

НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ

В сила от 25.11.2008 г.

Приета с ПМС № 279 от 17.11.2008 г.

Обн. ДВ. бр.101 от 25 Ноември 2008г., изм. ДВ. бр.58 от 30 Юли 2010г., изм. ДВ. бр.102 от 30 Декември 2010г., изм. и доп. ДВ. бр.48 от 31 Май 2013г.

Глава първа. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С наредбата се уреждат:

1. общите изисквания за оперативна съвместимост и мрежова и информационна сигурност за нуждите на предоставянето на вътрешни електронни административни услуги и обмяна на електронни документи между администрациите;
2. воденето, съхраняването и достъпът до регистъра на стандартите;
3. (отм. - ДВ, бр. 48 от 2013 г.)
4. Методиката за извършване на оценка за съответствие с изискванията за оперативна съвместимост и мрежова и информационна сигурност;
5. (изм. - ДВ, бр. 48 от 2013 г.) начинът на удостоверяване съответствието на внедряваните от административните органи информационни системи с установените нормативни изисквания за оперативна съвместимост и информационна сигурност и вписването им в списъка на информационните системи, чието съответствие е удостоверено по реда на наредбата.

(2) Наредбата не урежда мрежовата и информационната сигурност на информационните системи на административните органи и правилата за информационна сигурност при използване на класифицирана информация.

Чл. 2. (1) Задълженията на административните органи по наредбата се прилагат и по отношение на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, при предоставяне на вътрешни електронни административни услуги, освен ако в закон е предвидено друго.

(2) (Изм. - ДВ, бр. 48 от 2013 г.) Прилагането на разпоредбите на глава трета и използването на информационни системи, удостоверени по реда на наредбата, могат да се прилагат от лицата, осъществяващи публични функции, и от организациите, предоставящи обществени услуги.

Чл. 3. Спазването на изискванията за оперативна съвместимост и мрежова и информационна сигурност се гарантира чрез:

1. (изм. - ДВ, бр. 48 от 2013 г.) удостоверяване съответствието на информационните системи и продукти в съответствие с глава шеста;
2. функционалността на единната среда за обмен на електронни документи (ЕСОЕД), която допуска обмен само на видове документи, вписани в регистъра на информационните обекти, и със съдържание, отговарящо на вписаните в регистъра изисквания;
3. сертификация и одит на администрациите по отношение на система за управление на

информационната сигурност, в съответствие с международния стандарт ISO 27001:2005;

4. (изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) контрол от страна на министъра на транспорта, информационните технологии и съобщенията в изпълнение на чл. 60 от Закона за електронното управление.

Глава втора. ОПЕРАТИВНА СЪВМЕСТИМОСТ

Раздел I.

Изисквания за свързаност между информационните системи на административните органи

Чл. 4. (1) Администрациите са длъжни да изпращат и да получават електронни документи помежду си за нуждите на предоставяне на вътрешни електронни административни услуги чрез ЕСОЕД.

(2) Изключения по ал. 1 се допускат:

1. когато администрацията не разполага с техническа възможност за обмен на документи през ЕСОЕД;

2. когато ЕСОЕД не функционира вследствие на технически неизправности, профилактика или други причини.

Чл. 5. (1) Когато електронни документи се изпращат по изключение чрез отворени мрежи, комуникационните интерфейси и протоколите за обмен трябва да съответстват на задължителните стандарти и нормативните актове, вписани в раздел "Комуникация и процедури за обмен" на регистъра на стандартите.

(2) В случаите по ал. 1, когато документи се изпращат онлайн по стандартизиран протокол чрез публичнодостъпно уеббазирано приложение, комуникационните интерфейси и протоколите за обмен трябва да съответстват на задължителните стандарти, вписани в регистъра на стандартите.

Чл. 6. (1) Директна връзка между информационни системи на различни административни органи се допуска само в случаи, когато техническите средства, работещи в условията на оперативна съвместимост, не удовлетворяват особени изисквания за интегритет, бързо действие и конфиденциалност.

(2) Изграждането на директни връзки по ал. 1 не отменя задължението за предоставяне на услуги към други администрации чрез ЕСОЕД.

(3) Изграждането на директни връзки по ал. 1 се извършва в съответствие с Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, приета с Постановление № 101 на Министерския съвет от 2008 г. (ДВ, бр. 48 от 2008 г.).

Чл. 7. (*) (Предишен текст на ал. 2, изм. - ДВ, бр. 48 от 2013 г.) Използването на вече изградена директна връзка между информационните системи на два административни органа от трети се счита за самостоятелно изграждане на директна връзка и за изграждането ѝ се спазват правилата по чл. 6.

Раздел II.

Изисквания за оперативна съвместимост по отношение на данните

Чл. 8. (1) Представянето на цифри, букви, препинателни знаци и други символи в информационните системи на административните органи трябва да се осъществява чрез стандартите, вписани в раздел "Интеграция на данните" на регистъра на стандартите.

(2) Представянето на илюстрации, фотографии и мултимедия трябва да се осъществява чрез стандартите, вписани в раздел "Потребителски интерфейси" на регистъра на стандартите.

(3) За компресиране на предаваните данни при осъществяване на електронна административна услуга трябва да се използват следните методи, съответстващи на стандарти, вписани в регистъра на стандартите:

1. за текстови файлове - методи за компресия без загуба;
2. за илюстрации, фотографии, мултимедия и други може да се използват и методи за компресия със загуба.

Чл. 9. (Доп. - ДВ, бр. 102 от 2010 г.) Администрациите използват в своята дейност само унифицирани описания на данни, регистрирани в съответните раздели на регистъра на регистрите и данните, в съответствие с чл. 8 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите при наличие на такива описания.

Чл. 10. При наличие само на неунифицирано описание на данни съответната администрация създава унифицирано описание на тези данни и започва да ги използва след тяхната регистрация в регистъра на регистрите и данните съгласно чл. 3, ал. 2 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Чл. 11. Контролът за използването на унифицирани описания на данни от администрациите се извършва при проверка на вътрешните им правила, създадени съгласно Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Чл. 12. (Изм. - ДВ, бр. 58 от 2010 г., в сила от 30.07.2010 г.) Министърът на транспорта, информационните технологии и съобщенията съгласува проектите на нормативни актове по отношение на спазване на изискването за използване само на унифицирани описания на данни, вписани в регистъра на регистрите и данните, след становище на съвета по вписванията.

Чл. 13. (1) В регистъра на информационните обекти могат да се вписват формализирани описания на данни само когато те са вписани в регистъра на регистрите и данните като унифицирани данни.

(2) Формализираните описания по ал. 1 трябва да имат същия състав, както съответните описания на данните, регистрирани в регистъра на регистрите и данните.

(3) (Изм. - ДВ, бр. 58 от 2010 г., в сила от 30.07.2010 г.) Създаването на формализирани описания се извършва съгласно критерии и правила за прилагането им за вписвания, утвърдени от министъра на транспорта, информационните технологии и съобщенията съгласно чл. 32 от Наредбата за регистрите на информационните обекти и регистъра на електронните услуги, приета с Постановление № 98 на Министерския съвет от 2008 г. (ДВ, бр. 48 от 2008 г.).

(4) (Изм. - ДВ, бр. 58 от 2010 г., в сила от 30.07.2010 г.) Контролът за спазване на изискванията по ал. 1 - 3 се извършва от министъра на транспорта, информационните технологии и съобщенията чрез Съвета по вписванията.

Раздел III.

Изисквания за оперативна съвместимост по отношение на електронните документи

Чл. 14. (1) (Доп. - ДВ, бр. 102 от 2010 г.) Формализираните електронни документи, обменяни между администрациите и издавани от тях към други лица и организации, трябва да бъдат с организация на данните в тях, съответстваща на вписаната в регистъра на информационните обекти при наличие на такива данни.

(2) (Доп. - ДВ, бр. 102 от 2010 г.) Електронните документи по ал. 1 трябва да съдържат валидни данни съгласно вписаните изисквания за това в регистъра на информационните обекти при наличие на такива документи.

Раздел IV.

Изисквания за оперативна съвместимост по отношение на приложения за визуализация и/или редактиране на електронни документи

Чл. 15. (1) Приложенията за визуализация на електронни документи, вписани в регистъра на информационните обекти, и приложенията за редактиране на електронни документи, вписани в регистъра на електронните услуги, трябва да отговарят на изискванията на този раздел.

(2) (Изм. - ДВ, бр. 48 от 2013 г.) Приложенията по ал. 1 трябва да бъдат удостоверени за съответствие с изискванията за оперативна съвместимост и информационна сигурност, когато те служат за визуализиране или редактиране на електронни документи, с които се обменят служебно данни между администрации посредством вътрешни електронни административни услуги или документите са резултат от предоставянето на електронни административни услуги.

Чл. 16. (1) (Изм. - ДВ, бр. 48 от 2013 г.) Приложенията, за които успешно е приключила процедура по удостоверяване, се вписват в списъка на удостоверените информационни системи.

(2) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Приложения, удостоверени по ал. 1, вписвани и в регистъра на информационните обекти, се предоставят от министъра на транспорта, информационните технологии и съобщенията за безплатно ползване чрез осигуряване на достъп за зареждане на инсталационен комплект от списъка на удостоверените информационни системи или посредством достъп до публично достъпно уеб базирано приложение.

(3) (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 17. Приложенията, осигуряващи само визуализация на електронни документи, трябва да визуализират съдържанието им, като:

1. съдържанието на всички данни се визуализира съгласно указанията, вписани при тяхната регистрация в регистъра на информационните обекти;
2. (отм. - ДВ, бр. 102 от 2010 г.)
3. (отм. - ДВ, бр. 102 от 2010 г.)
4. за всички данни е осигурена индикация за наименованието на грешка съгласно тяхната регистрация в регистъра на информационните обекти, ако проверката за тяхната валидност е

неуспешна;

5. за всяка установена грешка е осигурен достъп до текста на нейното определение, с който тя е вписана в регистъра на информационните обекти чрез подходящ интерфейс.

Чл. 18. Приложенията, осигуряващи редактиране на електронни документи, освен функциите по визуализация на съдържание на електронен документ по чл. 17 трябва да съдържат и функции за:

1. запис и четене на файлово съдържание на електронен документ във и от средата на файлова система, намираща се пряко под контрол на потребителя на приложението за редактиране, включително разположена върху преносим физически носител;

2. въвеждане, коригиране и изтриване на стойност за всички данни в електронен документ.

Чл. 19. (1) Приложенията трябва да осигуряват възможност за установяване на несъответствия в съдържанието на визуализиран или редактиран документ с регистрацията му в регистъра на информационните обекти.

(2) Приложенията трябва да сигнализират за установените несъответствия чрез визуализация на съответната грешка съгласно регистрацията на документа в регистъра на информационните обекти.

(3) (Отм. - ДВ, бр. 48 от 2013 г.)

(4) (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Раздел V.

Оперативна съвместимост по отношение на информационни системи

Чл. 20. (1) Административните информационни системи съгласно чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите трябва да отговарят на изискванията на този раздел.

(2) (Изм. - ДВ, бр. 48 от 2013 г.) Правилата на този раздел се отнасят и за специализираните информационни системи, осигуряващи изцяло или частично функциите на административна информационна система, когато създават и/или издават, и/или приемат, и/или регистрират, и/или съхраняват електронни документи, регламентирани в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Чл. 21. (1) При автоматично създаване на електронни документи от информационна система проверка за изпълнение на изискванията на чл. 14 се извършва по време на създаването.

(2) При неуспешна проверка по ал. 1 създаването се прекратява и за това се уведомява служителят, осъществяващ функции по обработка в неавтоматизиран режим или контролиращ автоматичното изпълнение на етап от услуга или процедура, при което се извършва създаването на документа.

(3) (Отм. - ДВ, бр. 48 от 2013 г.)

(4) (Отм. - ДВ, бр. 102 от 2010 г.)

Чл. 22. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 23. (Изм. - ДВ, бр. 102 от 2010 г.) При наличие на данни, вписани в регистъра на информационните обекти, които се поддържат от информационните системи, съдържанието на данните се визуализира съгласно указанията, вписани при тяхната регистрация в регистъра на информационните обекти.

Глава трета. ИНФОРМАЦИОННА СИГУРНОСТ

Раздел I. Политика за информационна сигурност

Чл. 24. Всички информационни системи на административните органи трябва да отговарят на изискванията и политиката за мрежова и информационна сигурност с оглед защитата им срещу неправомерен или случаен достъп, използване, правене достояние на трети лица, промяна или унищожаване, доколкото такива събития или действия могат да нарушат достъпността, автентичността, целостта и конфиденциалността на съхраняваните или предаваните данни, а също така на предоставяните електронни услуги, свързани с тези мрежи и системи.

Чл. 25. (1) За постигане на мрежова и информационна сигурност ръководителите на администрациите провеждат собствена политика, съобразена със спецификата на административните процеси в конкретната администрация, като предприемат съответни административни и технологични мерки.

(2) Политиките на отделните административни органи и предприеманите мерки трябва да отговарят на общите принципи съгласно приложение № 1.

Раздел II. Организация на мрежовата и информационната сигурност

Чл. 26. (1) Ръководителите на администрациите отговарят пряко за мрежовата и информационната сигурност в администрациите.

(2) Ръководителите на администрациите разработват и утвърждават вътрешни правила за мрежовата и информационната сигурност на техните информационни системи и за видовете информационен обмен, който се извършва между тях.

(3) Вътрешните правила по ал. 2 се изграждат по модела на "Системи за управление на информационната сигурност", регламентиран с изискванията на международния стандарт ISO 27001:2005 и в съответствие с изискванията на наредбата.

(4) Ръководителите на администрациите издават заповеди за разпределение на отговорностите на своите служители за гарантиране на мрежовата и информационната сигурност на използваните информационни системи.

Чл. 27. (1) Ръководителите на администрациите осигуряват сертификация на вътрешните правила като "Система за управление на информационната сигурност" по смисъла на ISO 27001:2005 от оправомощена за това организация.

(2) Ръководителите на администрациите организират комплексни проверки за оценяване степента на постигнатата мрежова и информационна сигурност в използваните от тях информационни системи в съответствие с клауза 7 от ISO 27001:2005.

(3) (Изм. - ДВ, бр. 102 от 2010 г.) Резултатите от сертификацията по ал. 1 и от проверките по ал. 2 се предоставят незабавно и на министъра на транспорта, информационните технологии и съобщенията за целите на текущия контрол в съответствие с чл. 60 от Закона за електронното управление.

(4) (Изм. - ДВ, бр. 102 от 2010 г.) Предоставянето на информацията по ал. 3 се осъществява като вътрешна електронна административна услуга, която министърът на транспорта, информационните технологии и съобщенията разработва и вписва в регистъра на електронните услуги.

Чл. 28. (1) Всеки ръководител на администрация определя служител или административно звено, отговарящо за мрежовата и информационната сигурност.

(2) Служителят или звеното по ал. 1 са пряко подчинени на ръководителя на администрацията.

(3) Функциите на служителите или на звеното по информационна сигурност са описани в приложение № 2.

(4) Когато администрация към административен орган има териториални структури и разпределени информационни системи, служител, отговарящ за информационната сигурност, се определя и във всяко териториално звено.

Чл. 29. Ръководителите на администрациите осигуряват необходимата инфраструктура за гарантиране на информационната сигурност на използваните от тях информационни системи съгласно вътрешните правила по чл. 26, ал. 2.

Чл. 30. (1) (Изм. - ДВ, бр. 102 от 2010 г.) Към министъра на транспорта, информационните технологии и съобщенията се създава Съвет за мрежова и информационна сигурност на информационните системи на административните органи като постояннодействащ консултативен орган за координиране на дейността за постигане на мрежова и информационна сигурност на използваните информационни системи.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Съветът за мрежова и информационна сигурност на информационните системи на административните органи работи въз основа на правилник, утвърден от министъра на транспорта, информационните технологии и съобщенията.

(3) Периодично, но не по-малко от веднъж в годината Съветът за мрежова и информационна сигурност на информационните системи на административните органи изготвя доклад за състоянието на информационната сигурност.

Чл. 31. (1) Ръководителите на администрациите задължително включват в утвърждаваните от тях вътрешни правила по чл. 26, ал. 2 раздел, осигуряващ оценка и управление на риска за мрежова и информационна сигурност.

(2) Препоръчителните действия по оценка и управление на риска трябва да съответстват на т. 4.2.1 от ISO 27001:2005 и на приложение № 3.

(3) Потенциалните рискови фактори за мрежовата и информационната сигурност, формулирани и класифицирани в международния стандарт ISO/IEC TR 13335:2000, са посочени в

приложение № 4.

Раздел III.

Управление на достъпа и защита срещу неправомерен достъп

Чл. 32. (1) Вътрешните правила за мрежова и информационна сигурност регламентират достъпа до информационните ресурси.

(2) Контролът по упражняване на регламентиран достъп се извършва по правила и процедури, посочени в приложение № 5.

Чл. 33. (1) Ръководителите на администрациите вземат мерки за предотвратяване на неправомерен достъп от трети лица до ресурсите на техните информационни системи.

(2) Рискът от неправомерен достъп по ал. 1 се анализира в годишните доклади на Съвета за мрежова и информационна сигурност.

(3) При наличие на неприемливо ниво на риска, регистриран по ал. 2, административният орган планира и провежда необходимите действия за неговото намаляване.

Чл. 34. Ръководителите на администрациите определят в утвърждаваните от тях вътрешни правила по чл. 26, ал. 2 нивото на защита от неправомерен достъп до всеки информационен актив съгласно следната класификация:

1. ниво "0" или "D" - ниво на свободен достъп;
2. ниво "1" или "C" - ниво на произволно управление на достъпа;
3. ниво "2" или "B" - ниво на принудително управление на достъпа;
4. ниво "3" или "A" - ниво на проверена сигурност.

Чл. 35. Ръководителите на администрациите са длъжни да предприемат необходимите действия за създаване и поддържане на инвентарни списъци на наличните информационни активи съгласно приложение № 6.

Раздел IV.

Управление на експлоатационните процеси

Чл. 36. (1) (Изм. - ДВ, бр. 102 от 2010 г.) Към министъра на транспорта, информационните технологии и съобщенията се създава Национален център за действие при инциденти по отношение на информационната сигурност като административно звено в специализираната администрация.

(2) Създаването на Националния център за действие при инциденти по отношение на информационната сигурност се извършва в съответствие с методическите указания (WP2006/5.1(CERT-D1/D2)) на Европейската агенция за мрежова и информационна сигурност (ENISA).

Чл. 37. Ръководителите на администрациите осигуряват мерките за сигурност при управление на експлоатационните процеси в информационните системи, посочени в приложение № 7, включително сигурността на електронните съобщения съгласно приложение № 8.

Чл. 38. (1) Служителят или звеното по информационна сигурност следи за неправомерно инсталиран софтуер на работните станции или сървъри и взема мерки за неговото отстраняване.

(2) Ръководителите на администрациите осигуряват необходимите технически и организационни средства за извършване на контрола по ал. 1, включително в случаите на териториална отдалеченост.

Чл. 39. (1) Съхранението и достъпът до данните в информационните системи се осъществяват чрез системи за управление на бази данни.

(2) Системите за управление на бази данни трябва да бъдат сертифицирани в съответствие с международния стандарт ISO/IEC 15408:2005, определящ т.нар. "Common Criteria for Information Technology Security Evaluation (CC)", или националните му приложения, като "IT-Grundschatz Methodology" на BSI (Германия), или с американския федерален профил "US Government Protection Profile for Database Management System in Basic Robustness Environments".

(3) При осигуряване на многопотребителски достъп до съдържанието на електронни документи информационните системи трябва да осигуряват функциите по заключване и отключване на документи за осигуряване на съвместна работа с документи.

(4) Минималното ниво на защита на достъпа до ресурсите на информационните системи в администрацията трябва да бъде "1" или "С".

Раздел V.

Защита срещу нежелан софтуер

Чл. 40. Защитата срещу нежелан софтуер в информационните системи на администрацията се организира от служителите или звената, отговарящи за мрежовата и информационната сигурност в съответната администрация.

Чл. 41. Мерките за защита срещу нежелан софтуер са посочени в приложение № 9.

Чл. 42. Националният център за действие при инциденти по отношение на информационната сигурност поддържа актуална информация за всички опити за проникване на нежелан софтуер в информационните системи на административните органи, както и за предприетите действия за защита от тях.

Раздел VI.

Мониторинг

Чл. 43. (1) Ръководителите на администрациите организират мониторинг на събитията и инцидентите, настъпили в използваните от тях информационни системи, като създават указания за извършването му в утвърждаваните от тях вътрешни правила.

(2) Мониторингът по ал. 1 се регламентира във вътрешните правила за мрежовата и информационната сигурност в съответствие с т. 4.2.3 от ISO 27001:2005 и приложение № 10.

Чл. 44. В годишните доклади за състоянието на информационната сигурност на информационните системи на администрациите, приемани от Съвета за мрежова и информационна сигурност на информационните системи на административните органи, задължително се включва информация за мониторинга на събитията и инцидентите и за неговата ефективност.

Раздел VII.

Физическа сигурност и защита на околната среда

Чл. 45. (1) Ръководителите на администрациите осигуряват мерки за физическата защита на техните информационни системи.

(2) Режимът за защита се урежда с вътрешните правила за мрежовата и информационната сигурност в съответствие с приложение № 11.

Чл. 46. (1) Ръководителите на администрациите предприемат превантивни действия за защита на информационните системи от природни бедствия.

(2) Ръководителите на администрациите застраховат риска от щети от природни бедствия на информационните системи в рамките на задължителните годишни застраховки.

Чл. 47. Ръководителите на администрациите осигуряват условия, при които неовластени лица не могат да получат физически достъп до работните станции и сървърите, използвани от администрацията.

Раздел VIII.

Управление на инциденти, свързани с информационната сигурност

Чл. 48. Ръководителите на администрациите утвърждават план за действие при инциденти, свързани с мрежовата и информационната сигурност на използваните от тях информационни системи, с цел осигуряване непрекъсваемост на дейността на съответната администрация. Планът трябва да съответства на изискванията на приложение № 12.

Чл. 49. Служителят или звеното по информационна сигурност в съответната администрация са длъжни да уведомяват незабавно Националния център за действие при инциденти по отношение на информационната сигурност за всеки инцидент в информационните системи на администрацията.

Чл. 50. (Изм. - ДВ, бр. 102 от 2010 г.) Съветът за мрежова и информационна сигурност на информационните системи на административните органи периодично обсъжда и предлага на министъра на транспорта, информационните технологии и съобщенията за утвърждаване препоръчителни управленски мерки за предотвратяване на инциденти в информационната сигурност.

Раздел IX.

Сигурност, свързана със служителите в администрацията

Чл. 51. Ръководителите на администрациите включват в утвърждаваните от тях вътрешни правила по чл. 26, ал. 2 раздел, регламентиращ мерки по сигурността, свързани със служителите в администрацията, в съответствие с приложение № 13.

Чл. 52. Ръководителите на администрациите определят профили за достъпа на различните групи служители до ресурсите в информационните системи в съответната администрация.

Глава четвърта. РЕГИСТЪР НА СТАНДАРТИТЕ

Раздел I. Общи положения за регистъра на стандартите

Чл. 53. Регистърът на стандартите е база от данни, управлявана от информационна система, съдържаща техническите стандарти и спецификации, които трябва да се прилагат от административните органи за предоставяне на електронни услуги, както и за осигуряване на оперативна съвместимост и информационна сигурност.

Чл. 54. (Изм. - ДВ, бр. 102 от 2010 г.) Регистърът на стандартите се води от министъра на транспорта, информационните технологии и съобщенията чрез овластени от него лица.

Чл. 55. (1) На вписване в регистъра на стандартите подлежат само предвидените в наредбата обстоятелства и техните елементи.

(2) Регистърът се осъвременява в съответствие с динамиката на международните стандартизационни процеси и възможностите за прилагането им в текущия момент.

(3) Новите версии на вписаните в регистъра стандарти не трябва да създават пречки за функциониране на вече реализираните решения, освен ако използваните в тези решения стандарти биха довели до нарушаване изискванията на информационна сигурност.

Чл. 56. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията създава организация за:

1. разпространение на знание относно прилагането на стандартите, осигуряващи оперативна съвместимост на информационните системи и информационна сигурност;

2. предложения пред Българския институт за стандартизация за приемане на международни или европейски стандарти като български държавни стандарти;

3. предложения пред Българския институт за стандартизация за разработване на нови български държавни стандарти.

Раздел II. Подлежащи на вписване обстоятелства

Чл. 57. Стандарти по смисъла на наредбата са:

1. формални хармонизирани технически стандарти в областта на информационните технологии, електронните комуникации и информационната сигурност, утвърждавани от междуправителствени стандартизационни органи, като ISO, ITU - на международно ниво, или CEN, CENELEC, ETSI - на европейско ниво;

2. международно приети неформални и хибридни технически стандарти и спецификации в областта на информационните технологии, комуникациите и информационната сигурност - резултат от стандартизационни процеси от секторни консорциуми, като OASIS, IETF, W3Consortium, UN/CEFACT, OMG.

Чл. 58. На вписване в регистъра на стандартите подлежат следните обстоятелства:

1. наименование на стандарт - вписва се пълното наименование на стандарта, установено от международната организация, създала и поддържаща стандарта, в превод на български език и в оригинал на английски език;

2. идентификатор на стандарт - вписва се кодов идентификатор на стандарта, установен от международната организация, създала и поддържаща стандарта;

3. пояснение за стандарта - вписва се кратко текстово пояснение за стандарта;

4. версия - вписва се последната международно приета версия на стандарта;

5. дата - вписва се датата на приемане на последната международно приета версия на стандарта;

6. организация - вписват се данни за организацията, създала и поддържаща стандарта;

7. текст - вписва се текст на стандарта, ако стандартът е публикуван със свободен достъп от създалата го и поддържаща организация;

8. URL на публикация - вписва се електронният адрес (URL) на интернет страницата, от която се осъществява достъп до указания за доставка на стандарта, ако той не е със свободен достъп;

9. степен на приложимост - вписва се характеристика, която може да има стойности: "задължителен", "препоръчителен", "под наблюдение", "бял списък", "сив списък" и "черен списък";

10. тематична принадлежност - вписва се характеристика, която може да има стойности: "комуникация и процедури за обмен", "уеб-услуги", "интеграция на данни", "управление на съдържанието и дефиниции на мета-данни", "потребителски интерфейси", "работни станции", "вътрешна организация на дейността и работни процеси", "управление на електронната идентичност" и "информационна сигурност";

11. обхват на приложимост - вписва се възможността за прилагане на целия стандарт или се изброяват само съответните части от него;

12. URL партида - вписва се автоматично генерираният електронен адрес (URL) на интернет страницата, от която се осъществява достъп до съдържанието на партидата на стандарта в регистъра.

Раздел III. Водене на регистъра

Чл. 59. (1) Производството по вписване започва със заявление, подадено от административен орган.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Производство по вписване може да започне и по инициатива на министъра на транспорта, информационните технологии и съобщенията по

предложение на Съвета по стандартите за оперативна съвместимост и информационна сигурност по чл. 73.

(3) (Изм. - ДВ, бр. 102 от 2010 г.) Лица извън посочените в ал. 1 и 2 могат да предложат на министъра на транспорта, информационните технологии и съобщенията да започне производство за вписване.

Чл. 60. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията предоставя следните електронни услуги, свързани с регистъра на стандартите:

1. вписване на стандарт;
2. вписване на промени в обстоятелствата за стандарт;
3. справка за вписванията в регистъра на стандартите за отделен стандарт или за стандарти по определени критерии.

Чл. 61. (1) (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията утвърждава задължителни образци в електронна форма за:

1. заявление за първоначално вписване на стандарт;
2. заявление за вписване на допълнителни обстоятелства към вече вписан стандарт;
3. заявление за справка за вписванията в регистъра на стандартите;
4. справка за вписванията в регистъра на стандартите за отделен стандарт или за стандарти по определени критерии.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Образците по ал. 1 се вписват в раздел "Документи" на регистъра на информационните обекти и се публикуват на интернет страницата на Министерството на транспорта, информационните технологии и съобщенията.

Чл. 62. (1) Процедурата за първоначално вписване на стандарт или за промени на вписаните обстоятелства включва:

1. приемане на заявлението за вписване;
2. проверка за допустимост и основателност на вписването;
3. проверка дали стандартът или новото обстоятелство е вече вписано;
4. извършване на вписването или издаване на мотивиран отказ за извършване на вписване;
5. уведомяване на заявителя за отказа да бъде извършено вписване.

(2) Проверките по т. 2 и 3 се извършват от Съвета по стандартите за оперативна съвместимост и информационна сигурност.

Чл. 63. (1) (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията извършва вписване след становище на Съвета по стандартите за оперативна съвместимост и информационна сигурност.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Преди да постанови отказ, министърът на транспорта, информационните технологии и съобщенията указва на заявителя на вписването да отстрани нередностите.

(3) Отказ се постановява, ако в срок 14 дни от уведомлението по ал. 2 нередностите не бъдат отстранени.

Чл. 64. При първоначално вписване на стандарт задължително се въвеждат всички обстоятелства, определени в чл. 58.

Чл. 65. (1) При първоначално вписване на стандарт за него се създава партия.

(2) За всяка създадена партия се генерира уникален регистров идентификатор, състоящ се от:

1. уникален регистров идентификатор на регистъра на стандартите - вписва се уникалният регистров идентификатор, създаден в регистъра на регистрите и данните при регистрацията на регистъра на стандартите в него;

2. партиден номер - вписва се поредният номер на партия в регистъра на стандартите.

(3) За всяка партия се поддържа описание, включващо:

1. (изм. - ДВ, бр. 102 от 2010 г.) заявител на вписването - вписват се данни за административния орган, заявил вписването, а в случаите по чл. 59, ал. 3 - Министерството на транспорта, информационните технологии и съобщенията;

2. уникален регистров идентификатор на заявлението за вписване - вписва се уникалният регистров идентификатор на заявлението, с което е заявено вписването;

3. време на вписване - вписват се автоматично генерирани данни за времето на извършеното вписване в регистъра;

4. служител, извършил вписване - вписват се автоматично данни, идентифициращи чрез информационната система, поддържаща регистъра, служителя, извършил вписването в регистъра.

Чл. 66. Към съдържанието на всяко вписано обстоятелство се поддържа описание, включващо:

1. номер на вписване - вписва се автоматично генериран пореден номер на вписването по обстоятелство в състава на партията;

2. уникален регистров идентификатор на обстоятелство - вписва се уникален регистров идентификатор на типа на обстоятелството/данните в раздел "Типове обстоятелства" или раздел "Унифицирани данни" на регистъра на регистрите и данните;

3. съдържание на обстоятелството - вписват се данните, формиращи съдържанието на обстоятелството, подлежащо на вписване;

4. уникален регистров идентификатор на заявление за вписване - вписва се уникалният регистров идентификатор на заявление, с което е заявено вписването;

5. (изм. - ДВ, бр. 102 от 2010 г.) заявител на вписването - вписва се наименование, единен идентификатор, адрес на електронната поща и телефон на административния орган, заявил вписването, а в случаите по чл. 59, ал. 3 - на Министерството на транспорта, информационните технологии и съобщенията;

6. време на вписване - вписват се автоматично генерирани данни за времето на извършеното вписване в регистъра;

7. служител, извършил вписването - вписват се автоматично данни, идентифициращи чрез информационната система, поддържаща регистъра, служителя, извършил вписването в регистъра.

Чл. 67. (1) Вписване на промяна в обстоятелствата за стандарт в регистъра се извършва чрез вписване на ново обстоятелство.

(2) След извършване на вписването по ал. 1 актуалното състояние на партидата на стандарта отразява последното вписване.

Раздел IV. Съхраняване и достъп до регистъра

Чл. 68. Регистърът на стандартите се съхранява безсрочно.

Чл. 69. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията съхранява регистъра на стандартите в съответствие с изискванията на наредбата като система с клас на информационна сигурност 3 или А.

Чл. 70. (Изм. - ДВ, бр. 102 от 2010 г.) Регистърът на стандартите е достъпен чрез интернет страницата на Министерството на транспорта, информационните технологии и съобщенията и по друг начин в зависимост от технологичната готовност на агенцията.

Чл. 71. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията осигурява възможност за преглед на актуалното състояние на партидите на стандартите към момента на проверката, както и на състоянието им към определена дата назад във времето.

Чл. 72. (1) (Изм. - ДВ, бр. 102 от 2010 г.) Всеки може да иска и извършва справка за вписванията в регистъра чрез интернет страницата на Министерството на транспорта, информационните технологии и съобщенията.

(2) Справки могат да се получават и чрез услугата по чл. 60, т. 3.

(3) Справките в регистъра са безплатни.

Раздел V.

Съвет по стандарти за оперативна съвместимост и информационна сигурност

Чл. 73. (Изм. - ДВ, бр. 102 от 2010 г.) Към министъра на транспорта, информационните технологии и съобщенията се създава Съвет по стандартите за оперативна съвместимост и информационна сигурност.

Чл. 74. (Изм. - ДВ, бр. 102 от 2010 г.) Съветът по стандартите за оперативна съвместимост и информационна сигурност е помощен консултативен орган и включва експерти, определени със заповед на министъра на транспорта, информационните технологии и съобщенията.

Чл. 75. Съветът по стандартите за оперативна съвместимост и информационна сигурност взема решения относно допустимостта и основателността за извършване на вписванията в регистъра на стандартите.

Чл. 76. (1) Съветът по стандартите за оперативна съвместимост и информационна сигурност може да провежда заседания, ако присъстват повече от половината от неговите членове.

(2) Решенията на съвета се вземат с обикновено мнозинство.

(3) (Изм. - ДВ, бр. 102 от 2010 г.) Правилата за работа на съвета се утвърждават от министъра на транспорта, информационните технологии и съобщенията.

Чл. 77. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията утвърждава Методика за оценка и подготовка на стандарти за вписване от Съвета по стандартите за оперативна съвместимост и информационна сигурност в съответствие с документа "Общ метод за оценка на стандартите" ("Common assessment method for standards and specifications" (CAMSS), разработван в рамките на Програма IDABC на Европейската комисия.

Глава пета.

АКРЕДИТАЦИЯ НА ПРОВЕРЯВАЩИ ЛИЦА (ОТМ. - ДВ, БР. 48 ОТ 2013 Г.)

Раздел I.

Общи положения (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 78. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 79. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 80. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 81. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 82. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 83. (Отм. - ДВ, бр. 48 от 2013 г.)

Раздел II.

Ред за акредитация на лицата, извършващи сертификация на информационни системи (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 84. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 85. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 86. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 87. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 88. (Отм. - ДВ, бр. 48 от 2013 г.)

**Раздел III.
Контрол (Отм. - ДВ, бр. 48 от 2013 г.)**

Чл. 89. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 90. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 91. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 92. (Отм. - ДВ, бр. 48 от 2013 г.)

**Раздел IV.
Спиране и отнемане на акредитация (Отм. - ДВ, бр. 48 от 2013 г.)**

Чл. 93. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 94. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 95. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 96. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 97. (Отм. - ДВ, бр. 48 от 2013 г.)

**Глава шеста.
ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ОПЕРАТИВНА
СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ (ЗАГЛ. ИЗМ. - ДВ, БР. 48 ОТ
2013 Г.)**

Раздел I.

Общи положения

Чл. 98. (Изм. - ДВ, бр. 48 от 2013 г.) (1) Администрациите са длъжни да използват само информационни системи, които съответстват на установените със Закона за електронното управление и подзаконовите актове по прилагането му изисквания за оперативна съвместимост и информационна сигурност и това съответствие е удостоверено от министъра на транспорта, информационните технологии и съобщенията по реда на наредбата.

(2) Министърът на транспорта, информационните технологии и съобщенията удостоверява съответствието на информационните системи с изискванията за оперативна съвместимост по чл. 125 и с изискванията за информационна сигурност по чл. 39.

(3) Министърът на транспорта, информационните технологии и съобщенията удостоверява съответствието на програмните приложения за визуализация и редактиране на електронни документи с изискванията за оперативна съвместимост и информационна сигурност по чл. 113 и 114 за всеки електронен документ по чл. 15, ал. 2.

Чл. 99. (Изм. - ДВ, бр. 48 от 2013 г.) По реда на наредбата не се извършва удостоверяване на съответствието на:

1. информационни системи, предназначени за обработка и съхранение на класифицирана информация;

2. информационни системи със специално предназначение (национална сигурност, отбрана и др.).

Чл. 100. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 101. (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Информационните системи и програмните приложения, удостоверени по реда на наредбата, се вписват в публичен списък на удостоверените информационни системи, поддържан от министъра на транспорта, информационните технологии и съобщенията.

Раздел II.

Обекти на оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност. Удостоверяване на съответствието (Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 102. (Изм. - ДВ, бр. 48 от 2013 г.) (1) На оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност подлежат технически спецификации по чл. 28, ал. 1, т. 4 от Закона за обществените поръчки за:

1. разработване или придобиване на административна информационна система по смисъла на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите;

2. разработване или придобиване на специализирани информационни системи по чл. 20, ал. 2.

(2) Министърът на транспорта, информационните технологии и съобщенията удостоверява съответствието с изискванията за оперативна съвместимост и информационна сигурност на техническите спецификации по ал. 1 въз основа на подадена от заинтересуван

административен орган справка-декларация за извършени проверки по сценарий, описан в приложение № 14.

Чл. 103. (1) (Изм. - ДВ, бр. 48 от 2013 г.) На оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност подлежи информационна система, която:

1. има функционалност съгласно изискванията на чл. 20;

2. (изм. - ДВ, бр. 48 от 2013 г.) е нова версия на информационна система, която е вече удостоверена съгласно т. 1.

(2) (Изм. - ДВ, бр. 48 от 2013 г.) Министърът на транспорта, информационните технологии и съобщенията удостоверява съответствието с изискванията за оперативна съвместимост и информационна сигурност на информационните системи по ал. 1 въз основа на подадена от заинтересувано лице, доставящо или разработващо информационната система, справка-декларация за извършени проверки по сценарии, описани в приложение № 15.

(3) (Нова - ДВ, бр. 48 от 2013 г.) Проверките по ал. 2 се извършват от заинтересуваните лица като част от тестовете за приемане на информационната система и/или приложение.

Чл. 104. (1) (Изм. - ДВ, бр. 48 от 2013 г.) На оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност подлежат програмни приложения, които изпълняват функции по визуализация и/или редактиране на електронни документи по чл. 15, ал. 2.

(2) (Изм. - ДВ, бр. 48 от 2013 г.) Министърът на транспорта, информационните технологии и съобщенията удостоверява съответствието с изискванията за оперативна съвместимост и информационна сигурност на приложенията по ал. 1 въз основа на подадена от заинтересувано лице, доставящо или разработващо програмното приложение, справка-декларация за извършени проверки по сценарии, описани в приложение № 16.

(3) (Нова - ДВ, бр. 48 от 2013 г.) Проверките по ал. 2 се извършват от заинтересуваните лица като част от тестовете за приемане на информационната система и/или приложение.

(4) (Нова - ДВ, бр. 48 от 2013 г.) Към справка-декларацията по ал. 2 за приложения, които подлежат на вписване в регистъра на информационните обекти, заинтересуваното лице предоставя инсталационен комплект на провереното приложение или хипервръзка към публично достъпно уеб базирано приложение.

Чл. 104а. (Нов - ДВ, бр. 48 от 2013 г.) (1) Когато към момента на извършване тестовете на информационната система и/или приложение по чл. 103, ал. 3 и чл. 104, ал. 3 електронните документи, които се редактират и/или визуализират с приложението по чл. 104, не са вписани в регистъра на информационните обекти, проверката се извършва спрямо заявените за вписване обстоятелства за тези информационни обекти.

(2) В случаите по ал. 1, когато вписаните обстоятелства за електронния документ и съответстващия му сегмент в регистъра на информационните обекти се различават от заявените за вписване, заинтересуваното лице се задължава в периода за гаранционна поддръжка да обнови съответните приложения, да извърши повторна проверка и да подаде нова справка-декларация.

Чл. 104б. (Нов - ДВ, бр. 48 от 2013 г.) (1) Министърът на транспорта, информационните технологии и съобщенията чрез оправомощени от него длъжностни лица може да извърши основна проверка на съответствието на спецификацията, системата или приложението, за което е

подадена справка-декларация по чл. 102, ал. 2, чл. 103, ал. 2 или чл. 104, ал. 2, за което уведомява заинтересувания административен орган, съответно заинтересуваните лица по чл. 103, ал. 2 или чл. 104, ал. 2, в 10-дневен срок от получаване на искането за удостоверяване и вписване.

(2) Длъжностните лица по ал. 1 извършват проверката по ал. 1 в присъствието на заинтересувания административен орган, съответно заинтересуваното лице, доставящо или разработващо информационната система и/или програмното приложение.

(3) Длъжностните лица по ал. 1 проверяват съответствието на предоставения инсталационен пакет или уеб базираното приложение по чл. 104, ал. 4 с провереното приложение.

(4) Удостоверяването на съответствието с изискванията за оперативна съвместимост се извършва, ако не са констатирани несъответствия при проверките по ал. 2 и 3.

Чл. 104в. (Нов - ДВ, бр. 48 от 2013 г.) (1) При констатиране на несъответствия от длъжностните лица при извършване на проверките по чл. 102, ал. 2 заинтересуваният административен орган преработва техническата спецификация и извършва проверките отново до пълно отстраняване на всички несъответствия.

(2) При констатиране на несъответствия от длъжностните лица при извършване на проверките по чл. 103, ал. 2 и чл. 104, ал. 2 заинтересуваното лице извършва промени в информационната система и/или приложение и извършва проверките отново до пълно отстраняване на всички несъответствия.

(3) В случаите по чл. 104, ал. 4 при констатиране на несъответствия в проверките по чл. 104, ал. 2 заинтересуваното лице е длъжно да предостави инсталационен комплект, съответстващ на провереното приложение, или хипервръзка към публично достъпно уеб базирано приложение, съответстващо на провереното приложение.

(4) Заинтересуваният административен орган, съответно заинтересуваните лица, подават справки-декларации за извършените от тях проверки по ал. 1 – 3. Длъжностните лица извършват проверки по чл. 102, ал. 2, чл. 103, ал. 2, чл. 104, ал. 2 и чл. 104б, ал. 3 на подадените справки-декларации.

Чл. 105. (Отм. - ДВ, бр. 48 от 2013 г.)

Раздел III.

Проверка за оперативна съвместимост и информационна сигурност на технически спецификации (Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 106. (Изм. - ДВ, бр. 48 от 2013 г.) (1) Техническата спецификация по чл. 28, ал. 1, т. 4 от Закона за обществените поръчки за разработване на информационна система трябва да съдържа изрично и ясно указание дали тя попада в обхвата на чл. 20.

(2) Заинтересуваният административен орган извършва проверки по чл. 102, ал. 2 на техническата спецификация по ал. 1. При установяване на несъответствия при извършване на проверките заинтересуваният административен орган преработва техническата спецификация и извършва проверките отново до пълно отстраняване на всички несъответствия.

Чл. 107. (Изм. - ДВ, бр. 48 от 2013 г.) Технически спецификации, за които не са установени несъответствия по чл. 106, ал. 2, се вписват в списъка на удостоверените

информационни системи по искане на заинтересувания административен орган със заповед на министъра на транспорта, информационните технологии и съобщенията.

Раздел IV.

Подготовка на документи, съдържащи тестови данни, за провеждане на процедури по проверки за оперативна съвместимост (Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 108. (1) (Доп. - ДВ, бр. 48 от 2013 г.) За всеки вид електронен документ по чл. 15, ал. 2, регистриран в регистъра на информационните обекти, заинтересуваното лице представя набор от документи от същия вид, съдържащи тестови данни за провеждане на тестове за съответствие с регистрацията в регистъра на информационните обекти.

(2) В набора от документи по ал. 1 само един документ не трябва да съдържа отклонения от регистрацията на съответния вид документ.

(3) Тестовите се създават по начин, позволяващ заложените в тях грешни стойности и нарушенията в организацията на данните да представят всички възможни отклонения от регистрацията на съответния вид документ в регистъра на информационните обекти.

(4) (Отм. - ДВ, бр. 48 от 2013 г.)

(5) (Изм. - ДВ, бр. 48 от 2013 г.) Отговорността за пълнотата на набора от документи, съдържащи тестови данни по ал. 1, е на заинтересуваното лице.

Чл. 109. (1) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Заедно със справка-декларацията по чл. 103, ал. 2 и чл. 104, ал. 2 заинтересуваното лице изпраща на министъра на транспорта, информационните технологии и съобщенията пълните набори от документи по чл. 108, ал. 1.

(2) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Министърът на транспорта, информационните технологии и съобщенията вписва наборите по ал. 1 в списъка на удостоверените информационни системи.

(3) Проверките по отношение на регистриран в регистъра на информационните обекти документ, за който има вписани набори от документи по чл. 108, ал. 1 и 4, се извършват по тези набори.

Чл. 110. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 111. (1) (Изм. - ДВ, бр. 48 от 2013 г.) Промени във вписани набори от документи по чл. 108, ал. 1 се извършват по реда на чл. 109 при:

1. установяване на грешки в документите с тестове;

2. установяване на функционална непълнота в тестовите в набор от документи.

(2) (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Раздел V.

Проверки за оперативна съвместимост и информационна сигурност на приложения за визуализация или редактиране на електронни документи (Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 112. (1) (Изм. и доп. - ДВ, бр. 48 от 2013 г.) Заинтересувано лице извършва проверка за оперативна съвместимост и информационна сигурност на приложение за визуализация или

редактиране на електронни документи по чл. 15, ал. 2.

(2) (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 113. (Изм. - ДВ, бр. 48 от 2013 г.) Заинтересуваното лице извършва следните проверки за установяване на техническата функционалност на приложението за:

1. четене и визуализиране на съдържание на електронен документ от файл, записан в информационната система, намираща се под контрол на потребителя, или записан върху външен носител;

2. (отм. - ДВ, бр. 48 от 2013 г.)

3. наличие на функционалност за вярна и точна визуализация на всички грешки - резултат от извършване на тестове с набора от документи, съдържащи тестови данни по чл. 108, ал. 1, при изпълнение на проверката по т. 2;

4. наличие на функционалност за вярна и точна визуализация на съобщенията, съдържащи наименованията и описанията на всички грешки, предизвикани при извършване на тестове с набора от документи;

5. (изм. - ДВ, бр. 102 от 2010 г.) наличие на функционалност за вярна и точна визуализация на съдържанието на всички данни съгласно регистрацията на визуализирания електронен документ в регистъра на информационните обекти.

Чл. 114. (Изм. - ДВ, бр. 48 от 2013 г.) При проверка за оперативна съвместимост и информационна сигурност на приложение за редактиране на електронни документи освен проверките по чл. 113 се извършват и проверки за установяване наличието на функционалност за:

1. запис на електронен документ като файл в информационната система, намираща се под контрол на потребителя, включително върху външен носител;

2. създаване, изтриване и корекция на съдържанието на всички данни съгласно регистрацията на електронния документ в регистъра на информационните обекти.

Чл. 115. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 116. (Изм. - ДВ, бр. 48 от 2013 г.) Проверките на приложение за визуализация или редактиране, което работи с няколко документа, се извършват за всеки от тях.

Чл. 117. (Изм. - ДВ, бр. 48 от 2013 г.) Заинтересуваното лице извършва проверки по чл. 104, ал. 2 на приложението по чл. 112, ал. 1. При установяване на несъответствия при извършването на проверките заинтересуваното лице прави промени в приложението и извършва проверките отново до пълно отстраняване на всички несъответствия.

Чл. 118. (Изм. - ДВ, бр. 48 от 2013 г.) При разширяване обхвата на електронните документи, които могат да се визуализират или редактират с удостовереното приложение, се извършват проверки и се подава справка-декларация по чл. 104, ал. 2 само за новите документи.

Раздел VI.

Сертификация на приложения за проверка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 119. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 120. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 121. (Отм. - ДВ, бр. 48 от 2013 г.)

Раздел VII.

Проверки за оперативна съвместимост и информационна сигурност на информационни системи (Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 122. (1) (Изм. - ДВ, бр. 48 от 2013 г.) Заинтересувано лице извършва проверки за оперативна съвместимост и информационна сигурност на информационна система.

(2) (Отм. - ДВ, бр. 48 от 2013 г.)

(3) (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 123. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията изгражда, поддържа и предоставя специална среда-полигон за извършване на проверки за съответствие на информационните системи с изискванията за оперативна съвместимост и информационна сигурност.

Чл. 124. (1) (Доп. - ДВ, бр. 48 от 2013 г.) Заинтересуваното лице само извършва инсталирането на информационната система в средата-полигон по чл. 123 в случаите по чл. 104а.

(2) (Доп. - ДВ, бр. 48 от 2013 г.) Заинтересуваното лице осигурява технически сътрудник, който под ръководството на акредитираното лице извършва въвеждане на данни и активиране на съответните функции в информационната система в случаите по чл. 104а.

Чл. 125. За всеки документ, създаден от административната информационна система, посочен в приложение № 1 към Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, се проверява:

1. възможността за въвеждане в ръчен или автоматичен режим на стойностите на данните в състава на проверяван документ;

2. възможността за генериране в ръчен или автоматичен режим на валиден документ от проверявания тип, съдържащ данните, въведени по т. 1.

Чл. 126. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 127. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 128. (Изм. - ДВ, бр. 48 от 2013 г.) Заинтересуваното лице извършва проверка за изпълнение на изискванията за информационна сигурност по чл. 39.

Раздел VIII.

Промени в издаден сертификат (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 129. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 130. (Отм. - ДВ, бр. 48 от 2013 г.)

Раздел IX.

Задължение за уведомяване. Събиране на информация

Чл. 131. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 132. (1) Акредитираните лица са длъжни да съхраняват всички документи и протоколи от извършените оценки в срок 10 години.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Акредитираните лица представят документите по ал. 1 на министъра на транспорта, информационните технологии и съобщенията при извършване на проверки.

Чл. 133. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 133а. (Нов - ДВ, бр. 48 от 2013 г.) (1) Заинтересуваните административни органи, извършили проверки за оперативна съвместимост и информационна сигурност на технически спецификации по чл. 102, ал. 2, изпращат справка-декларация за извършените проверки, при които няма установени несъответствия, незабавно след приключване на проверката.

(2) Към справка-декларацията се прилагат проверените технически спецификации и протокол от извършените проверки съгласно приложение № 14.

(3) Заинтересуваните лица по чл. 103, ал. 2 или чл. 104, ал. 2, извършили проверка за оперативна съвместимост и информационна сигурност на информационна система или приложение, изпращат заявление за вписване, придружено от справка-декларация за проверки по чл. 103, ал. 2 и чл. 104, ал. 2, при които няма установени несъответствия, незабавно след подписване на протокола от извършените проверки от административния орган – възложител, за вписване в списъка на удостоверените информационни системи. Към справка-декларацията се прилага протокол от извършените проверки съгласно приложение № 15 и/или приложение № 16.

(4) Административните органи по чл. 102, ал. 2 и заинтересуваните лица по чл. 103, ал. 2 и чл. 104, ал. 2 са длъжни да съхраняват всички документи и протоколи от извършените оценки в срок 10 години.

(5) Административните органи по чл. 102, ал. 2 и заинтересуваните лица по чл. 103, ал. 2 и чл. 104, ал. 2 представят документите по ал. 4 на министъра на транспорта, информационните технологии и съобщенията при извършване на проверки.

(6) Министърът на транспорта, информационните технологии и съобщенията вписва удостоверената техническа спецификация, информационна система или приложение със заповед за вписване в списъка на удостоверените информационни системи в срок 10 дни от получаване на справка-декларацията по ал. 1 или 3, а в случаите по чл. 104б – в 10-дневен срок от установяването на съответствие с изискванията за оперативна съвместимост и информационна сигурност от оправомощените длъжностни лица.

(7) Документацията за участие в обществената поръчка, част от която е техническата спецификация, подлежи на одобряване по реда на чл. 25 от Закона за обществените поръчки след вписването на удостоверената техническа спецификация в списъка на удостоверените информационни системи.

Глава седма.

СПИСЪК НА УДОСТОВЕРЕНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ (ЗАГЛ. ИЗМ. - ДВ, БР. 48 ОТ 2013 Г.)

Чл. 134. (Изм. - ДВ, бр. 48 от 2013 г.) (1) В списъка на удостоверените информационни системи се вписват обстоятелства относно удостоверените технически спецификации, информационни системи и приложения.

(2) Списъкът по ал. 1 се води от министъра на транспорта, информационните технологии и съобщенията чрез определени от него длъжностни лица.

Чл. 135. (1) (Изм. - ДВ, бр. 48 от 2013 г.) Списъкът е база от данни, управлявана от информационна система, съдържаща описанията на състава и организацията на данните по чл. 134, ал. 1.

(2) В списъците се поддържа история на вписванията.

Чл. 136. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 137. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 138. (1) (Изм. - ДВ, бр. 48 от 2013 г.) В списъка на удостоверените информационни системи се вписват следните видове обекти:

1. (изм. - ДВ, бр. 48 от 2013 г.) обекти от вид "удостоверена система";
2. (изм. - ДВ, бр. 48 от 2013 г.) обекти от вид "удостоверено приложение";
3. (изм. - ДВ, бр. 48 от 2013 г.) обекти от вид "удостоверена техническа спецификация";
4. обекти от вид "тестов набор от документи".

(2) Списъкът по ал. 1 се състои от следните раздели, обособени по видове обекти, в които се вписват обстоятелствата относно тези обекти:

1. (изм. - ДВ, бр. 48 от 2013 г.) раздел "Удостоверени системи";
2. (изм. - ДВ, бр. 48 от 2013 г.) раздел "Удостоверени приложения";
3. (изм. - ДВ, бр. 48 от 2013 г.) раздел "Удостоверени технически спецификации";
4. раздел "Тестови набори от документи".

Чл. 139. (Изм. - ДВ, бр. 48 от 2013 г.) В раздел "Удостоверени информационни системи" от списъка на удостоверените информационни системи се вписват следните обстоятелства за обекти от вид "удостоверена информационна система":

1. данни, идентифициращи удостоверената система, като модел, версия, конфигурация и др.;
2. данни, идентифициращи заинтересуваното лице;
3. данни за административния орган – възложител на информационната система;
4. обхват на проверка;
5. дата на удостоверяване.

Чл. 140. (Изм. - ДВ, бр. 48 от 2013 г.) В раздел "Удостоверени приложения" от списъка на удостоверените информационни системи се вписват следните обстоятелства за обекти от вид "удостоверено приложение":

1. данни, идентифициращи удостовереното приложение, като модел, версия, конфигурация и др.;
2. тип на удостовереното приложение – приложение за визуализация и редактиране или приложение за визуализация;
3. данни, идентифициращи заинтересуваното лице;
4. данни за административния орган – възложител на приложението;
5. обхват на проверка, включваща видовете електронни документи, които поддържа приложението, и дали приложението е проверено по реда на чл. 98, ал. 5;
6. дата на удостоверяване;
7. хипервръзка за достъп до инсталационния пакет на приложението, когато удостовереното приложение е вписано като обстоятелство в регистъра на информационните обекти или в регистъра на електронните услуги.

Чл. 141. (Изм. - ДВ, бр. 48 от 2013 г.) В раздел "Удостоверени технически спецификации" от списъка на удостоверените информационни системи се вписват следните обстоятелства за обекти от вид "проверена техническа спецификация":

1. данни, идентифициращи удостоверената техническа спецификация;
2. данни, идентифициращи административния орган, възложител по Закона за обществените поръчки;
3. дата на удостоверяване.

Чл. 142. (Изм. - ДВ, бр. 48 от 2013 г.) В раздел "Тестови набори от документи" от списъка на удостоверените информационни системи се вписват следните обстоятелства за обекти от вид "тестов набор от документи":

1. вид на електронните документи, които се проверяват с тестовия набор;
2. съдържание на тестови документи;
3. данни за заинтересуваното лице, изпратило набора за вписване;
4. дата на удостоверяване.

Чл. 143. (1) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Министърът на транспорта, информационните технологии и съобщенията предоставя следните електронни услуги, свързани със списъка на удостоверените информационни системи:

1. (отм. - ДВ, бр. 48 от 2013 г.)
 2. (отм. - ДВ, бр. 48 от 2013 г.)
 3. (отм. - ДВ, бр. 48 от 2013 г.)
 4. (изм. - ДВ, бр. 48 от 2013 г.) вписване на удостоверена техническа спецификация, информационна система или приложение;
 5. (изм. - ДВ, бр. 48 от 2013 г.) вписване на промени в обстоятелствата за удостоверена техническа спецификация, информационна система или приложение;
 6. (изм. - ДВ, бр. 48 от 2013 г.) справка за вписванията в списъка на удостоверените информационни системи.
- (2) (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 144. (1) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Министърът на транспорта, информационните технологии и съобщенията утвърждава задължителни образци в електронна форма за справки-декларациите, с които се заявяват услугите по чл. 143, т. 4 и 5 и за заявленията за предоставяне на услуги по чл. 143, т. 6.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Образците по ал. 1 се вписват в раздел "Документи" от регистъра на информационните обекти и се публикуват на интернет страницата на Министерството на транспорта, информационните технологии и съобщенията.

Чл. 145. (Отм. - ДВ, бр. 48 от 2013 г.)

Чл. 146. (1) (Изм. - ДВ, бр. 48 от 2013 г.) Процедурата за първоначално вписване на удостоверена техническа спецификация, информационна система или приложение или на промени на вписаните обстоятелства включва:

1. приемане на заявлението за вписване;
2. (изм. - ДВ, бр. 48 от 2013 г.) проверка за редовност и допустимост на искането;
3. проверка дали обектът или новото обстоятелство вече са вписани;
- 3а. (нова - ДВ, бр. 48 от 2013 г.) проверка от оправомощени длъжностни лица в случаите по чл. 104б и 104в;
4. извършване на вписването или издаване на мотивиран отказ за вписване;
5. уведомяване на заявителя за постановения отказ.

(2) (Изм. - ДВ, бр. 102 от 2010 г.) Преди да постанови отказ, министърът на транспорта, информационните технологии и съобщенията указва на заявителя на вписването да отстрани нередностите.

(3) (Доп. - ДВ, бр. 48 от 2013 г.) Отказ се постановява, ако в срок 14 дни от уведомлението по ал. 2 нередностите не бъдат отстранени, а в случаите по чл. 104б, ако несъответствията не бъдат отстранени в срок 3 месеца от подаването на справка-декларацията по чл. 102, ал. 2, чл. 103, ал. 2 или чл. 104, ал. 2.

Чл. 147. (Изм. - ДВ, бр. 48 от 2013 г.) Вписването в списъка се извършва чрез въвеждане на данни за вписаните обстоятелства в базата от данни на списъка.

Чл. 148. (1) При първоначално вписване за всеки обект се създава партида.

(2) За всяка създадена партида се генерира уникален регистров идентификатор, състоящ

се от:

1. (изм. - ДВ, бр. 48 от 2013 г.) уникален регистров идентификатор на раздел на списъците - вписват се уникалният регистров идентификатор, създаден в регистъра на регистрите, и данните при регистрацията на списъка на удостоверените информационни системи в него;

2. партиден номер - вписва се поредният номер на партията.

(3) За всяка партия се поддържа описание, включващо:

1. време на вписване - вписват се автоматично генерирани данни за времето на извършеното вписване в списъка;

2. служител, извършил вписване - вписват се автоматично данни, идентифициращи чрез информационната система, поддържаща списъците, служителя, извършил вписването в съответния списък.

Чл. 149. Към съдържанието на всяко вписано обстоятелство се поддържа описание, включващо:

1. номер на вписване - вписва се автоматично генериран пореден номер на вписване по обстоятелство в състава на партията;

2. уникален регистров идентификатор на обстоятелство - вписва се уникален регистров идентификатор на типа на обстоятелството/данните в раздел "Типове обстоятелства" или раздел "Унифицирани данни" от регистъра на регистрите и данните;

3. съдържание на обстоятелството - вписват се данните, формиращи съдържанието на обстоятелството, подлежащо на вписване;

4. време на вписване - вписват се автоматично генерирани данни за времето на извършеното вписване в съответния списък;

5. уникален регистров идентификатор на заявление за вписване - вписва се уникалният регистров идентификатор на заявление, с което е заявено вписването;

6. заявител на вписването - вписва се наименование, код по БУЛСТАТ, адрес на електронната поща и телефон на централа на административния орган, заявил вписването;

7. служител, извършил вписването - вписват се автоматично данни, идентифициращи чрез информационната система, поддържаща списъците, служителя, извършил вписването.

Чл. 150. (1) Промяна в обстоятелствата се извършва чрез вписване на новото обстоятелство.

(2) След извършване на вписването по ал. 1 актуалното състояние на партията на съответния обект отразява последното вписване.

Чл. 151. (Изм. - ДВ, бр. 48 от 2013 г.) Списъкът на удостоверените информационни системи се съхранява безсрочно.

Чл. 152. (Изм. - ДВ, бр. 102 от 2010 г.) Министърът на транспорта, информационните технологии и съобщенията съхранява списъците в съответствие с изискванията на наредбата като система с клас на информационна сигурност 3 или А.

Чл. 153. (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Списъкът на

удостоверените информационни системи е достъпен чрез интернет страницата на Министерството на транспорта, информационните технологии и съобщенията и по друг начин в зависимост от технологичната готовност на министерството.

Чл. 154. (Изм. - ДВ, бр. 102 от 2010 г., отм. - ДВ, бр. 48 от 2013 г.)

Чл. 155. (1) (Изм. - ДВ, бр. 102 от 2010 г., изм. - ДВ, бр. 48 от 2013 г.) Всеки може да иска и да извършва справка за вписванията в списъка чрез интернет страницата на Министерството на транспорта, информационните технологии и съобщенията.

(2) Справки могат да се правят и чрез формализирана заявка.

(3) (Изм. - ДВ, бр. 48 от 2013 г.) Справките в списъка са безплатни.

Допълнителни разпоредби

§ 1. По смисъла на наредбата:

1. "Административна информационна система" е информационна система по смисъла на чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

2. "Електронни услуги" е общото понятие за електронни административни услуги и вътрешни електронни административни услуги.

3. "Мрежова и информационна сигурност" е способност на мрежите и информационните системи да се противопоставят на определено ниво на въздействие или на случайни събития, които могат да нарушат достъпността, автентичността, интегритета и конфиденциалността на съхраняваните или предаваните данни и на услугите, свързани с тези мрежи и системи.

4. "Информационни активи" са материалните и нематериалните активи и информационни обекти, свързани с информационна система, които имат полезна стойност за определена администрация.

5. "Инцидент по сигурността на информацията" е единично или поредица от неочаквани събития по сигурността на информацията, които увреждат или съществува сериозна вероятност да увредят операции или да застрашат информационната сигурност.

6. "Нежелан софтуер" е компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите информационните системи лица и е предназначена за привеждане на информационните системи или компютърни мрежи в нежелани от ползващите ги състояния или в осъществяване на нежелани резултати, както и компютърна програма, която е предназначена за нарушаване дейността на информационна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на данни без разрешение, когато такова се изисква.

7. "Политика за информационна сигурност" е съвкупност от документирани решения, взети от ръководител на администрация, насочени към защитата на информацията и асоциираните с нея ресурси.

8. "Уебуслуга" е автономна, завършена и изпълнима функционалност на информационна система с унифициран и автоматизиран вход и изход, притежаваща следните свойства:

а) независимост от съпътстващите я приложения, които я пораждат, и от тези, които тя поражда;

б) слабо свързана функционалност, основана на системна техническа, платформена и

софтуерна независимост между информационната система на доставчика на услугата и на получателя ѝ;

в) функционални и операционни спецификации за качеството при предоставяне на услугата, като максимално време за предоставяне на услугата, процедури за обработване на грешки и др.;

г) функционалност, основана на определен набор международно приети стандарти;

д) лесна откриваемост и използваемост без особени действия от страна на нейния доставчик.

9. "Отворена мрежа" е мрежа, свободна от ограничения за вида на оборудването, което може да бъде присъединено, както и за начините на комуникация, които не ограничават съдържанието, сайтовете или платформите.

10. "Профил на достъп" е описание на информационните активи на системата, които могат да бъдат ползвани от група потребители с аналогични права на достъп.

§ 2. Нивата на защита на информационната система от нерегламентиран достъп, регламентирани в чл. 34 от наредбата, се характеризират със следните основни мерки:

1. Ниво "0" или "D" обхваща открита и общодостъпна информация (например публикувана на интернет страниците на администрациите). То предполага анонимно ползване на информацията и липса на средства за конфиденциалност.

2. Ниво "1" или "C" изисква:

а) достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;

б) ползвателите да се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп. За установяване на идентичността трябва да се използва защитен механизъм от типа идентификатор/парола. Няма изисквания за доказателство за идентичността при регистрация;

в) идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;

г) доверителната изчислителна система, т.е. функционалността на информационната система, която управлява достъпа до ресурсите ѝ, трябва да поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи ходът на работата;

д) информационната система трябва да разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;

е) защитните механизми трябва да са преминали тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.

3. Ниво "2" или "B" изисква в допълнение към изискванията към предишното ниво:

а) като механизъм за проверка на идентичността да се използва удостоверение за електронен подпис, независимо дали е издадено за вътрешноведомствени нужди в рамките на вътрешна инфраструктура на публичния ключ, или е издадено от външен доставчик на удостоверителни услуги;

б) при издаване на удостоверението издаващият орган проверява съществените данни за личността на ползвателя, без да е необходимо личното му присъствие;

в) доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;

г) доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.

4. Ниво "3" или "A" изисква в допълнение към изискванията към предишното ниво:

- а) като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;
- б) при издаване на удостоверението да е гарантирана физическата идентичност на лицето;
- в) доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;
- г) комуникацията между потребителя и системата да се осъществява единствено чрез протокол Transport Layer Security (TLS) или Secure Sockets Layer (SSL), като минималната дължина на симетричния ключ трябва да е 128 бита;
- д) доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

Преходни и Заключителни разпоредби

§ 3. Председателят на ДАИТС осигурява първоначалното въвеждане на данни в регистъра на стандартите в срок 3 месеца от обнародването на наредбата в "Държавен вестник".

§ 4. (1) В срок 12 месеца от влизането в сила на наредбата ръководителите на администрациите организират разработването на вътрешни правила съгласно чл. 26 и извършват сертификацията им като Система за управление на информационната сигурност по ISO 27001:2005.

(2) В срок 24 месеца от влизането в сила на наредбата ръководителите на отделните администрации организират провеждането на одит от оторизирана независима организация за признаване на съответствие между разработените вътрешноведомствени правила "Системи за управление на информационната сигурност" и международния стандарт ISO 27001:2005.

§ 5. (Отм. - ДВ, бр. 48 от 2013 г.)

§ 6. В срок 12 месеца от влизането в сила на наредбата председателят на ДАИТС създава Съвет за мрежова и информационна сигурност на информационните системи на административните органи като консултативен орган, подпомагащ неговата дейност.

§ 7. В срок 12 месеца от влизането в сила на наредбата председателят на ДАИТС провежда консултации с представители на Асоциацията на българските застрахователи относно възможността за предоставяне на застрахователен продукт "Застраховка на риска по отношение на мрежовата и информационната сигурност".

§ 8. Председателят на ДАИТС създава Национален център за действие при инциденти по отношение на информационната сигурност не по-късно от 6 месеца от влизането в сила на наредбата.

§ 9. Наредбата се приема на основание чл. 43, ал. 2 от Закона за електронното управление.

§ 10. Наредбата влиза в сила от деня на обнародването ѝ в "Държавен вестник" с изключение на чл. 7, който влиза в сила след въвеждането в действие на Единната среда за обмен на електронни документи (ЕСОЕД).

ПОСТАНОВЛЕНИЕ № 147 ОТ 23 ЮЛИ 2010 Г. ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НОРМАТИВНИ АКТОВЕ НА МИНИСТЕРСКИЯ СЪВЕТ

(ОБН. - ДВ, БР. 58 ОТ 2010 Г., В СИЛА ОТ 30.07.2010 Г.)

§ 16. Навсякъде в Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, приета с Постановление № 279 на Министерския съвет от 2008 г. (ДВ, бр. 101 от 2008 г.), думите "министъра на държавната администрация и административната реформа" и "Министърът на държавната администрация и административната реформа" се заменят съответно с "министъра на транспорта, информационните технологии и съобщенията" и "Министърът на транспорта, информационните технологии и съобщенията".

.....

Заключителни разпоредби

КЪМ ПОСТАНОВЛЕНИЕ № 147 ОТ 23 ЮЛИ 2010 Г. ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НОРМАТИВНИ АКТОВЕ НА МИНИСТЕРСКИЯ СЪВЕТ

(ОБН. - ДВ, БР. 58 ОТ 2010 Г., В СИЛА ОТ 30.07.2010 Г.)

§ 29. Постановлението влиза в сила от деня на обнародването му в "Държавен вестник".

ПОСТАНОВЛЕНИЕ № 311 ОТ 20 ДЕКЕМВРИ 2010 Г. ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НОРМАТИВНИ АКТОВЕ НА МИНИСТЕРСКИЯ СЪВЕТ

(ОБН. - ДВ, БР. 102 ОТ 2010 Г.)

§ 1. В Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, приета с Постановление № 279 на Министерския съвет от 2008 г. (обн., ДВ, бр. 101 от 2008 г.; изм., бр. 58 от 2010 г.), се правят следните изменения и допълнения:

.....

10. Навсякъде в наредбата думите "председателят на ДАИТС", "председателя на ДАИТС" и "ДАИТС" се заменят съответно с "министърът на транспорта, информационните технологии и съобщенията", "министъра на транспорта, информационните технологии и съобщенията" и "Министерството на транспорта, информационните технологии и съобщенията".

Преходни и Заключителни разпоредби

КЪМ ПОСТАНОВЛЕНИЕ № 115 ОТ 18 МАЙ 2013 Г. ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НАРЕДБАТА ЗА ОБЩИТЕ ИЗИСКВАНИЯ ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ, ПРИЕТА С ПОСТАНОВЛЕНИЕ № 279 НА МИНИСТЕРСКИЯ СЪВЕТ ОТ 2008 Г.

(ОБН. - ДВ, БР. 48 ОТ 2013 Г.)

§ 69. Техническите спецификации, информационните системи и приложения, сертифицирани до влизането в сила на постановлението, се считат за удостоверени за съответствие технически спецификации, информационни системи и приложения и се вписват служебно в списъка на удостоверените информационни системи.

Приложение № 1 към чл. 25, ал. 2

Общи стратегии за информационна сигурност

1. Политиката за информационна сигурност е набор от нормативни документи, правила и норми за поведение, които определят как организацията защитава обработката, съхранението и разпространението на информацията.

2. Политиката за сигурност на информационни системи на административните органи трябва да бъде съобразена с групата международни стандарти ISO 270XX, обединяваща мнозинството от съществуващи стандарти за управление на информационната сигурност - основно със стандарта ISO 27001:2005, предоставящ модел на система за управление на информационната сигурност за адекватен и пропорционален контрол на сигурността за защита на информационните активи и създаване на доверие в заинтересуваните страни.

3. Решенията относно политиките за мрежова и информационна сигурност трябва да се изграждат за осигуряване няколко нива на сигурност по отношение на:

- а) мрежа;
- б) система;
- в) приложения;
- г) информация.

4. За всяко от нивата по т. 3 трябва да се осигури съответният контрол с цел да се обезпечи сигурността на общото програмно приложение за защита. За осигуряване на адекватно ниво на сигурност трябва да се прилага практиката, наречена "дълбока отбрана", обезпечаваша многослойна защита, за ограничаване проникването на всякакви атаки и осигуряване на невъзможност за компрометиране на общото програмно приложение за защита.

5. При създаването на политика за сигурност трябва да се използват следните принципи:

а) "Минимална привилегия" - концепция, при която се ограничава достъпът само до ресурси, които са необходими за изпълняване на одобрените функции. Определен ползвател или процес трябва да има само такива права, които са необходими за изпълняване на конкретната задача.

б) "Дълбока отбрана" - концепция, при която се поверява защитата на повече от един компонент или механизъм, осигуряващ сигурността по такъв начин, че невъзможността на един компонент или механизъм да ограничи атаката да не доведе до компрометиране на общата защита.

в) "Точка на запусване" - концепция, при която се принуждават лица, извършващи интервенции, да използват тесен канал за достъп, който позволява действията да бъдат наблюдавани и контролирани. Обикновено се прилага на входа и изхода на т.нар. "Демилитаризирани зони" ("DMZ").

г) "Най-слабо звено" - концепция, при която се наблюдават и елиминират звената с най-слаба устойчивост на интервенции или с наличие на възможност за проникване.

д) "Позиция на безопасно спиране" - концепция, при която системите трябва да преустановяват работа безопасно и да се предотврати възможността при неочакваното

преустановяване на работа на една система да се осигури достъп на лицата, извършващи интервенции до системата.

е) "Универсално участие" - концепция, при която всички звена на системата следят за сигурността при наличие на разпределение на функциите за това, което ограничава възможността на лицата, извършващи интервенции, да се възползват от липсата на защитна активност от конкретно звено.

ж) "Разнообразие на защитата" - концепция, при която не се разчита само на една система или приложение за сигурност, независимо от това, колко надеждни или изчерпателни са те.

з) "Простота" - концепция, при която се осигурява поддържането на опростена обща среда, за която се осигурява по-лесно защита срещу интервенции.

и) "Фрагментиране" - концепция, при която се осигурява свеждане до минимум на възможните вредни последици върху една информационна система чрез фрагментиране на максимален брой отделни единици; по този начин се ограничава възможността за достъп до цялата система в случай на проникване в изолирана единица.

к) "Защита срещу вътрешни и външни заплахи" - концепция, при която се въвеждат правила за потребителите за недопускане действия на служителите, които да осигуряват възможност за интервенции; такива правила могат да бъдат правила за управление на съдържанието, допълнителни нива за идентификация, регистрация за достъп до критични информационни активи и др.

Приложение № 2 към чл. 28, ал. 3

Функции на служителя (звено) по информационна сигурност

1. Ръководи дейностите, свързани с постигане на мрежова и информационна сигурност на администрацията, в която работи, в съответствие с нормативната уредба и политиките и целите за мрежова и информационна сигурност на организацията във взаимодействие със звената за информационно осигуряване и за вътрешен одит.

2. Следи за прилагането на стандартите, политиките и правилата за информационна сигурност и управление на риска в администрацията.

3. Консултира ръководството на администрацията във връзка с информационната сигурност.

4. Ръководи периодичните оценки на рисковете за информационната сигурност и спазването на приетите политики и процедури.

5. Периодично (не по-малко от два пъти годишно) изготвя доклади за състоянието на информационната сигурност в административното звено и ги представя на ръководителя.

6. Координира обучението на ръководителите и служителите в административното звено във връзка с информационната сигурност.

7. Участва в организирането, тренировките и анализа на резултатите от тренировките за действия при настъпване на инциденти.

8. Отговаря за защитата на интелектуалната собственост и материалните активи на административното звено в областта на информационните и комуникационните технологии.

9. Участва в изготвянето на политиките, целите, процедурите и метриката за оценка на информационната сигурност.

10. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.

11. Разследва и анализира инцидентите в областта на мрежовата и информационната

сигурност в административното звено, реакциите при инциденти и предлага действия за подобряване на мрежовата и информационната сигурност.

12. Предлага санкции за служителите от администрацията при нарушаване на правилата за сигурност.

13. Разработва и предлага за утвърждаване от ръководителя на съответната администрация инструкциите, произтичащи от наредбата, както и всички други необходими указания и процедури.

14. Следи за изпълнението на утвърдените от ръководителя на администрацията инструкции и процедури, свързани с информационната сигурност.

15. Актуализира списъка от заплахи и потенциални рискове за съответната администрация.

16. Координира оценяването на финансовите и други загуби при настъпване на идентифицирана заплаха.

17. Изготвя доклади и анализи за настъпили инциденти, засягащи мрежовата и информационната сигурност, и предлага действия за компенсиране на последствията и предотвратяване на други подобни инциденти.

18. Следи новостите за заплахи за сигурността, отчитайки наличния в съответната администрация софтуер и хардуер, и организира своевременното инсталиране на коригиращ софтуер (patches).

19. При възникване на какъвто и да е инцидент, свързан с информационната сигурност, го документираща и информира незабавно ръководителя на съответната администрация и Националния център за действие при инциденти по отношение на информационната сигурност в информационните системи на административните органи.

20. Разработва и предлага иновативни решения и архитектури за подобряване на информационната сигурност на съответната администрация.

21. Следи за появата на нови вируси и зловреден код, спам, атаки и взема адекватни мерки.

22. Организира тестове за проникване, разкрива слабите места в мрежата на съответното административно звено и предлага мерки за подобряване на мрежовата и информационната сигурност.

Приложение № 3 към чл. 31, ал. 2

Действия по оценка и управление на риска

1. Всички административни органи са длъжни да оценяват рисковете за сигурността съгласно международния стандарт ISO/IEC TR 13335-3:1998 и ISO/IEC TR 13335-4:2000 (в процес на преработване в ISO/IEC 27005).

2. По смисъла на това приложение рискът за сигурността е фактическо състояние, което създава заплахи за уязвяване на един или няколко информационни актива, което да предизвика тяхното повреждане или унищожаване.

3. Оценката на риска се определя чрез изчисление на вероятността за уязвяване въз основа на ефективността на съществуващите или планираните мерки за сигурност.

4. Заплахите за мрежовата и информационната сигурност се класифицират по следните критерии:

а) по елементите на информационната сигурност (достъпност, цялостност, конфиденциалност), към които са насочени;

б) по компонентите на информационната система (апаратура, софтуер, данни,

поддържаща инфраструктура), към които са насочени;

в) по начина на осъществяване (случайни/преднамерени действия, от природен/технологичен характер и др.);

г) по разположението на източника (вътре във/извън информационната система).

5. Действията по управление на риска трябва да обхващат оценка на неговия размер, изработване на ефективни и икономични мерки за неговото снижаване и оценка дали резултативният риск е в приемливи граници. Управлението на риска следва да се извършва чрез последователно прилагане на два типа циклично повтарящи се действия:

а) оценка (преоценка) на риска;

б) избор на ефективни и икономични средства за неговата неутрализация.

6. При идентифициране на риск трябва да се предприеме едно от следните действия:

а) ликвидиране на риска (например чрез отстраняване на причиняващите го обстоятелства);

б) намаляване на риска (например чрез използване на допълнителни защитни средства);

в) приемане на риска и разработване на план за действия в обстановка на риск;

г) преадресиране на риска (например чрез сключване на съответната застраховка).

7. Процесът на управление на риска трябва да включва следните етапи:

а) избор на анализируемите обекти и нивото на детайлизация на анализа;

б) избор на методология за оценка на риска;

в) идентификация на информационните активи;

г) анализ на заплахите и последствията от тях, откриване на уязвимите места в защитата;

д) оценка на рисковете;

е) избор на защитни мерки;

ж) реализация и проверка на избраните мерки;

з) оценка на остатъчния риск.

8. Процесът на управление на риска трябва да бъде циклически процес. Последният етап се явява начало на нов цикъл на оценка. Новият цикъл се провежда:

а) ако остатъчният риск не удовлетворява ръководството на администрацията;

б) след изтичане на определен срок, определен във вътрешните правила за мрежовата и информационната сигурност на администрацията.

Приложение № 4 към чл. 31, ал. 3

Заплахи срещу мрежовата и информационната сигурност, формулирани в международния стандарт ISO/IEC TR 13335:2000

Видовете заплахи, които могат да застрашат конфиденциалността, интегритета и достъпността, са следните:

1. Подслушване, изразяващо се в достъп до служебна информация чрез прихващане на електронни съобщения независимо от използваната технология.

2. Електромагнитно излъчване, изразяващо се в действия на трето лице, целящо да получи знание за обменяни данни посредством информационна система.

3. Нежелан код, който може да доведе до загуба на конфиденциалността чрез записването и разкриването на пароли и до нарушаване на интегритета при интервенции от трети лица, осъществили нерегламентиран достъп с помощта на такъв код. Нежелан код може да се използва, за да се заобиколи проверка за достоверност, както и всички защитни функции, свързани с нея. В резултат кодът може да доведе до загуба на достъпността, когато данните или файловете са разрушени от лицето, получило нерегламентиран достъп с помощта на нежелан

код.

4. Маскиране на потребителската идентичност може да доведе до заобикаляне на проверката за достоверност и всички услуги и защитни функции, свързани с нея.

5. Погрешно насочване или пренасочване на съобщенията може да доведе до загуба на конфиденциалност, ако се осъществи нерегламентиран достъп от трети лица. Погрешното насочване или пренасочване на съобщенията може да доведе и до нарушаване на интегритета, ако погрешно насочените съобщения са променени и след това насочени към първоначалния адресат. Погрешното насочване на съобщения води до загуба на достъпността до тези съобщения.

6. Софтуерни грешки могат да застрашат конфиденциалността, ако софтуерът е създаден с контрол на достъпа или за криптиране или ако грешка в софтуера осигури възможност за нежелан достъп в информационна система.

7. Кражбата на информационни активи може да доведе до разкриване на информация, която представлява служебна или друга защитена от закона тайна. Кражбата може да застраши достъпността до данните или информационното оборудване.

8. Нерегламентиран достъп до компютри, информационни ресурси, услуги и приложения може да доведе до разкриване на поверителни данни и до нарушаване интегритета на тези данни, ако нерегламентираната им промяна е възможна. Нерегламентираният достъп до компютри, данни, услуги и приложения може да наруши достъпността до данните, ако тяхното изтриване или заличаване е възможно.

9. Нерегламентиран достъп до носител на данни може да застраши съхраняваните върху него данни.

10. Повреждане на носител на информация може да наруши интегритета и достъпността до данните, които се съхраняват на този носител.

11. Грешка при поддръжката. Неизвършването на редовна поддръжка на информационните системи или допускане на грешки по време на процеса по поддръжка може да доведе до нарушаване на достъпността до данни.

12. Аварии в електрозахранване и климатични инсталации могат да доведат до нарушаване на интегритета и достъпността до данни, ако вследствие на настъпването на аварията са увредени информационни системи или носители на данни.

13. Технически аварии (например аварии в мрежите) могат да нарушат интегритета и достъпността до информация, която се съхранява или разпространява чрез тази мрежа.

14. Грешки при предаването на информацията могат да доведат до нарушаване на нейната цялост и достъпност.

15. Употреба на нерегламентирани програми и информация могат да нарушат интегритета и достъпността до данните, съхранявани и разпространявани чрез информационната система, в която е настъпило такова събитие, и програмите и информацията се използват, за да се изменят съществуващи програми и данни по неразрешен начин или ако те съдържат нежелан код.

16. Потребителски грешки могат да нарушат интегритета и достъпността до данни чрез неумишлено или умишлено действие.

17. Липса на потвърждаване може да застраши интегритета на данните. Предпазните мерки за предотвратяване на непотвърждаването трябва да се прилагат в случаите, когато е важно да се получи доказателство за това, че дадено съобщение е изпратено и е/не е получено, както и за това, че мрежата е пренесла съобщението.

18. Интервенции срещу интегритета на данните могат да доведат до тяхното сериозно увреждане и до невъзможност от по-нататъшното им използване.

19. Аварии в комуникационното оборудване и услуги могат да увредят достъпността на данните, предавана чрез тези услуги.

20. Външни въздействия с огън, вода, химикали и др. могат да доведат до увреждане или

унищожаване на информационното оборудване.

21. Злоупотреба с ресурси може да доведе до недостъпност до данни или услуги.

22. Природни бедствия могат да доведат до унищожаване на данни и информационни системи.

23. Претоварване на комуникационния трафик може да доведе до нарушаване на достъпността до обменяни данни.

Приложение № 5 към чл. 32, ал. 2

Средства за управление на достъпа на участниците в електронния обмен

1. Защитата на системните ресурси на информационни системи на административните органи е процес, при който използването на системните ресурси се регулира в съответствие с политиката в областта на мрежовата и информационна сигурност и е позволено само за упълномощени лица чрез използването от тях информационни системи. Това включва предотвратяването на нерегламентиран достъп до ресурсите, включително предотвратяване на достъп до ресурсите по нерегламентиран начин.

2. Управлението на защитата от нерегламентиран достъп се категоризира на няколко степени в зависимост от оценките на потенциалните последствия за администрацията при нарушаване на конфиденциалността, интегритета и/или достъпността, както следва:

а) ограничено, когато организацията продължава да изпълнява функциите си, но с понижена ефективност, на информационните активи са причинени незначителни вреди и финансовите загуби са незначителни;

б) умерено, когато ефективността на основните функции на администрацията е съществено понижена, на информационните активи са причинени значителни вреди и финансовите загуби са значителни;

в) високо, когато загубата на конфиденциалност, интегритет и/или достъпност оказва тежко или непоправимо въздействие на администрацията, при която тя загубва способност да изпълнява основните си функции, на информационните активи са причинени тежки вреди и финансовите загуби са много големи.

3. Средствата за управление на достъпа позволяват да се определят и контролират действията, които различни ползватели на информационните системи и процеси в тях могат да извършват по отношение на информационни ресурси. Логическото управление на достъпа трябва да позволява да се определят множество допустими операции за всеки ползвател или процес и да се контролира изпълнението на установените правила.

4. Средствата за управление на достъпа на участниците в електронния обмен трябва да включват три категории функции:

а) административни функции - създаване и съпровождане на атрибути за управление на достъпа;

б) спомагателни функции - обслужване на процесите на достъп на ползвателите;

в) информационни функции - събиране на информация за процесите на достъп с оглед подобряване на взаимодействието.

5. Всяко самостоятелно звено на администрацията управлява идентификаторите на ползвателите на информационните системи чрез:

а) уникална идентификация на всеки ползвател;

б) верификация на идентификатора на всеки ползвател;

в) регламентиране на административните процедури за разпространение, заместване на загубени, компрометирани или повредени идентификатори;

г) прекратяване действието на идентификатора след определен период на липса на активност;

д) архивиране на идентификаторите.

6. Информационните системи на административните органи трябва да скриват ехо изображението на идентифициращата информация в процеса на проверка на идентичността с цел да я защитят от възможно използване от страна на неоправомощени лица.

7. При проверка на идентичността чрез криптографски модули информационната система трябва да прилага методи, отговарящи на стандартите, вписани в раздел "Информационна сигурност" от регистъра на стандартите.

8. За изграждане на вътрешни правила за мрежовата и информационната сигурност в администрациите се препоръчва следното съдържание на раздела, свързан с управлението на достъпа на участниците в електронния обмен:

а) документирана политика по управление на достъпа, включваща цели, обхват, задължения, координация на организационните структури;

б) документираните процедури по присвояване на привилегии, акаунти и други права в съответствие с политиката;

в) определяне на ограничения на количеството несполучливи опити на ползвателя за вход в система за определен интервал от време, след което акаунтът му се заключва;

г) определяне на предупреждаващите съобщения, информиращи потребителя преди предоставяне на достъп, относно:

- общите ограничения, налагани от системата;

- възможния мониторинг, протоколиране и одит на използването на системата;

- необходимото съгласие на ползвателя за мониторинг и протоколиране в случай на използване на системата;

- забраните и възможните санкции при несанкционирано използване на системата;

- възможните действия на ползвателя, които могат да бъдат изпълнени от информационната система без необходимост от аутентикация и оторизация.

9. В съответствие с процедурите по т. 3 ръководителите на администрациите организират провеждането на следните мероприятия:

а) организиране предоставянето на услуги на всички граждани и организации с еднакъв приоритет;

б) записване в поддържаните от системата списъци на участниците на всички граждани и организации, които са участвали в електронния информационен обмен в информационните системи на административните органи;

в) съхраняване на архивна информация за период една година за всички участници, които са използвали електронни административни услуги от публичните информационни системи;

г) организиране достъпа на служителите от администрацията чрез система от индивидуални пароли; паролите трябва да се променят периодично, но най-малко веднъж на 6 месеца;

д) извършване на преглед и актуализиране на правата за достъп на служителите, които поддържат работата на информационни системи в администрациите.

10. Всеки служител в администрацията, записан в съответния директориен LDAP сървър (централен или локален), трябва да получава уникални потребителско име и парола за достъп само до информационните системи, които са необходими, за да изпълнява служебните си задължения. Паролата трябва да съдържа между 8 и 16 буквено-цифрови символа и да изисква автоматична промяна всеки месец.

Приложение № 6 към чл. 35

Класификация, контрол и управление на информационните активи

1. Картите на наличните информационни ресурси в съответната администрация трябва да определят еднозначно:

а) конкретен служител за кои информационни ресурси (компютри, устройства, софтуерни продукти/системи, бази данни и др.) отговаря;

б) конкретен софтуерен продукт/информационна система и/или коя база от данни на кои компютри и устройства се използват.

2. Инвентарните списъци за наличните информационни ресурси в съответната администрация трябва да включват:

а) за хардуерни устройства (без бързо амортизируемите, като мишки, клавиатури и други подобни) минималният набор от данни, които трябва да се поддържат, включва:

- сериен номер;

- фабричен номер;

- модел;

- описание на основните технически параметри (процесор/честота, размер на паметта и вид/тип, модел на диска и размер, захранване - мощност и модел/тип, списък на аксесоарите към устройството и др.);

- дата на придобиване;

- дата на пускане в експлоатация;

- дата на извеждане от употреба;

- дата на продажба/бракуване/даряване;

- местоположение на устройството;

- име на служителя, отговарящ за функциониране на устройството;

- име/имена на служителя/служителите, ползващ/ползващи устройството;

- дати на обслужване и ремонт на устройството;

- описание на извършеното обслужване/ремонт;

- с кои устройства е свързано това устройство;

- работата на кои устройства зависи от правилното функциониране на това устройство;

- правилното функциониране на това устройство от работата на кои устройства зависи;

- кои работни процеси обслужва това устройство;

б) за софтуерни продукти минималният набор от данни, които трябва да се поддържат, включва:

- име на продукта;

- версия на продукта;

- списък на минималните изисквания към хардуера за нормална работа на продукта;

- дата на придобиване;

- дата на инсталиране и настройка;

- дата, от която започва да тече лицензът за ползване на продукта;

- машина/машини, на която/които е инсталиран продуктът;

- дата на извеждане от употреба;

- дата на изтичане на лиценза за ползване на продукта;

- дата, на която са извършени промени в настройки или в самия продукт;

- описание на извършените промени;

- име на служителя, инсталирал продукта;

- име на служителя, извършил настройките;

- име на служителя, извършил промените;

- име на файла, в който се пази състоянието преди промените;
- кои работни процеси обслужва този софтуерен продукт;
- работата на кои софтуерни продукти зависи от правилното функциониране на този софтуерен продукт;
- правилното функциониране на този софтуерен продукт от работата на кои софтуерни продукти зависи.

3. Върху работните станции и сървърите в администрациите да се инсталират само софтуерни продукти, за които съответната администрация разполага с лиценз за ползване.

4. Всички информационни системи, които се въвеждат в експлоатация в администрациите, трябва да се съпровождат с подробна документация за:

- а) всички функции на клиента, приложението и базите данни;
- б) административните средства за достъп и настройка;
- в) схеми на базите данни с подробно описание на таблиците и връзките;
- г) контролите при въвеждане и обмен на данни;
- д) контролите при обработката и резултатите от обработката;
- е) приложението с всички модули, "use cases", UML схеми и интерфейси.

5. Инсталирането и настройката на нови софтуерни и хардуерни продукти да се планира и всички лица, използващи засегнатите ресурси, да се уведомяват не по малко от 3 дни преди извършване на инсталацията или настройката.

6. Преди извършване на инсталация да се направят резервни копия на софтуера, файловете и базите данни, като се разработи и "roll back" план.

7. Инсталирането, настройката и поддръжката на нови софтуерни и хардуерни продукти да се извършват в периоди с минимално натоварване на съответните ресурси.

8. Преди инсталиране в оперативно действащите системи на нови софтуерни и хардуерни продукти те да се тестват в тестова среда максимално близка до реалните работни условия.

9. Служителите в администрациите носят материална отговорност за мобилните устройства, които са им предоставени за ползване. Мобилните устройства се получават от служителите, които ги използват, срещу подпис върху документ, съдържащ пълното описание на мобилното устройство и инсталирания софтуер.

10. Услугите по активен анализ на защитеността на системата (активни скенери на защитеността) позволяват да се открият и отстранят недостатъци в системата за защита на информационните активи, преди от тях да са се възползвали злонамерени лица.

Приложение № 7 към чл. 37

Управление на експлоатационните процеси

1. Като основно средство за управление на експлоатационните процеси в информационните системи на администрациите за осигуряване на информационна сигурност се препоръчва създаване на зони на сигурност в информационната система, произтичащи от международния стандарт ISO/IEC 15408-2 "Common Criteria".

2. Зоните на сигурност са области от софтуерната архитектура на системата, в които е определен специфичен комплекс от мерки, осигуряващи конкретно ниво на сигурност. Зоните са адекватно разделени една от друга, като преносите на данни от една зона в друга са строго регламентирани и се осъществяват през контролни обекти, като защитни стени, прокси-сървъри и др.

3. При изграждане на сигурността следва да се поддържа "демилитаризирана зона (DMZ)" - мрежова област, разположена между публичната неконтролируема част на мрежата

(обичайно свързана с интернет) и вътрешната защитена част на системата. Демилитаризираната зона трябва да организира информационни услуги към двете части на мрежата, като защитава вътрешната част от нерегламентиран достъп.

4. Мерките за сигурност при управление на експлоатационните процеси в информационни системи на администрациите трябва да включват:

а) при проектиране на информационни системи да се отдава предпочитание на системи с многослойна архитектура, в които клиентът, приложението и данните са логически и физически разделени;

б) да се изготви и утвърди Инstrukция за резервиране и архивиране на данни и файлове;

в) да се осигури редовно изготвяне на резервни копия на базите данни и файловете във файловете сървъри; графиците за резервиране се определят в зависимост от характера на дейността на всяка администрация; препоръчително е ежедневно резервиране;

г) да се осигури съхраняване на резервните копия в специално отделно помещение/място/огнеупорна каса;

д) да се осигури редовно обновяване на носителите, върху които се записват резервни копия (на период около 2/3 от срока им на годност);

е) да се осигури редовно изготвяне на архивни копия на базите данни и файловете във файловете сървъри; графиците за резервиране се определят в зависимост от характера на дейността на всяка администрация; препоръчително е ежемесечно резервиране;

ж) да се осигури редовно обновяване на носителите, върху които се записват архивни копия (на период около 2/3 от срока им на годност);

з) архивните копия да се съхраняват в друга сграда в огнеупорна каса;

и) достъпът до резервни и архивни копия се извършва под контрола на служителя по информационна сигурност.

Приложение № 8 към чл. 37

Управление на електронните съобщения

1. Управлението на електронните съобщения в администрациите се извършва съгласно Препоръка X.700 на Международния съюз по телекомуникации (ITU - International Telecommunication Union) и се осъществява чрез:

а) мониторинг на компонентите;

б) контрол (т.е. изработване и реализация на управляващи въздействия);

в) координация на работата на компонентите на системата.

2. Системите за управление трябва:

а) да дават възможност на администраторите да планират, организират, контролират и отчитат използването на процесите, свързани с осигуряване на мрежова и информационна сигурност;

б) да позволяват нагаждане на системата към изменения на изискванията за сигурност;

в) да осигуряват предсказуемо поведение на системата при различни обстоятелства.

3. Управлението на мрежовата сигурност се основава на препоръки X.800 и X.805 на Международния съюз по телекомуникации (ITU - International Telecommunication Union).

4. Съгласно препоръките по т. 3 за реализация на функциите на мрежовата сигурност трябва да се използват следните механизми и комбинации от тях:

а) криптиране;

б) цифрови сертификати;

в) механизми за управление на достъпа;

г) механизми за контрол на интегритета на данните, в т.ч. интегритета на потока съобщения;

д) механизми за идентификация;

е) механизми за допълване на трафика;

ж) механизми за управление на маршрутизацията;

з) механизми за отбелязвания и записи на комуникационните характеристики.

5. Защитата на електронните съобщения в интернет включва:

а) защитна стена;

б) защита от вируси и нежелан код;

в) защита от спам;

г) проверка на прикачените файлове за вируси и нежелан код;

д) защита от DoS (denial of service) атаки;

е) защита от HA (harvesting attacks);

ж) защита на e-mail адресите от търсещи работи;

з) защита от изтичане на информация;

и) защита от шпионски софтуер (spyware);

к) защита на IM (instant messaging);

л) защита на гласовите комуникации (Skype, ICQ, др.);

м) проверка за съответствие с наложените политики в съответната администрация;

н) проверка за съответствие с приетите нормативни документи;

о) контрол върху обмена (изпращане/получаване) на големи файлове в съответствие с приетите политики;

п) приоритизация на входящата и изходящата поща в зависимост от профила на всеки служител;

р) пренасочване на пощата в зависимост от приетите политики;

с) автоматично криптиране на изходящата поща при необходимост в съответствие с приетите политики;

т) автоматично добавяне на текст към входящи/изходящи съобщения в съответствие с приетите политики.

6. Получени съобщения, автоматично категоризирани като спам или съдържащи нежелан код, да се записват в специализирани папки и да са достъпни за контрол и обработка от упълномощени лица (служителя по информационна сигурност, специалисти от Националния център за действие при инциденти по отношение на информационната сигурност в информационните системи на административните органи и др.).

7. За защитата на "рутинг-инфраструктурата" и "рутинг-протоколите" трябва да се използват Препоръките на Работните групи RPSEC (Routing Protocol Security Requirements) и SIDR (Secure Inter-Domain Routing) на международната организация IETF (Internet Engineering Task Force).

8. За управление на имената и домейните в инфраструктурата в интернет да се използва "система за управление на имената на домейните (DNS)" с модификация на DNS протокола с разширения за идентификация (DNSSEC), която се основава на спецификацията на IETF RFC 4033.

9. За осъществяване на защитен обмен на съобщения по протоколите HTTP, LDAP, FTP и други да се използва Протокол SSL ("Secure Socket Layer") версия 3.0, формулиран от IETF ("Internet Engineering Task Force") или VPN ("Virtual Private Networking") решения за сигурно криптиране на сесиите.

10. За криптиране на XML базирани съобщения на ниво "сесия" да се използва Протокол XMLENC, формулиран от консорциума W3C.

11. За електронно подписване на XML базирани документи да се използва Протокол

XAdES (XML Advanced Electronic Signature), формулиран в Препоръка TS 101 903 на ETSI (European Telecommunications Standards Institute) и основан на Препоръка XML DSIG на Работна група "XML-Signature Working Group" на консорциума W3C.

12. За работа с публичните ключове при електронно подписване на XML базирани документи да се използва Протокол XKMS ("XML Key Manipulation Service"), основан на Препоръка XKMS 2.0 на консорциума W3C.

13. Копие от цялата служебна електронна поща на служителя се съхранява на пощенския сървър на съответната администрация не по-малко от две години, след като служителят напусне работа.

14. Служителите в администрациите могат да използват за получаване и изпращане на служебна кореспонденция единствено служебната си електронна поща.

15. Електронни съобщения, изпратени от служители в държавната администрация, съдържат задължително идентифицираща информация за контакт със съответния служител:

- а) име;
- б) телефон;
- в) електронна поща;
- г) длъжност;
- д) учреждение.

16. В края на всяко изходящо електронно съобщение автоматично да се прикачва изявление за ограничаване на отговорността (disclaimer) и указания към адресата за действия при погрешно получаване.

Приложение № 9 към чл. 41

Защита срещу нежелан софтуер

1. Нежеланият софтуер, който може да експлоатира уязвимостта на един или няколко информационни актива и да предизвика смущаване на нормалната им работа, увреждане или унищожаване, включва следните основни програми:

- а) компютърни вируси;
- б) мрежови червеи;
- в) троянски коне, и
- г) логически бомби.

2. Защитата срещу нежелан софтуер в информационните системи на административните органи трябва да бъде ориентирана в две основни направления:

- а) чрез забрана за използване на нерегламентиран софтуер;
- б) чрез задължително използване на утвърден за цялата администрация антивирусен софтуер и софтуер за откриване на нерегламентирани промени на информационните активи.

3. Администраторът на единната национална мрежа (ЕНМ) трябва да прилага средства за откриване на опити за проникване на различни нива и периметри на мрежата.

4. Програмните продукти, предназначени за откриване на опити за проникване, трябва да разпознават следните подозрителни действия в мрежата:

- а) опити да се използват услуги, блокирани от защитни стени;
- б) неочаквани заявки, особено от непознати адреси;
- в) неочаквани шифровани съобщения;
- г) извънредно активен трафик от непознати сървъри и устройства;
- д) значителни изменения на предишни действия на мрежата;
- е) опити за използване на известни системни грешки или уязвимости;

- ж) опити за вход от непознати потребители от неочаквани адреси;
- з) несанкционирано или подозрително използване на администраторски функции;
- и) значителни изменения в обичайните действия на потребител и пр.

5. При установяване на открити опити за проникване трябва незабавно:

- а) да се уведомява системният администратор за предприемане на адекватни мерки;
- б) да се изключват или ограничават мрежовите услуги, свързани с информационния актив - обект на проникването.

6. Всяко устройство, което се включва в мрежата на съответната администрация, автоматично да се проверява за вируси и нежелан софтуер, преди да получи достъп до ресурсите на мрежата.

Приложение № 10 към чл. 43, ал. 2

Действия при мониторинг на събитията и инцидентите в информационните системи на администрациите

1. При съхраняването на информация за събития и инциденти, свързани с информационните системи на администрациите, трябва да се създават следните записи:

- а) дата и време на настъпване на събитието;
- б) уникален идентификатор на ползвателя - инициатор на действието;
- в) тип на събитието;
- г) резултат от събитието;
- д) източник на събитието;
- е) списък на засегнатите обекти;
- ж) описание на измененията в системата за защита, произтекли от събитието.

2. Ръководителите на администрациите трябва да определят точни процедури за мониторинг на използването на системата, с които да осигурят изпълнението само на регламентирани процеси от страна на ползвателите. Процедурите за мониторинг трябва да осигуряват:

- а) реалистична оценка и мерки за управление на риска;
- б) проследяване на изключения или ненормално поведение на ползватели за определен период;
- в) осигуряване на записи както на успешните, така и на отказаните опити за достъп в системата.

3. За осигуряване на точност и пълнота на записите на логовете, които могат да се използват за разследване на неправомерни действия или за нуждите на ангажиране на съдебни доказателства, ръководителите на ведомствата трябва да осигурят поддържането на единно време в информационните системи съгласно Наредбата за електронните административни услуги, приета с Постановление № 107 на Министерския съвет от 2008 г. (ДВ, бр. 48 от 2008 г.).

Приложение № 11 към чл. 45 ал. 2

Параметри на физическата сигурност

1. За осигуряване физическата защита на информационни системи ръководителите на администрациите предприемат следните мерки:

- а) мерки по управление на физическия достъп;

- б) противопожарни мерки;
- в) защита на поддържащата инфраструктура;
- г) защита на мобилните системи.

2. Препоръчва се мерките за физическа защита да включват следните инфраструктурни компоненти:

2.1. Сградите и помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи на административните органи, да отговарят на следните архитектурно-строителни изисквания:

- а) помещенията да имат бетонни или тухлени стени;
- б) плочите да бъдат стоманобетонни с дебелина 0,15 [m];
- в) помещенията да имат специални подвижни отвори, които предпазват от свръхналягане;
- г) двойният под да има височина не по-малка от 0,30 [m];
- д) окаченият таван да има височина не по-малка от 0,50 [m];
- е) климатичните системи за помещенията да позволяват управление от алармени сигнали на пожарогасителна система;
- ж) до помещенията да се осигури отделна стая, в която да се разположат действащата и резервната батерии бутилки с пожарогасителния агент.

2.2. Помещенията, в които се разполагат техническото оборудване, софтуерът и архивите, необходими за информационните системи на администрациите, се оборудват със следните технически системи за защита, безопасност и охрана:

- а) пожарогасителна система, която трябва да отговаря на изискванията на EN 14520;
- б) климатизация;
- в) резервно електрозахранване;
- г) системи за телевизионно видеонаблюдение;
- д) системи за контрол на достъпа.

3. Срещите между посетителите и служителите в администрациите трябва да се извършват в специализирани помещения.

4. В случаите по т. 3 да се води списък на посетителите кога и с кого са се срещали и по какъв въпрос. Списъкът да се съхранява не по-малко от една година от датата на посещението. Списъкът може да се води и само в електронна форма.

5. Служителите, използващи преносими компютри, трябва задължително да използват пароли за достъп до ресурсите на мобилните устройства (дискети устройства, системни платки, софтуер и др.).

Приложение № 12 към чл. 48

Управление на инциденти, свързани с информационната сигурност

1. Планирането на дейността по управление на инциденти, свързани с информационната сигурност, трябва да включва следните етапи:

- а) определяне на критично важните функции на системата и установяване на приоритетите за възстановителни работи;
- б) идентификация на ресурсите, необходими за изпълнение на критично важните функции;
- в) определяне списък на възможните инциденти с вероятности за появяването им, изхождайки от оценките на риска;
- г) разработка на стратегии за възстановителни работи;

д) подготовка на мероприятия за реализация на стратегиите.

2. Цикълът на управлението на инциденти трябва да включва следните основни етапи:

а) подготовка;

б) откриване и анализ;

в) ограничаване на влиянието, премахване на причината, възстановяване;

г) дейности след инцидента.

3. Критичен елемент от управлението на инциденти е незабавното възстановяване на дейността на системата.

4. Политиката за защита от инциденти и възстановителни работи на съответната администрация, която произтича от оценката на риска по глава трета, раздел III от наредбата, трябва ясно да идентифицира средствата за резервиране и възстановяване с оглед покриване ниво на резервиране над пето по класацията на Асоциация Share.

5. Средствата по т. 4 могат да бъдат:

а) паралелно записване или огледална репликация на съхраняваните данни (технологии "Disk Mirroring" или "RAID" ("Redundant Array of Independent Drives"));

б) създаване на център за възстановяване след инциденти (т.нар. "Disaster Recovery Center"), в който се извършва постоянно архивно съхранение ("back-up") на информацията от системата, така че да може да се възстанови нейната дейност след инцидента;

в) създаване на резервен изчислителен център, в който се поддържа репликирано състояние на критичните оперативно действащи системи, така че дейността им да бъде незабавно поета от него.

6. Планът за действия при инциденти на съответната структура в администрацията трябва да включва мероприятия, които да се проведат след възстановяването и които да целят избягване на подобни инциденти. Това могат да бъдат мерки по:

а) повишаване нивото на контрол на достъпа;

б) промяна на конфигурациите на зоните за сигурност;

в) изменение на режима на физически достъп;

г) инсталиране на допълнителни модули за защита към софтуера на системата;

д) саниране и декласификация на носителите и пр.

Приложение № 13 към чл. 51

Мерки за постигане сигурност по отношение на персонала

1. За постигане на информационна сигурност по отношение на персонала ръководителите на администрациите са длъжни да предприемат следните мерки за идентификацията на служителите и оправомощаването им да извършват определени действия по отношение на експлоатацията на информационните системи:

а) достъпът на служителите в администрацията до работните им станции и общите информационни системи да се осъществява със служебни потребителско име и парола;

б) достъпът на служителите в държавната администрация до специализираните информационни системи да се осъществява със служебни потребителско име, парола и удостоверение за публичен ключ;

в) осигуряването на права за достъп на различни групи служители и ръководители до ресурсите на информационните системи в съответната администрация да се извършва на базата на утвърдените профили съгласно чл. 52 от наредбата;

г) за всеки служител в администрацията да бъде определена принадлежност към профил, съответстващ на служебните му задължения, вписани в длъжностната му характеристика;

д) служителите в администрацията да имат право на достъп само до тези ресурси на информационните системи в администрацията, в която работят, или до системите на други администрации само доколкото са им необходими за изпълнение на служебните задължения съгласно длъжностната им характеристика;

е) всяка година да се провеждат опреснителни курсове по мрежова и информационна сигурност, през които да преминават всички служители в администрацията;

ж) всички служители в администрацията да преминават обучение за действия при инциденти с мрежовата и информационна сигурност.

2. Приложението за проверка на удостоверения за публични ключове (вкл. електронни подписи) трябва да използва процедурата за проверка чрез Certificate Revocation Lists (CRL), базиран на спецификацията RFC 3280 на IETF (Internet Engineering Task Force) или по Протокол OCSP (Online Certificate Status Protocol), основан на спецификацията RFC 2560 на IETF.

Приложение № 14 към чл. 102, ал. 2

(Ново - ДВ, бр. 48 от 2013 г.)

Сценарий за проверка за съответствие с изискванията за оперативна съвместимост и информационна сигурност на техническа спецификация за разработване или придобиване на административна информационна система

Данни, идентифициращи техническата спецификация:

№ по ред	Проверка	Резултат от проверката	Инструкция за попълване на резултата и преценка дали проверката е успешна	Препоръки за отстраняване на проблемите при неуспешни проверки
1	2	3	4	5
1.	Проверка за оформяне и представяне на техническата спецификация			
1.1.	Проверка дали техническата спецификация и прилежащите графични изображения са подписани от административния орган или ръководителя на администрацията	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
2.	Проверка по чл. 106, ал. 1 Проверка дали техническата спецификация за разработване на информационна система съдържа изрично и ясно указание дали това е:		Следва с "ДА" да е попълнен или ред 2.1, или ред 2.2. Ако и в двата реда е попълнено "НЕ", системата не подлежи на проверка	
2.1.	Административна информационна система по смисъла на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите	Да/Не		
2.2.	Специализирана	Да/Не		

	информационна система, осигуряваща изцяло или частично функциите на административна информационна система, доколкото създава и/или издава, и/или приема, и/или регистрира, и/или съхранява електронни документи, регламентирани в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите			
3.	Проверка за наличие на предпоставки за проверка на придобивана или изградена информационна система			
3.1.	В техническата спецификация в явна и недвусмислена форма има изисквания за проверка на придобиваната или изгражданата информационна система по реда на чл. 103 като част от тестовете за приемане на системата	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
3.2.	В техническата спецификация в явна и недвусмислена форма е посочено, че условие за приемане на разработката е ангажимент на изпълнителя за проверка на разработваната информационна система, без да се предвиждат допълнителни разходи за възложителя	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
4.	Проверка за включени в техническата спецификация приложения за визуализация и/или редактиране на електронни документи			
4.1.	Проверка дали с техническата спецификация е предвидено създаване на приложения за визуализация и/или редактиране на структурирани електронни документи, вписани в регистъра на информационните обекти	Да/Не	Ако е попълнено с "НЕ", ред 4.2 се попълва с "НЕ Е ПРИЛОЖИМО"	
4.2.	Проверка дали в техническата спецификация има ясно и недвусмислено изискване за проверка на приложенията за визуализация на електронни документи, вписани в регистъра на информационните обекти по реда на чл. 104 като част от тестовете за приемане на	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът в ред 4.1 и в настоящия ред е "ДА", или когато отговорът в ред 4.1 е "НЕ" и в настоящия ред е "НЕ Е ПРИЛОЖИМО"	

	системата			
5.	Проверка за съответствие на техническата спецификация с изискванията за оперативна съвместимост и информационна сигурност към АИС			
5.1.	Проверка дали техническата спецификация не противоречи на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, както следва. Извършва се проверка дали в техническата спецификация няма изисквания, които са в нарушение на съответната глава или раздел на посочената наредба			
5.1.1.	о Изисквания на глава трета. Регистрация на документи в АИС. Официален документен регистър - извършва се проверка дали в техническата спецификация няма изисквания, които са в нарушение на изискванията на посочената наредба	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.2.	о Изисквания на глава четвърта. Работа със структури. Поддръжка на номенклатури			
5.1.2.1.	• Раздел II. Поддържане на преписки от документи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.2.2.	• Раздел III. Ведомствена номенклатура на видовете документи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.2.3.	• Раздел IV. Ведомствена номенклатура на етапи от услуги или процедури	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.2.4.	• Раздел V. Ведомствена номенклатура на услугите и процедурите	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.2.5.	• Раздел VII. Статус на услуга или процедура	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.3.	о Изисквания на глава пета. Получаване на електронни документи			
5.1.3.1.	• Раздел I. Приемане на електронни документи чрез уеб базирано приложение	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.3.2.	• Раздел II. Приемане на електронни документи чрез електронна поща	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	

5.1.3.3.	• Раздел III. Приемане на електронни документи на физически носител	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.3.4.	• Раздел IV. Приемане на електронни документи чрез единната среда за обмен на електронни документи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.3.5.	• Раздел V. Приложени документи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.	о Изисквания на глава шеста. Действия в състава на процедури			
5.1.4.1.	• Раздел I. Проверка за редовност	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.2.	• Раздел II. Обработката на получени документи, които не са заявление по услуга или инициращ документ по процедура	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.3.	• Раздел III. Създаване на документи и начало на тяхната обработка	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.4.	• Раздел V. Издаване на електронни документи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.5.	• Раздел VI. Възлагане на задачи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.6.	• Раздел VII. Контрол по изпълнението на пряко възложени задачи	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.7.	• Раздел VIII. Контрол на изпълнението на задачи по услуги или процедури. Анализ на дейността	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
5.1.4.8.	• Раздел IX. Достъп до преписка през интернет	Противоречи/ Не противоречи	Проверката е успешна, когато отговорът е "НЕ ПРОТИВОРЕЧИ"	
6.	Проверка относно изискванията за информационна сигурност по чл. 39 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност	Да/Не	Проверката е успешна, когато отговорът е "ДА"	

Заключение:

--

Наименование на административния орган - възложител на обществената поръчка, част от документацията за която е техническата спецификация:

Длъжност на лицето, извършило проверката:	Основание за възлагане на правомощия за извършване на проверките от посоченото лице (например номер на заповед на административния орган, вътрешни правила на администрацията):
---	---

Име на лицето, извършило проверката: Подпис на лицето, извършило проверката:
Дата:

Приложение № 15 към чл. 103, ал. 2

(Ново - ДВ, бр. 48 от 2013 г.)

Сценарий за проверка за съответствие с изискванията за оперативна съвместимост и информационна сигурност на информационна система

Проверявана информационна система: <наименование на проверяваната информационна система>
 Описание на системата като АИС: <АИС по чл. 20, ал. 1/специализирана информационна система по чл. 20, ал. 2>

Обхват на информационната системата: (попълва се за специализирана информационна система по чл. 20, ал. 2, така че да стане ясно кои проверки не са приложими за нея)

Версия на системата: <версия на проверяваната информационна система>

База от данни: <посочва се базата от данни, за която е разработена и ще бъде инсталирана системата във връзка с проверката по чл. 39, ал. 2>

№ по ред	Проверка	Подготвителни действия и въведени данни	Резултат от проверката	Инструкция за попълване на резултата и преценка дали проверката е успешна	Препоръки за отстраняване на проблемите при неуспешни проверки
1	2	3	4	5	6
1.	Проверка за създаван документ от АИС по чл. 125 от наредбата				
1.1.	Проверка за генериране на съобщение, че получаването не се потвърждава съгласно изискванията на чл. 69, ал. 3 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, който съдържа:	За да се провери генерирането на това съобщение, електронният документ (заявление) се подава в 7 различни варианта, 6 от които да симулират 6-те различни видове грешки, а един - повече от една грешка. Заявлението следва да е подадено с възможно най-пълни данни, за да може да се проследи дали документът съобщение, че получаването не се потвърждава, се генерира в съответствие с регистрацията му в Регистъра на		Тази проверка не се извършва и редовете по-долу се попълват с "НЕ Е ПРИЛОЖИМО", когато става дума за специализирана информационна система по чл. 20, ал. 2, която не приема електронни документи	

		информационните обекти с уникален регистров идентификатор 0010- 000001			
1.1.1.	УРИ на съобщението	Съобщението се регистрира от АИС и се попълва в документа	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.2.	Доставчик на електронната административна услуга	Попълва се от приложението по данни на информационната система	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.3.	Идентификатор на доставчика на електронната административна услуга	Попълва се от приложението по данни на информационната система	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.4.	Вид на пренос	Попълва се от приложението в зависимост от канала, по който се подава документът	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.	Съобщение, че получаването не се потвърждава за всяка от неуспешните проверки, извършени по реда на	За всяка от проверките по-долу се подава отделен документ съгласно описаното в редове 2.1.5.1 - 2.1.5.7.			

	чл. 48, ал. 1 от Наредбата за електронните административни услуги, приета с Постановление № 107 на Министерския съвет от 2008 г., с текст, както следва:	Информационната система извършва проверката и извежда съответстващото съобщение за причината, поради която получаването не се потвърждава			
1.1.5.1.	Размерът на заявлението заедно с приложенията надвишава определения от административния орган размер за електронните административни услуги, предоставяни от съответната администрация	Подава се заявление с прикачени документи, което надхвърля определен размер на файла, размерът се конфигурира	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.2.	Подаваното заявление не е в нормативно установения формат	Симулира се подаването на заявление, което е с нарушена структура	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.3.	Заявителят не е посочил електронен пощенски адрес	Подава се заявление, в което не е попълнен адрес на електронната поща	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.4.	Приложените към заявлението документи не са в нормативно установения формат	Подава се заявление, в което е приложен документ във форма, който не е посочен в чл. 65 от Наредбата за електронните административни услуги	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.5.	Подаденото заявление и	Подава се заявление, в което е	Да/Не/Не е приложимо	Проверката е успешна, когато	

	приложенията към него съдържат вируси или друг нежелан софтуер	приложен документ със симулация на вирус		отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.6.	Подаденото заявление не съдържа уникален идентификатор на заявителя и на получателя на електронната административна услуга при законово изискване за идентификация	Подава се заявление, в което не е попълнен уникалният идентификатор на заявителя, а услугата, за която се подава заявлението, изисква идентификация на заявителя	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.5.7.	Проверка на едновременно съобщаване на повече от една неуспешна проверка	Подава се заявление, в което не е попълнен адресът на електронната поща и уникалният идентификатор на заявителя, един от приложените документи е с недопустим формат и е приложен документ със симулация на вирус	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.6.	Сегмент "Заявител на електронна административна услуга"	Попълва се с всички данни за този сегмент от заявлението, в случаите, когато документът може да се прочете и данните да се извлекат	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.7.	Подаден документ	Попълват се данните за подадения електронен документ (заявление)	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни	

				документи	
1.1.8.	Време на създаване на съобщението	Попълва се с времето на създаване на съобщението	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.1.9.	Електронен подпис	Електронен подпис, с който се подписва съобщението	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.	Проверка за генериране на документ "Потвърждаване за получаване" съгласно изискванията на чл. 70, ал. 2 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите със следното съдържание:	За да се провери генерирането на потвърждението за получаване, електронният документ (заявление) се подава така, че всички проверки по реда на чл. 48, ал. 1 от Наредбата за електронните административни услуги да бъдат успешни. Заявлението следва да е подадено с възможно най-пълни данни, за да може да се проследи дали документът потвърждаване за получаване се генерира в съответствие с регистрацията му в Регистъра на информационните обекти с уникален регистров идентификатор 0010-000002		Тази проверка не се извършва и редовете по-долу се попълват с "НЕ Е ПРИЛОЖИМО", когато става дума за специализирана информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.1.	Наименование на администрацията	Попълва се от приложението по	Да/Не/Не е приложимо	Проверката е успешна, когато	

		данни на информационната система		отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.2.	Идентификатор на администрацията	Попълва се от приложението по данни на информационната система	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.3.	Уникален регистров идентификатор на подадения документ	Попълва се регистрацията в АИС на подаденото заявление	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.4.	Вид на пренос	Попълва се от приложението в зависимост от канала, по който се подава документът	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.5.	Сегмент "Заявител на електронната административна услуга"	Попълва се с всички данни за този сегмент от заявлението в случаите, когато документът може да се прочете и данните да се извлекат	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.6.	Подаден документ	Попълват се данните	Да/Не/Не е	Проверката е	

		за вида подаден документ (заявление) с данните за регистрацията на този вид подаден документ в Регистъра на информационните обекти	приложимо	успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.7.	Извършил регистрацията	В АИС се записват данните на лицето или информационната система (когато регистрацията е направена в автоматичен режим)	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.8.	Време на получаване	Попълва се с времето на получаването (регистрацията) на заявлението	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.9.	Информация за достъп до получения документ и всички приложения към него документи	Попълва се информацията за достъп до получения документ и всички приложения към него документи в информационната система. Подход за реализация: <тук следва да се опише как се дава сигурен достъп посредством информацията за достъп до получения документ и всички приложения към него документи в информационната система>	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.2.10.	Електронен подпис	Електронен подпис, с който се подписва потвърждението	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е	

				ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която не приема електронни документи	
1.3.	Проверка за генериране на документ "Контейнер за пренос" съгласно изискванията на чл. 79 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, вписан в Регистъра на информационните обекти с уникален регистров идентификатор 0010-000003	<Тук се описва начинът на конкретната бизнес логика на създаването и попълването на контейнера за пренос за конкретната информационна система>		Тази проверка не се извършва и редовете по-долу се попълват с "НЕ Е ПРИЛОЖИМО", когато става дума за специализирана информационна система по чл. 20, ал. 2, която обменя данни с други администрации само като структурирани документи и не се налага използването на контейнер за пренос	
1.3.1.	УРИ на контейнер за пренос	Въвежда се УРИ на регистрацията на контейнера за пренос в информационната система	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която обменя само структурирани документи и не използва контейнер за пренос	
1.3.2.	Кратко и разширено описание на преноса за контейнера	Въвежда се краткото и разширеното описание на преноса за контейнера	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която обменя само структурирани документи и не използва контейнер за пренос	
1.3.3.	Пренасян документ	Въвежда се УРИ на регистрацията, кратко и разширено описание и файлово	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е	

		съдържание на пренасяния документ		ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която обменя само структурирани документи и не използва контейнер за пренос	
1.3.4.	Електронен подпис	Електронен подпис, с който се подписва контейнерът за пренос	Да/Не/Не е приложимо	Проверката е успешна, когато отговорът е "ДА", както и "НЕ Е ПРИЛОЖИМО" само в случаите, когато става дума за информационна система по чл. 20, ал. 2, която обменя само структурирани документи и не използва контейнер за пренос	

№ по ред	Проверка	Резултат от проверката	Инструкция за попълване на резултата и преценка дали проверката е успешна	Препоръки за отстраняване на проблемите при неуспешни проверки
1	2	3	4	5
2.	Проверка на системата за управление на бази данни			
2.1.	Проверка дали съхранението и достъпът до данните в АИС се осъществяват чрез системи за управление на бази данни и се идентифицира нейният вид	ДА/НЕ	Проверката е успешна, когато отговорът е "ДА"	
2.2.	Проверка дали системата за управление на бази е сертифицирана в съответствие с международния стандарт ISO/IEC 15408:2005, определящ т.нар. "Common Criteria for Information Technology Security Evaluation (CC)", в съответствие с националните приложения на международния стандарт ISO/IEC 15408:2005, като "IT-Grundschutz Methodology" на BSI (Германия), или е сертифицирана с американския федерален профил "US Government Protection Profile for Database Management System in Basic Robustness Environments". Тук се посочва препратка към съответния сертификат	ДА/НЕ	Проверката е успешна, когато отговорът е "ДА"	
3.	Проверка на способността на системата за работа с файлове	ДА/НЕ	Проверката е успешна, когато отговорът е	

	съдържание на документи в многопотребителски режим Прави се проверка дали е осигурен многопотребителски достъп до съдържанието на електронни документи чрез информационната система и дали има функции по заключване и отключване на документи за осигуряване на съвместна работа с документи		"ДА"	
4.	Проверка на ниво на защита			
4.1.	Извършва се проверка дали минималното ниво на защита на достъпа до ресурсите на информационната система е "1" или "С", както следва:			
4.1.1.	Достъпът до точно определени обекти се разрешава на точно определени ползватели			
4.1.2.	Ползвателите се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп. За установяване на идентичността се използва защитен механизъм от типа идентификатор/парола			
4.1.3.	Идентифициращата информация трябва да е защитена от нерегламентиран достъп			
4.1.4.	Доверителната изчислителна система, т.е. функционалността на информационната система, която управлява достъпа до ресурсите ѝ, поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи ходът на работата			
4.1.5.	Информационната система разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система			
4.1.6.	Извършен тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система			

Заключение:

--

Наименование на заинтересуваното лице - доставчик или разработчик на информационната система:	
<Управляващ/представяващ заинтересуваното лице> (не се попълва, ако заинтересуваното лице е физическо лице):	Наименование и идентификатор на заинтересуваното лице:

Име на управляващия/представяващия заинтересуваното лице:	Подпис:
Дата:	

Приложение № 16 към чл. 104, ал. 2

(Ново - ДВ, бр. 48 от 2013 г.)

Сценарий за проверка за съответствие с изискванията за оперативна съвместимост и информационна сигурност на програмни приложения за визуализация и/или редактиране на електронни документи

Вид на приложението: <приложение за визуализация/приложение за редактиране и визуализация>

Приложенията могат да бъдат:

1. Приложение за визуализация на електронни документи, когато с него могат само да се визуализират електронни документи.
2. Приложение за редактиране и визуализация на електронни документи, когато с него могат да се създават и редактират електронните документи. В този случай те се и визуализират.

Списък от електронни документи, които се редактират и/или визуализират с приложението

№ по ред	Проверка	Резултат от проверката	Инструкция за попълване на резултата и преценка дали проверката е успешна	Препоръки за отстраняване на проблемите при неуспешни проверки
1	2	3	4	5
1.	Проверка за четене и визуализиране на съдържание на електронен документ от файл Прави се проверка дали приложението може да прочете и визуализира съдържанието на електронния документ от файл, записан в информационната система, намираща се под контрол на потребителя:		Тази проверка се прави и за двата вида приложения - приложение за визуализация или приложение за редактиране и визуализация	
1.1.	На локален диск	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
1.2.	На външен носител	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
2.	Проверка на приложение за редактиране и визуализация на електронни документи за наличие на функционалност за запис на електронен документ Прави се проверка на приложението за редактиране и визуализация на електронни документи като файл в информационната система, намираща се под контрол на потребителя			
2.1.	На локален диск	Да/Не/Не е приложимо	Когато приложението е за редактиране и	

			визуализация на електронни документи, проверката е успешна, когато отговорът е "ДА". Когато приложението е само за визуализация на електронни документи, в този ред се попълва "НЕ Е ПРИЛОЖИМО"	
2.2.	На външен носител	Да/Не/Не е приложимо	Когато приложението е за редактиране и визуализация на електронен документ, проверката е успешна, когато отговорът е "ДА". Когато приложението е само за визуализация на електронен документ, в този ред се попълва "НЕ Е ПРИЛОЖИМО"	
3.	Проверка дали приложенията за визуализация и/или редактиране на електронен документ осигуряват възможност за установяване на несъответствия в съдържанието на визуализиран или редактиран документ с регистрацията му в регистъра на информационните обекти	Да/Не	Проверката е успешна, когато отговорът е "ДА"	

Следващите проверки се правят поотделно за всеки електронен документ, който се визуализира и/или редактира с приложението. За електронния документ с неговия уникален регистров идентификатор на вписване в Регистъра на информационните обекти се взема сегментът, с който се създава този документ, като този сегмент се проследява през неговите съставни сегменти и стойности надолу по йерархията на съставлящите ги данни, докато се извлекат всички единични данни в състава на електронния документ. За сегмента, с който се създава документът, и всички създаващи го сегменти и стойности надолу по йерархията на данните се установяват всички възможни грешки, описани в Регистъра на електронните документи за определените по-горе сегменти и стойности, със съответните съобщения за грешки.

За да се проиграят всички случаи, заинтересуваното лице трябва да подготви тестов набор от документи, съдържащи тестови данни за провеждане на тестове за съответствие с регистрацията в регистъра на информационните обекти. В тестовия набор от документи само един документ не трябва да съдържа отклонения от регистрацията на съответния вид документ. Заинтересуваното лице може да използва вписан в Регистъра на проверените системи тестов набор от данни за конкретния електронен документ. Независимо от това дали заинтересуваното лице е подготвило, или използва готов тестов набор от данни, отговорността за пълнотата на набора от документи е негова.

Следващата секция следва да се включи толкова пъти, колко вида електронни документи се визуализират и/или редактират с приложението.

Наименование на електронния документ:

Уникален регистров идентификатор на вписване на електронния документ, за който се извършва проверката, в Регистъра на информационните обекти:

(ако електронният документ не е вписан, тук се посочва входящият номер на заявлението за вписване и поредният номер на електронния документ в заявлението)

Данни за заинтересуваното лице, изпратило за вписване набора от тестови документи, с който е извършена проверката:
(попълва се, ако се използва готов набор от тестови документи, вписан в списъка на проверените информационни системи)

№ по ред	Проверка	Резултат от проверката	Инструкция за попълване на резултата и преценка дали проверката е успешна	Препоръки за отстраняване на проблемите при неуспешни проверки
1	2	3	4	5
4.1.	<p>Проверка дали всички данни от състава на електронния документ (представени със сегменти и стойности) вярно и точно се визуализират в съответствие с регистрацията на този електронен документ в регистъра на информационните обекти. Проверката се прави с документа от тестовия набор от документи, който не съдържа отклонения от регистрацията за документа в Регистъра на информационните обекти.</p> <p>По-долу се описват всички сегменти и стойности в тяхната йерархия в състава на електронния документ, за които е извършена проверката за визуализация:</p> <ul style="list-style-type: none"> - <Сегмент 1> - <Сегмент 2> - <Стойност 1> <p>.....</p>	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
4.2.	<p>Проверка дали приложението ще изведе съобщения за грешка за всеки вид грешки, вписани в регистъра на информационните обекти, за всеки сегмент и стойност в състава на електронния документ. Проверката се прави с документите от тестовия набор от документи, които съдържат съответното отклонение от регистрацията на документа в Регистъра на информационните обекти. За всяка грешка следва да се изведе съобщение със съответния уникален регистров идентификатор на термин в Регистъра на информационните обекти.</p> <p>По-долу се описват всички сегменти и стойности в тяхната йерархия в състава на електронния документ и грешките за тях, за които е извършена проверката:</p> <ul style="list-style-type: none"> - <Сегмент 1> <ul style="list-style-type: none"> a. Грешка 1 b. Грешка 2 - <Сегмент 2> <ul style="list-style-type: none"> a. Грешка 3 b. Грешка 4 - <Стойност 1> <p>.....</p> <ul style="list-style-type: none"> a. Грешка 5 	Да/Не	Проверката е успешна, когато отговорът е "ДА"	
4.3.	<p>Проверка на приложение за редактиране и визуализация на електронни документи за наличие на функционалност за създаване, изтриване и корекция на съдържанието на всички данни съгласно регистрацията на електронния документ в Регистъра на информационните обекти</p>			

4.3.1.	<p>Създаване</p> <p>По-долу се описват всички сегменти и стойности в тяхната йерархия в състава на електронния документ, за които е извършена проверката за визуализация:</p> <p>- <Сегмент 1> - <Сегмент 2> - <Стойност 1> </p>	Да/Не/Не е приложимо	<p>Когато приложението е за редактиране и визуализация на електронни документи, проверката е успешна, когато отговорът е "ДА" Когато приложението е само за визуализация на електронни документи, в този ред се попълва "НЕ Е ПРИЛОЖИМО"</p>	
4.3.2.	<p>Изтриване</p> <p>По-долу се описват всички сегменти и стойности в тяхната йерархия в състава на електронния документ, за които е извършена проверката за визуализация:</p> <p>- <Сегмент 1> - <Сегмент 2> - <Стойност 1> </p>	Да/Не/Не е приложимо	<p>Когато приложението е за редактиране и визуализация на електронни документи, проверката е успешна, когато отговорът е "ДА". Когато приложението е само за визуализация на електронни документи, в този ред се попълва "НЕ Е ПРИЛОЖИМО"</p>	
4.3.3.	<p>Корекция</p> <p>По-долу се описват всички сегменти и стойности в тяхната йерархия в състава на електронния документ, за които е извършена проверката за</p>	Да/Не/Не е приложимо	<p>Когато приложението е за редактиране и визуализация на електронни документи, проверката е успешна, когато отговорът е "ДА". Когато приложението е само за</p>	

<p>визуализация:</p> <p>- <Сегмент 1> - <Сегмент 2> - <Стойност 1></p> <p>.....</p>	<p>визуализация на електронни документи, в този ред се попълва "НЕ Е ПРИЛОЖИМО".</p>
---	--

Заклучение:

<p>Наименование на заинтересуваното лице - доставчик или разработчик на приложението за визуализация и/или редактиране:</p>	
<p><Управляващ/представляващ заинтересуваното лице> (не се попълва, ако заинтересуваното лице е физическо лице):</p>	<p>Наименование и идентификатор на заинтересуваното лице:</p>
<p>Име на управляващия/представляващия заинтересуваното лице:</p>	<p>Подпис:</p>
<p>Дата:</p>	