Формуляр за частична предварителна оценка на въздействието* * Приложете към формуляра допълнителна информация/документи	
Институция: **Държавна агенция „Национална сигурност“**	**Нормативен акт:** **Проект на Постановление на Министерския съвет за приемане на Наредба за сигурността на комуникационните и информационните системи**
За включване в законодателна/оперативната програма на Министерския съвет за периода: **01 юли - 31 декември 2019 г.**	**Дата:** **05.08.2019г.**
Контакт за въпроси: Михаил Чиллев	**Телефон: 02/8147847**

Дефиниране на проблема:

1.1. Кратко опишете проблема и причините за неговото възникване. Посочете аргументите, които оправдават нормативната промяна.

Необходимостта от приемане на Наредба за сигурността на комуникационните и информационните системи е породена в резултат от изменението и допълнението на Закона за защита на класифицираната информация (ЗЗКИ) (обн., ДВ, бр. 88 от 2018г.) във връзка със синхронизиране и адаптиране на българското законодателство с европейската стратегическа рамка (Политика за сигурност по отношение на осигуреността на информацията от гледна точка на междусистемните връзки - IASP 3 и Политика за сигурност във връзка с осигуреността на информацията по ТЕМПЕСТ - IASP 7) и тази на НАТО (AD 070-001 ACO Security Directive, AC/322-D/0030-REV5, AC/322-D(2010)0049 и SDIP-27), произтичащо от членството ни в Европейския съюз и НАТО.

Предвидените промени в законовата уредба са свързани със сигурността на автоматизираните информационни системи или мрежи, използвани за работа с класифицирана информация, както и запълване на празноти по отношение на регулирането на свързаността между автоматизираните информационни системи (АИС) за обработка на класифицирана информация с АИС за некласифицирана информация, в т.ч. и с публични мрежи.

Основни изменения и допълнения, предвидени в ЗЗКИ, които налагат приемането на Наредба от Министерския са съвет, са в следните насоки:

1. Разрешено е да има междусистемна връзка на КИС, предназначени за класифицирана информация до ниво „Секретно” включително, с други КИС за класифицирана информация със същото или различно ниво на класификация, както и към информационни системи от затворен тип при условията, посочени в наредбата по чл. 90, ал. 1;

2. Разрешено е да има междусистемна връзка на КИС, предназначени за класифицирана информация с ниво „За служебно ползване”, към Интернет и/или други публични мрежи при условията, посочени в наредбата по чл. 90, ал. 1;

3. Не е разрешено да има междусистемна връзка на КИС, предназначени за класифицирана информация с ниво „Поверително” и „Секретно” с КИС,

предназначени за класифицирана информация с ниво „За служебно ползване”, които са свързани към Интернет и/или други публични мрежи;

4. Не е разрешено да има междусистемна връзка на КИС, предназначени за класифицирана информация с ниво „Строго секретно”;

5. Междусистемната връзка е разрешена само когато:

5.1. В КИС са приложени механизми за защита на границата, одобрени от Държавна агенция „Национална сигурност”, по реда и при условията определени с наредбата по чл. 90, ал. 1.

5.2. КИС притежават издаден валиден сертификат по чл. 14, т. 2.

6. В ЗЗКИ са въведени следните изменения и допълнения по отношение на терминологията:

- терминът „АИС или мрежи” е заменен с „КИС”;

- въведено е определение за „Граница на КИС”;

- въведено е определение за „Междусистемна връзка”;

- въведено е определение за „Механизъм за защита на границата”;

- въведено е определение за „Информационна система от затворен тип”;

- въведено е определение за „Компрометиращи електромагнитни излъчвания”;

- въведено е определение за TEMPEST;

- въведено е определение за „Контрамерки по TEMPEST”;

- отпаднали са термините „Автоматизирани информационни системи“ и „Автоматизирани информационни мрежи“.

Разпоредбата на чл. 90, ал. 1 от ЗЗКИ съдържа законова делегация, съгласно която задължителните общи условия за сигурност на КИС да бъдат определени в наредба, приета от Министерския съвет по предложение на Държавна агенция „Национална сигурност“ (ДАНС).

Съгласно чл. 7, ал. 2 от Закона за нормативните актове наредбата е нормативен акт, който се издава за прилагане на отделни разпоредби или подразделения на нормативен акт от по-висока степен.

Действащата Наредба за задължителните общи условия за сигурност на автоматизирантие информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация не е в съответствие с новоприетите законови положения, което е в противоречие на чл. 15, ал. 1 от Закона за нормативните

актове, съгласно който нормативният акт трябва да съответства на Конституцията на Република България и на другите нормативни актове от по-висока степен.

Преодоляването на горепосоченото несъответствие следва да стане чрез приемане на Наредба за сигурността на комуникационните и информационните системи, която да бъде приета с Постановление на Министерския съвет по предложение на председателя на ДАНС. Съществуващото несъответствие между ЗЗКИ и подзаконовата нормативна уредба в областта на сигурността на КИС не може да бъде преодоляно чрез използването на организационни, технически или други мерки.

1.2. Опишете какви са проблемите в приложението на съществуващото законодателство или възникналите обстоятелства, които налагат приемането на ново. Посочете възможно ли е проблемът да се реши в рамките на съществуващото законодателство чрез промяна в организацията на работа и/или въвеждане на нови технологични възможности (например съвместни инспекции между няколко органа и др.)

Предвидените в ЗЗКИ изменения и допълнения са съществени и важни по своята същност, поради което са констатирани проблеми, свързани с неясноти и противоречия между законова и подзаконова нормативна уредба, които водят до затруднения и невъзможност в отделни случаи да бъде постигнато правилно и законосъобразно прилагане на ЗЗКИ по отношение на сигурността на КИС.

В тази връзка констатираните проблеми, които не могат да бъдат преодолени по друг начин, освен с приемането на Наредба за сигурността на комуникационните и информационните системи, както следва:

- В действащата Наредба не е наличен регламент относно свързването на КИС за обработка на класифицирана информация с такива за некласифицирана информация или Интернет, което възпрепятства изпълнение на функционалните задължения на организационната единица (ОЕ), включително по осигуряване на националната сигурност и отбраната на Република България и изпълнението на конкретни задачи, свързани с членството в ЕС и НАТО (например при участие в съвместни мисии и/или операции). Необходимо е подробно да бъдат регламентирани общите изисквания при свързване на КИС, планирането, одобрение и въвеждане в експлоатация на механизми за защита на границата при междусистемна връзка, изискванията за сигурност при осъществяване на междусистемна връзка към информационни системи от затворен тип и към системи с публичен достъп.
- Фигурата на администратор на КИС не е достатъчно изчерпателно уредена в действащата Наредба, което налага изменения и допълнения на разпоредбите в тази връзка, като бъдат регламентирани неговите функции, задачи и правомощия.
- Предвид съвременните предизвикателства пред сигурността на КИС е необходимо от актуализиране на изискванията към сигурността, минималните изисквания за компютърна сигурност и одитните записи.
- Преодоляване на неясноти, констатирани при прилагането на отделни разпоредби от действащата Наредба, което налага нормативни промени и прецизиране на отделни разпоредби в следните насоки:
- по-подробно описание на функциите на служителите по сигурността на КИС;
- по отношение на ръководителя на организационната единица да определя със заповед ръководител и състав на орган по развитие и експлоатация на КИС (ОРЕ на КИС) в организационната единица;

- определяне на изискванията към администратора на КИС;

- определяне на по-детайлна и ясна процедура по отношение издаването на сертификат за сигурност на КИС преди завършване на процеса на акредитиране;

- регламентиране на изискване към ръководителя на организационната единица, още в етапа на проектиране на КИС, да подава до органа по акредитиране на сигурността (ОАС) на КИС информация за планирано използване на криптографски средства (тип криптографски средства и описание на предвижданата организация на тяхното използване) и общи сведения за връзки с други КИС и/или други системи, които включват:

а) наименования на свързаните КИС и/или други системи;

б)максималното най-високото ниво на класификация на информацията в свързаните КИС;

в) за всяка връзка посоката на обмен и нива на класификация на информацията, която ще се обменя;

г) предвиждани информационни услуги, които ще се предоставят или ползват при междусистемната връзка с всяка от системите;

д) предвиждани механизми за защита на границата.

С оглед преодоляване на обсъдените проблеми и съгласно чл. 90, ал. 1 от ЗЗКИ се налага необходимостта от приемане на Наредба за сигурността на КИС, като не са налице други начини за решаване на проблемите чрез промяна на начина на работа или други технологични възможности.

1.3. Посочете дали са изготвени последващи оценки на нормативния акт или анализи за изпълнението на политиката и какви са резултатите от тях?

Не са изготвяни последващи оценки на нормативния акт, както и анализи на неговото изпълнение.

2. Цели:

Посочете целите, които си поставя нормативната промяна по конкретен и измерим начин и график за тяхното постигане. Съответстват ли целите на действащата стратегическа рамка?

Целта на приемането на предложения акт е разпоредбите на подзаконовите нормативни актове да бъдат приведени в съответствие със законовите разпоредби на ЗЗКИ, като по този начин ще бъде изпълнено императивното изискване, регламентирано в чл. 15, ал. 1 от ЗНА.

Използваната терминология в подзаконовата нормативна уредба по отношение на сигурността на КИС ще бъде синхронизирана с въведената и използвана в ЗЗКИ.

Ще бъде регламентирано свързването на КИС с други КИС, както и с информационни системи за некласифицирана информация или Интернет.

С приемането на предложения проект на ПМС за приемане на Наредбата за сигурността на КИС ще се постигне допълване и/или прецизиране на разпоредби, при прилагането на които е констатирана необходимост от промяна или разширяване на техния обхват, както и изменение и допълнения на отделни разпоредби, за които е установено противоречиво тълкуване или неефективно прилагане.

Ще бъде внесена по-голяма яснота при определяне на процедурите по акредитиране на КИС, когато същите са свързани с процедура по одобрение на криптографски мрежи.

3. Идентифициране на заинтересованите страни:

Посочете всички потенциални засегнати и заинтересовани страни, върху които предложението ще окаже пряко или косвено въздействие (бизнес в дадена област/всички предприемачи, неправителствени организации, граждани/техни представители, държавни органи, др.).

Преки заинтересовани страни:

- ДКСИ, ДАНС и всички организационни единици по смисъла на § 1, т. 3 от Допълнителните разпоредби на ЗЗКИ.

Косвени засегнати и заинтересовани страни:

- Държавни органи, организации, юридически лица със стопанска и нестопанска цел, граждани и бизнеса, включително чрез техните организации, в качеството им на заинтересовани страни в отделни случаи (като участници в обществените консултации).

4. Варианти на действие:

Идентифицирайте основните регулаторни и нерегулаторни възможни варианти на действие от страна на държавата, включително и варианта „без намеса“.

Вариант за действие 1 „Без действие“:

В случай че не се приеме предложения проект на ПМС за приемане на Наредба за сигурността на КИС, няма да бъде актуализирана и приведена подзаконовата нормативна уредба в съответствие със ЗЗКИ.

Няма да бъде регламентиран начинът, по който следва да бъде осъществено свързване на КИС или КИС и информационни системи от затворен тип и интернет, като условията за това свързване следва да уредени в Наредбата по чл. 90, ал. 1 от ЗЗКИ.

Неприемането на Наредбата за сигурността на КИС ще доведе до невъзможност за изпълнение на функционалните задължения при някои от организационните единици;

Констатираните неясноти и затруднения при прилагането на отделни разпоредби от действащата Наредба няма да бъдат преодолени и ще продължат да затрудняват практическото прилагане на разпоредбите по отношение на сигурността на КИС.

Въведената нова терминология в законовите разпоредби ще е различна с тази, използвана в подзаконовите разпоредби, което ще доведе до неправилно тълкуване и прилагане на отделни разпоредби в процеса на акредитация при свързване на две и повече системи за обработване на класифицирана информация. Няма да бъде уеднаквена терминологията с тази, която е използвана в ЕС и НАТО.

Без наличен регламент ще бъде невъзможно свързването на КИС за обработка на класифицирана информация с такива за некласифицирана информация или интернет, поради което някои организационни единици няма да имат възможност за изпълнение на функционалните си задължения, включително по осигуряване на националната сигурност и отбраната на Република България и изпълнението на конкретни задачи, свързани с членството в ЕС и НАТО (например при участие в съвместни мисии и/или операции).

Вариант за действие 2 „Приемане на постановлението“:

В случай че бъде приет предложеният проект на ПМС за приемане на Наредба за сигурността на КИС, това ще доведе до:

- прецизиране и допълване на терминологията и определенията, което ще доведе до ясно и недвусмислено дефиниране на области, подпомагащи процеса на акредитация при свързване на две и повече системи за обработване на класифицирана информация, ще се въведе и новата терминология относно TEMPEST;
- ясно разпределение на отговорностите по сигурността на КИС между длъжностните лица, действията при компрометиране или съмнения за компрометиране, както и за провеждане на обучения на потребителите в КИС;
- определяне на правила и процедури, които да регулират свързаността между КИС, предназначени за обработване на класифицирана информация със системи за некласифицирана информация (включително Интернет), както и между КИС с различни нива на класификация на информацията, обработвана в тях, което беше забранено преди промените в закона;
- промяна на регламента по отношение на задължителните документи по сигурността на КИС. Промяната е продиктувана от необходимостта да се позволи на ОЕ да изготвят документите по сигурността в съответствие със сложността и обхвата на системата, като участие в определянето на обхвата на документите да има и ОАС;
- промяна на изискванията по отношение извършване и документиране на анализа на риска за КИС, като основна цел на промяната е постигане на ефективен процес на управление на риска;
- определяне на изискванията за сигурност съобразно извършен анализ на риска за съответна КИС, което е от значение и за структурата и съдържанието на специфичните изисквания за сигурност на КИС и структурата и съдържанието на процедурите за сигурност на КИС;
- въвеждане на срок, за който се издават сертификати за сигурност на КИС с ниво „За служебно ползване”. Необходимостта от въвеждане на срок е породена от повечето възможни рискове за КИС, породени от възможността за междусистемна връзка на същите;
- въвеждане на прекратяване на сертификат на КИС, без да е необходимо издаването на индивидуален административен акт, при изтичане на срока му на валидност;
- по-подробно описание на функциите на служителите по сигурността на КИС, което ще внесе яснота при разбирането относно необходимостта от разделяне на функциите по сигурността на КИС между различни категории служители;
- определяне на това, че ръководителят на организационната единица определя със заповед ръководител и състав на ОРЕ в организационната единица. Липсата на такава разпоредба до този момент предизвикваше неразбиране и наличие на различни практики при ОЕ;
- определяне на изискванията към администратора на КИС. Разпоредбата е необходима за внасяне на допълнителна яснота и точно разбиране на функциите на администратора;
- определяне на по-детайлна и ясна процедура по отношение издаването на сертификат преди завършване на процеса на акредитиране. Действащата процедура не предоставя механизъм за какъвто и да е предварителен контрол на приложените мерки за сигурност преди издаването на сертификат, което предоставяше възможност ОАС да издаде такъв сертификат без да има увереност, че са приложени минимални изисквания за сигурност;
- определяне на изискване към ръководителя на организационната единица, който още в етапа на проектиране на КИС да подава до ОАС информация за:

- планирано използване на криптографски средства (тип криптографски средства и описание на предвижданата организация на тяхното използване) и общи сведения за връзки с други КИС и/или други системи. Информацията е необходима на ОАС, за да бъдат обвързани процедурата по акредитиране на КИС с процедурата по въвеждане в експлоатация на криптографска мрежа, което е от значителна важност за постигане на достатъчно ниво на сигурност в КИС;

5. Негативни въздействия:

Опишете качествено (при възможност – и количествено) всички значими потенциални икономически, социални, екологични и други негативни въздействия за всеки един от вариантите, в т.ч. разходи за идентифицираните заинтересовани страни в резултат на предприемане на действията. Пояснете кои разходи се очаква да бъдат второстепенни, и кои да са значителни.

Вариант за действие 1 „Без действие“:

Неприемането на проект на ПМС за приемане на Наредба за сигурността на КИС ще се отрази негативно на процеса по актуализиране и привеждане в съответствие на подзаконовата нормативна уредба със ЗЗКИ.

Няма да бъде регламентиран начинът, по който следва да бъде осъществено свързване на КИС или КИС и информационни системи от затворен тип и интернет, като условията за това свързване следва да уредени в Наредбата по чл. 90, ал. 1 от ЗЗКИ.

Неприемането на Наредбата за сигурността на КИС ще доведе до невъзможност за изпълнение на функционални задължения при някои от организационните единици;

Констатираните неясноти и затруднения при прилагането на отделни разпоредби от действащата Наредба няма да бъдат преодолени и ще продължат да създават затруднение при практическото прилагане на разпоредбите по отношение на сигурността на КИС.

Употребяваната терминология в законовите и подзаконовите разпоредби ще бъде различна, което ще доведе до неясно и двусмислено тълкуване на отделни разпоредби в процеса на акредитация при свързване на две и повече системи за обработване на класифицирана информация. Няма да бъде уеднаквена терминологията с тази, използвана в НАТО и ЕС.

Без наличен регламент ще бъде невъзможно свързването на КИС за обработка на класифицирана информация с такива за некласифицирана информация или интернет, поради което някои организационни единици няма да имат възможност за изпълнение на функционалните си задължения, включително по осигуряване на националната сигурност и отбраната на Република България и изпълнението на конкретни задачи, свързани с членството в ЕС и НАТО (например при участие в съвместни мисии и/или операции).

Вариант за действие 2 „Приемане на постановлението“:

Няма негативни икономически, социални, екологични и други негативни въздействия нито за преките, нито за косвените заинтересовани страни.

6. Ползи:

Опишете качествено (при възможност – и количествено) всички значими потенциални икономически, социални, екологични и други ползи за идентифицираните заинтересовани страни за всеки един от вариантите в резултат на предприемане на действията. Посочете как очакваните ползи кореспондират с формулираните цели.

Вариант за действие 1 „Без действие“:

При този вариант не са идентифицирани ползи

Вариант за действие 2 „Приемане на постановлението“:

Заинтересованите страни, ще имат възможност да свързват КИС за обработка на класифицирана информация с такива за некласифицирана информация или Интернет, което ще е от особена полза особено за системи, събиращи и изобразяващи информация в реално време. С определянето на ред за осъществяване на свързаност на КИС за обработка на класифицирана информация с такива за некласифицирана информация или Интернет, ще се предостави възможност за по-ефективно и ефикасно изпълнение на функционални задължения на ОЕ, включително по осигуряване на националната сигурност и отбраната на Република България и изпълнението на конкретни задачи, свързани с членството в ЕС и НАТО (например при участие в съвместни мисии и/или операции).

Промяната на терминологията в областта на сигурността на КИС ще доведе до значително облекчаване на процеса по акредитиране и до по-ясно разбиране от ОЕ на процеса по акредитиране.

Ще бъдат прецизирани и разширени разпоредбите на подзаконовата нормативна база, което ще доведе до по-ясно и недвусмислено тълкуване.

7. Потенциални рискове:

Посочете възможните рискове от приемането на нормативната промяна, включително възникване на съдебни спорове.

Не са идентифицирани рискове от приемането на постановлението, включително възникване на съдебни спорове.

8.1. Административната тежест на физическите и юридическите лица:

☐Ще се повиши

☐Ще се намали

☑Няма ефект

8.2. Създават ли се нови регулаторни режими? Засягат ли се съществуващи режими и услуги?:

Не се създават нови регулаторни режими. Съществуващите контролни дейности от страна на органите на ДАНС ще бъдат прецизирани с цел гарантиране защитата на класифицираната информация във връзка с КИС.

9. Създават ли се нови регистри:

Ако отговорът е „да“ посочете колко и кои са те…

Не се създават нови регистри.

10. Въздействие върху микро, малки и средни предприятия (МСП):

☐Актът засяга пряко МСП

☐Актът не засяга МСП

☑Няма ефект

Приемането на ПМС няма да има ефект върху микро-, малките и средните предприятия, тъй като не се предвиждат промени, които да имат отношение към стопанската и икономическата дейност, търговията и инвестициите, поради което не следва да се очакват преки ефекти за МСП при приемането на акта.

11. Проектът на нормативен акт изисква цялостна оценка на въздействието:

☐Да

☑Не

12. Обществени консултации:

Обобщете най-важните въпроси за обществените консултации, посочете индикативен график за тяхното провеждане и видовете консултационни процедури.

Проектът на постановление ще бъде публикуван за обществени консултации за срок от 30 дни на Интернет страницата на Държавна агенция „Национална сигурност“ и на Портала за обществени консултации на Министерския съвет в съответствие с изискването на чл. 26 от Закона за нормативните актове. Справката за отразените становище ще бъде публикувана на Интернет страницята на ДАНС и на портала за обществени консултации на Министерския съвет.

13. Приемането на нормативния акт произтича ли от законодателството на ЕС:

☐Да

☑Не

Моля посочете изискванията за законодателството на ЕС, включително информацията по т.8.1. и 8.2., дали е извършена оценка на въздействието на ниво ЕС и я приложете (или връзка към източник)

14. Подпис на директор на дирекция, отговорна за изработването на нормативния акт:

Име и длъжност: Виолета Дъчева – директор на Специализирана дирекция „Информационна сигурност“ на Държавна агенция „Национална сигурност“

Дата: 05.08.2019 г

Подпис: