютърна сигурност

- Еднозначна идентификация и автентификация на потребителя, предхождаща всички останали негови действия в КИС;
- Контрол на достъпа по преценка;
- Непрекъснат и синхронизиран по време запис на събития, свързани със сигурността на КИС (одитни записи) и изучаване на одитните записи с цел установяване на свързаните със сигурността действия на отделните субекти на КИС;
- Защита на одитните записи, свързани със сигурността, срещу неоторизиран преглед, промяна и изтриване;
- Обработка на обекти на конкретната КИС, така че при следващото им разпределяне към субект той да не може да установи предишното им съдържание или да получи права за достъп на използвалите ги преди това субекти;
- Актуална защита от вредни програмни средства.

Общи изисквания за сигурност на КИС
Сигурност по време на експлоатация (1)

- Експлоатацията и развитието на сертифицирана КИС се извършват в пълно съответствие с установените мерки и процедури за сигурност и при съблюдаване на условията за нейното допълнително акредитиране;
- ОРЕ, служителят и администраторът по сигурността на КИС в рамките на своите отговорности контролират и оценяват всички промени в ГСС, ЛСС, ЕС и съвместно предлагат изменение на мерките и процедурите за сигурност;
- Най-малко 6 месеца преди изтичане срока на валидност на издадения сертификат за сигурност на КИС, когато е необходимо да се продължи нейното експлоатиране, заявителят подава до ОАС заявление за ново акредитиране.

Общи изисквания за сигурност на КИС
Сигурност по време на експлоатация (2)

По време на експлоатацията и развитието на КИС:

- се извършва проверка на материалните носители за многократен запис на КИ за наличието на вредни програмни средства;
- се извършва резервиране на системната и одитна информация;
- се извършва инсталиране на одобрени елементи и конфигуриране на КИС само оторизирани служители;
- се внедряват технически и програмни средства или на техни версии след одобрение от ОРЕ;
- се организира и извършва сервизна дейност по начин, недопускащ компрометиране сигурността на КИС;
- се извършва ремонт на криптографски средства по реда на наредбата по чл. 85 от ЗЗКИ;
- **не се допуска използване на носители на информация, технически и програмни средства, които са лична собственост.**

Сигурност при свързване на КИС
Общи изисквания при свързване на КИС

Сигурността при свързване на КИС представлява система от мерки за защита от нерегламентиран достъп до КИ при осъществяването на междусистемна връзка с други системи, които могат да бъдат:

- КИС, сертифицирани за работа с КИ със същото или с различно ниво на класификация на информацията;
- информационни системи от затворен тип;
- системи с публичен достъп, като интернет и други подобни.

РОЕ взема решение за необходимостта от осъществяване на междусистемна връзка след отчитане на специфичните рискове за сигурността на системата, произтичащи от такава връзка.

За всяка междусистемна връзка на КИС с други системи между РОЕ, в чиято отговорност са системите, се сключва споразумение.

При междусистемна връзка на КИС за работа с КИ с ниво на класификация „За служебно ползване“ с публична мрежа като интернет споразумение не се сключва.

Сигурност при свързване на КИС
Механизми за защита на границата

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

Механизмите за защита на границата на КИС се одобряват от ОАС и трябва да осигуряват предоставяне само на услуги и преминаване само на потоци от информация, които са необходими за постигане на целите на свързването – принцип на минималност.

Реализират се чрез компоненти за защита на границата, които могат да бъдат програмни или технически средства.

Минималните изискванията към механизмите за защита на границата; планирането, одобряването и въвеждането в експлоатация на механизми за защита на границата при междусистемна връзка са регламентирани в глава шеста, раздели II и III на Наредбата за сигурността на КИС.

Сигурност при свързване на КИС

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

1. Информационните системи от затворен тип:

- не трябва да предоставят публичен достъп и да не са свързани към публични системи;
- трябва да имат определени лица с възложени отговорности по експлоатирането, развитието, управлението и сигурността на системата;
- трябва да имат документално установени правила за: достъп до електронната среда в системата; предоставянето на достъп до системата само на определена категория потребители; запис на събития и възможност за изучаване на одитните записи, свързани с успешни и неуспешни опити за достъп от всички категории потребители.

2. Междусистемна връзка на КИС към система с публичен достъп се реализира посредством доставчик на услуга – при сключен договор за осигуряване на достъпност, качество и защита на предоставяната услуга.

ДЕЙНОСТИ, СВЪРЗАНИ С КРИПТОГРАФСКАТА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Криптографска сигурност на класифицираната информация

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.

„Криптографско средство“ е средство, предназначено за защита на класифицирана информация чрез комбинация от криптографски методи, или средство за управление на криптографски ключове.

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

Наредба за криптографската сигурност на класифицираната информация

С наредбата се определят:

1. Органите за криптографска сигурност на КИ в РБ
2. Условията и редът за:

- използване на криптографски методи и средства за защита на КИ, производство, маркиране, съхраняване, разпределяне, пренасяне, използване и унищожаване на криптографски материали и на криптографски средства за защита на КИ;
- издаване на разрешения и удостоверения за работа с криптографски средства;
- одобрение на криптографски средства за защита на КИ;
- контрол по използване на криптографски методи и средства за защита на КИ.

Органи за криптографска сигурност на класифицираната информация

На национално ниво

- Държавна комисия по сигурността на информацията
- Орган по криптографската сигурност - ДАНС

В организационната единица

- Служител по криптографската сигурност (СКС)
- Администратор по криптографската сигурност (АКС)
- Потребител на криптографски средства (ПКС)

Органи за криптографска сигурност

ДКСИ

Осъществява общо ръководство и контрол на дейностите по криптографска сигурност

Държавна комисия по сигурността на информацията

Органи за криптографска сигурност

Орган по криптографската сигурност на Република България (ОКС) - ДАНС (1)

1. *прилага националната политика за криптографска сигурност в съответствие със ЗЗКИ, тази наредба и другите подзаконови актове по защита на КИ;*
2. *дава указания и задължителни предписания по всички аспекти на криптографската сигурност;*
3. *извършва одобрение на криптографски методи и средства за защита на КИ и периодичен анализ за установяване на тяхната способност да защитават КИ, 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. *произвежда и разпределя ключови материали за криптографските мрежи на РБ;*
6. *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 КИ;*
7. *координира и контролира използването, производството и вноса на средства за криптографска защита на КИ;*

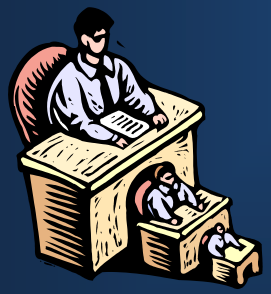
Органи за криптографска сигурност

Орган по криптографската сигурност на Република България (ОКС) - ДАНС (2)

8. провежда обучение в областта на криптографската сигурност и издава разрешения за работа с криптографски средства (КС);
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. води регистри на одобрените криптографски средства и мрежи, поекземплярно проверените криптографски средства и разрешенията за работа с криптографски средства;

Органи за криптографска сигурност в организационната единица

Служител по криптографската сигурност (СКС)



Да е служител на ОЕ, определен със заповед на РОЕ. При необходимост могат да бъдат повече от един.

Да притежава РДКИ до ниво "Строго секретно";
Да е получило разрешение за работа с криптографски средства;

Организира изготвянето на криптоплановете в ОЕ, които се утвърждават от ОКС;

Организира и осъществява подготовката на администраторите по криптографската сигурност и потребителите на криптографски средства;

Организира процедурата по снабдяване и водене на отчет на криптографските средства и криптографските материали в ОЕ;

Участва в установяване на обстоятелства, свързани с компрометиране на криптографската сигурност.

Органи за криптографска сигурност в организационната единица

Администратор по криптографската сигурност (АКС)

- *РОЕ по предложение на ССИ с писмена заповед възлага функции на администратор по криптографската сигурност ;*
- *Получил е удостоверение за работа с криптографски средства;*
- *Организира въвеждането в експлоатация на криптографската мрежа и осигурява снабдяването с криптографски материали, необходими за работа на криптографската мрежа;*
- *Контролира съхраняването, използването и унищожаването на криптографските материали;*
- *Контролира спазването на правилата за експлоатация на криптографските средства и криптоплана от потребителите и ги информира периодично за техните задължения;*
- *Участва заедно със служителя по криптографската сигурност в установяването на обстоятелствата, свързани с компрометирането на криптографската сигурост.*

Органи за криптографска сигурност в организационната единица

Потребител на криптографски средства

Определя се със заповед на РОЕ по предложение на служителя по сигурността на информацията;

Да е получил удостоверение за работа с криптографски средства;

Обработва КИ с криптографски средства;

Експлоатира криптографските средства при спазване на криптоплана;

Информира администратора по криптографската сигурност за всеки случай на неизправна работа на криптографските средства или компрометиране на криптографската сигурност.

Въвеждане в експлоатация на криптографски мрежи (1)

1. При взето решение от РОЕ за използване на криптографски средства (КрС):
   - РОЕ изпраща заявление до ОКС.
   - ОКС дава или отказва съгласие за използване на КС (в срок от 15 работни дни)
2. За въвеждане в експлоатация на криптографски мрежи е необходимо предварително да са налице:
   - одобрени и поекземплярно проверени КрС от ОКС;
   - администратор по криптографската сигурност и при необходимост потребители на КрС в ОЕ;
   - изпълнени изисквания по физическа и документална сигурност;
   - изпълнени изисквания за експлоатация на КрС;
   - изпълнени условия за експлоатация на криптографските средства;
   - утвърден от ОКС криптоплан, включващ организационни правила и правила за техническа експлоатация в областта на криптографската сигурност и план за действие при критични ситуации.

Въвеждане в експлоатация на криптографска мрежа (2)

3. Въвеждането в експлоатация на КрС и криптографска мрежа се одобрява с решение на комисия.

4. Комисията се назначава със съвместна заповед на ОКС и на ОЕ.

5. Решението съдържа:

- идентификация на одобрените криптографски средства (КрС);
- нивото за сигурност на КИ, която може да се защитава с одобрените КрС;
- задължителните условия за експлоатация, при които е гарантирана защитата на класифицираната информация;
- физическото разположение на криптографските средства по места и предприетите мерки по физическа и документална сигурност.

6. Когато криптографската мрежа обхваща повече от една ОЕ, между тях се сключва споразумение, определящо коя ОЕ е организатор на мрежата.

Експлоатация на криптографски средства (КрС)

- Експлоатацията на КрС и на криптографските ключове се извършва в съответствие с правилата за работа с тях и криптоплана;
- КрС се експлоатират в условия на осигурени мерки за физическа и документална сигурност. Нови КрС – след поекземплярна проверка от ОКС. Транспорт – с изтрити криптографски ключове;
- Криптографски ключове – проверка на защитната им опаковка, съхраняване, ред за унищожаване;
- Ремонт на криптографски средства – СКС уведомява писмено ОКС, ремонт - на територията на Р България, недопускане нерегламентиран достъп до класифицирана информация;
- Контролът по използването на КрС се извършва от ОКС и от служителите и администраторите по криптографската сигурност.
- СКС и АКС осъществяват текущ контрол по използването на КрС

Прекратяване експлоатацията на криптографски средства

Извършва се:

- При отпадане на необходимостта от използване на криптографските средства в организационната единица, за което писмено се уведомява ОКС;
- При установяване на неспособност на експлоатираните криптографски средства да осигуряват необходимото ниво на защита на класифицираната информация, което се удостоверява от ОКС;
- При компрометиране на криптографската сигурност след издадено писмено становище от ОКС.

Унищожаването на криптографски средства се извършва от комисия, назначена с писмена заповед на РОЕ. В нея задължително се включват служителят по криптографската сигурност и администратор по криптографската сигурност.

Производство, маркиране, съхраняване, разпределение, пренасяне и използване на ключови материали

Производството и разпределянето на ключови материали за криптографските мрежи в РБ се извършва от ОКС или от ОЕ, на които е дадено такова разрешение.

Съхраняването и разпределянето на криптографските материали се извършва в криптографска регистратура, която трябва да бъде разположена в зона за сигурност.

Съхраняването на криптографските материали в регистратурите се извършва в каси, а отчитането им – в отделни регистри.

Пренасянето на криптографски материали се извършва по реда за пренасяне на материали, съдържащи КИ, регламентиран в ППЗЗКИ.

Действия при компрометиране на криптографската сигурност

При съмнения или компрометиране на криптографската сигурност ССИ в ОЕ:

- взема мерки за предотвратяване или ограничаване на вредните последствия;
- незабавно информира ОКС и ОЕ – организатор на криптографската мрежа, ако събитието се е случило в различна от нея ОЕ.

По предложение на ССИ РОЕ назначава комисия за установяване на обстоятелствата, свързани с компрометирането на криптографската сигурност.

- в комисията задължително се включват СКС и АКС;
- резултатите от работата на комисията се отразяват в протокол;
- протоколът се предоставя на РОЕ, а копие от него се изпраща в ОКС.

Въз основа на протокола ОКС изготвя писмено становище, което се изпраща до ДКСИ и до организационната единица.

Разрешения и удостоверения за работа с криптографски средства

Разрешение за работа с криптографски средства се издава от ОКС на служител от организационната единица, определен да изпълнява задълженията на служител по криптографската сигурност.

Разрешението за работа с криптографски средства се издава за срок 5 години.

Удостоверение за работа с криптографски средства се издава от служителя по криптографската сигурност на служител в ОЕ, определен да изпълнява задълженията на администратор по криптографската сигурност, завеждащ криптографска регистратура или потребител на криптографски средства.

Удостоверение за работа с криптографски средства се издават за срок до 5 години.

Обучение по криптографска сигурност (1)

Обучението по криптографска сигурност включва:

- обучение по организационните принципи и правила за криптографска сигурност;
- обучение за работа с конкретни криптографски средства.

Обучението по организационните принципи и правила за криптографска сигурност се извършва от:

- ОКС - на служителите по криптографската сигурност;
- ОКС или от служителите по криптографската сигурност - на администраторите по криптографската сигурност;
- служителите или администраторите по криптографската сигурност - на други администратори по криптографската сигурност, на завеждащите криптографска регистратура и на потребителите на криптографски средства.

Успешно преминалите обучение получават свидетелство, което се издава за срок не по-дълъг от 5 години.

Обучение по криптографска сигурност (2)

Обучението за работа с конкретни криптографски средства се извършва от:

- доставчици или производители на криптографски средства;
- служители на ОКС, служители и администратори по криптографската сигурност, на които доставчикът или производителят е дал право да провеждат обучение.

На служителите от организационните единици, преминали успешно обучение за работа с конкретни криптографски средства, доставчиците или производителите на криптографски средства издават документ, в който се посочва:

- видът на криптографското средство, за което е проведено обучението;
- правото за провеждане на обучение, ако такова е дадено.

Държавна комисия по сигурността на информацията

Възможност за съвместяване на функции по сигурността на КИС и криптографската сигурност

Служител по сигурността на информацията
Служител по сигурността на КИС
Служител по криптографската сигурност

Служител по сигурността на КИС
Администратор по сигурността на КИС

Администратор по сигурността на КИС
Администратор по криптографската сигурност

Системен администратор
Приложен администратор