НАРЕДБА за общите изисквания за мрежова и информационна сигурност (Загл. изм. – ДВ, бр. 5 от 2017 г., в сила от 1.03.2017 г.)

Приета с ПМС № 279 от 17.11.2008 г., обн., ДВ, бр. 101 от 25.11.2008 г., в сила от 25.11.2008 г., изм., бр. 58 от 30.07.2010 г., в сила от 30.07.2010 г., изм. и доп., бр. 102 от 30.12.2010 г., бр. 48 от 31.05.2013 г., бр. 5 от 17.01.2017 г., в сила от 1.03.2017 г.

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С наредбата се уреждат:

1. (изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) общите изисквания за мрежова и информационна сигурност за нуждите на предоставянето на вътрешни електронни административни услуги и обмена на електронни документи между администрациите;

2. (отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.);

3. (отм. - ДВ, бр. 48 от 2013 г.);

4. (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Методиката за извършване на оценка за съответствие с изискванията за мрежова и информационна сигурност;

5. (изм. - ДВ, бр. 48 от 2013 г., изм. и доп., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) начинът на удостоверяване съответствието на внедряваните от административните органи информационни системи с установените нормативни изисквания за мрежова и информационна сигурност и вписването им в списъка на информационните системи, чието съответствие е удостоверено по реда на наредбата.

(2) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Наредбата не урежда мрежовата и информационната сигурност на информационните системи на административните органи и правилата за мрежова и 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. (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Спазването на изискванията за мрежова и информационна сигурност се гарантира чрез:

1. (изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.);

2. (отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.);

3. (доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) сертификация и одит на администрациите по отношение на система за управление на мрежовата и информационната сигурност, в съответствие с международния стандарт ISO 27001:2005;

4. (изм. - ДВ, бр. 48 от 2013 г., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) контрол от страна на председателя на Държавна агенция "Електронно управление" в изпълнение на чл. 60 от Закона за електронното управление.

Глава втора
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
ОПЕРАТИВНА СЪВМЕСТИМОСТ

Раздел I
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Изисквания за свързаност между информационните системи на административните органи

Чл. 4. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 5. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 6. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 7. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел II
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Изисквания за оперативна съвместимост по отношение на данните

Чл. 8. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 9. (Доп. - ДВ, бр. 102 от 2010 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 10. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 11. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 12. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 13. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел III
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)

Изисквания за оперативна съвместимост по отношение на електронните документи

Чл. 14. (Доп. - ДВ, бр. 102 от 2010 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел IV
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Изисквания за оперативна съвместимост по отношение на приложения за визуализация и/или редактиране на електронни документи

Чл. 15. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 16. (Изм. - ДВ, бр. 102 от 2010 г., бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 17. (Изм. – ДВ, бр. 102 от 2010 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 18. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 19. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел V
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Оперативна съвместимост по отношение на информационни системи

Чл. 20. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 21. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 22. (Изм. - ДВ, бр. 102 от 2010 г., отм., бр. 48 от 2013 г.).

Чл. 23. (Изм. - ДВ, бр. 102 от 2010 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Глава трета
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ
(Загл. доп. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)

Раздел I
Политика за мрежова и информационна сигурност

(Загл. доп. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)

Чл. 24. (1) (Предишен текст на чл. 24 – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) 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.

(2) (Нова, доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Политиката за мрежова и информационна сигурност трябва да отговаря на изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194 от 19 юли 2016 г.).

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) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Вътрешните правила по ал. 2 се изграждат по модела на "Системи за управление на мрежовата и 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.

(5) (Нова, доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление" изготвя образци на документи за осъществяване на политика за мрежова и информационна сигурност.

(6) (Нова, доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление" издава задължителни разпореждания към административните органи за привеждане на политиката им за мрежова и информационна сигурност към изискванията на тази глава.

(7) (Нова – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление" определя длъжностни лица, които извършват проверки за съответствие на вътрешни правила и

информационни системи с изискванията за мрежова и информационна сигурност.

Чл. 27. (1) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Ръководителите на администрациите осигуряват сертификация на вътрешните правила като "Система за управление на мрежовата и 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. 5 от 2017 г.** , в сила от 1.03.2017 г.) Резултатите от сертификацията по ал. 1 и от проверките по ал. 2 се предоставят незабавно и на председателя на Държавна агенция "Електронно управление" за целите на текущия контрол в съответствие с чл. 60 от Закона за електронното управление.

(4) (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Предоставянето на информацията по ал. 3 се осъществява като вътрешна електронна административна услуга, която председателят на Държавна агенция "Електронно управление" 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) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Функциите на служителя или на звеното по мрежова и информационна сигурност са описани в приложение № 2.

(4) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Когато администрация към административен орган има териториални структури и разпределени информационни системи, служител, отговарящ за мрежовата и информационната сигурност, се определя и във всяко териториално звено.

Чл. 29. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Ръководителите на администрациите осигуряват необходимата инфраструктура за гарантиране на мрежовата и информационната сигурност на използваните от тях информационни системи съгласно вътрешните правила по чл. 26, ал. 2.

Чл. 30. (1) (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Към председателя на Държавна агенция "Електронно управление" 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. 5 от 2017 г.** , в сила от 1.03.2017 г.) Съветът за мрежова и информационна сигурност на информационните системи на административните органи работи въз основа на правилник, утвърден от председателя на Държавна агенция "Електронно управление".

(3) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) 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 мрежовата и 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. (1) (Предишен текст на чл. 35 – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Ръководителите на администрациите са длъжни да предприемат необходимите действия за създаване и поддържане на инвентарни списъци на наличните информационни активи съгласно приложение № 6.

(2) (Нова – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) За инвентарен списък се считат вписаните данни в регистъра на информационните ресурси, воден от председателя на Държавна агенция "Електронно управление".

Чл. 35а. (Нов – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) (1) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление" води списък със сигнали за проблеми с мрежовата и информационната сигурност и техния статус.

(2) Ръководителят на администрацията, за чиято информационна система се отнася сигналът, взема необходимите мерки за отстраняване на проблема в срок един месец от подаването на сигнала.

(3) Шест месеца след подаването на сигнала той става публично достъпен в списъка на страницата на Държавна агенция "Електронно управление".

(4) Подаването на сигнали се извършва чрез уеббазиран формуляр или по електронна поща.

(5) Председателят на Държавна агенция "Електронно управление" определя правила за отговорно откриване и докладване на уязвимости. Правилата не могат да позволяват трайно извличане на лични данни или пароли извън необходимото за демонстриране на уязвимостта.

Раздел IV
Управление на експлоатационните процеси

Чл. 36. (1) (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Към председателя на Държавна агенция "Електронно управление" се създава Национален център за действие при инциденти по отношение на мрежовата и информационната сигурност като административно звено в специализираната администрация.

(2) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Създаването на Националния център за действие при инциденти по отношение на мрежовата и 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) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Служителят или звеното по мрежова и 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. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Националният център за действие при инциденти по отношение на мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) В годишните доклади за състоянието на мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Служителят или звеното по мрежова и

информационна сигурност в съответната администрация са длъжни да уведомяват незабавно Националния център за действие при инциденти по отношение на мрежовата и информационната сигурност за всеки инцидент в информационните системи на администрацията.

Чл. 50. (Изм. и доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Съветът за мрежова и информационна сигурност на информационните системи на административните органи периодично обсъжда и предлага на председателя на Държавна агенция "Електронно управление" за утвърждаване препоръчителни управленски мерки за предотвратяване на инциденти в мрежовата и 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
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
РЕГИСТЪР НА СТАНДАРТИТЕ

Раздел I
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Общи положения за регистъра на стандартите

Чл. 53. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 54. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 55. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 56. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел II
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Подлежащи на вписване обстоятелства

Чл. 57. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 58. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел III
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Водене на регистъра

Чл. 59. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 60. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 61. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 62. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 63. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 64. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 65. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 66. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 67. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел IV
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Съхраняване и достъп до регистъра

Чл. 68. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 69. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 70. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 71. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 72. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел V
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Съвет по стандарти за оперативна съвместимост и информационна сигурност

Чл. 73. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 74. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 75. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 76. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 77. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Глава пета
(Отм. - ДВ, бр. 48 от 2013 г.)
АКРЕДИТАЦИЯ НА ПРОВЕРЯВАЩИ ЛИЦА

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

Чл. 78. (Отм. - ДВ, бр. 48 от 2013 г.).

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

Чл. 80. (Отм. - ДВ, бр. 48 от 2013 г.).

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

Чл. 82. (Отм. - ДВ, бр. 48 от 2013 г.).

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

Раздел II

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

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. (Отм. - ДВ, бр. 48 от 2013 г.).

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

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

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

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

Чл. 91. (Отм. - ДВ, бр. 48 от 2013 г.).

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

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

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
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
ОЦЕНКА ЗА СЪОТВЕТСТВИЕ С ИЗИСКВАНИЯТА ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ
(Загл. изм. - ДВ, бр. 48 от 2013 г.)

Раздел I
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Общи положения

Чл. 98. (Изм. и доп. - ДВ, бр. 102 от 2010 г., изм., бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 99. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Чл. 101. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел II
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
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., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 103. (Изм. и доп. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 104. (Изм. и доп. - ДВ, бр. 48 от 2013 г., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 104а. (Нов - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 104б. (Нов - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 104в. (Нов - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Раздел III
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
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., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 107. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел IV
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
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. (Изм. и доп. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 109. (1) (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Чл. 111. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Раздел V
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
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. (Изм. и доп. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 113. (Изм. - ДВ, бр. 102 от 2010 г., бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 114. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Чл. 116. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 117. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 118. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

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
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Проверки за оперативна съвместимост и информационна сигурност на информационни системи
(Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 122. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 123. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 124. (Доп. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 125. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

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

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

Раздел IX
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
Задължение за уведомяване. Събиране на информация

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

Чл. 132. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Чл. 133а. (Нов - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Глава седма
(Отм. – ДВ, бр. 5 от 2017 г. , в сила от 1.03.2017 г.)
СПИСЪК НА УДОСТОВЕРЕНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ
(Загл. изм. - ДВ, бр. 48 от 2013 г.)

Чл. 134. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 135. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

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

Чл. 138. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 139. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 140. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 141. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 142. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 143. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 144. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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

Чл. 146. (Изм. и доп. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 147. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 148. (Изм. – ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 149. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 150. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 151. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 152. (Отм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 153. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

Чл. 154. (Отм. - ДВ, бр. 48 от 2013 г.).

Чл. 155. (Изм. - ДВ, бр. 48 от 2013 г., отм., **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.).

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. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) "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 мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) "Политика за мрежова и 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 функцион

алност, основана на системна техническа, платформена и софтуерна независимост между информационната система на доставчика на услугата и на получателя й;

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 й, 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. (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление осигурява първоначалното въвеждане на данни в регистъра на стандартите в срок 3 месеца от обнародването на наредбата в "Държавен вестник".

§ 4. (1) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) 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 мрежовата и информационната сигурност по ISO 27001:2005.

(2) (Доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) 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 мрежовата и информационната сигурност" и международния стандарт ISO 27001:2005.

§ 5. (Отм. - ДВ, бр. 48 от 2013 г.).

§ 6. (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) В срок 12 месеца от влизането в сила на наредбата председателят на Държавна агенция "Електронно управление създава Съвет за мрежова и информационна сигурност на информационните системи на административните органи като консултативен орган, подпомагащ неговата дейност.

§ 7. (Изм. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) В срок 12 месеца от влизането в сила на наредбата председателят на Държавна агенция "Електронно управление 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. (Изм. и доп. – ДВ, **бр. 5 от 2017 г.** , в сила от 1.03.2017 г.) Председателят на Държавна агенция "Електронно управление създава Национален център за действие при инциденти по отношение на мрежовата и 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

на Министерския съвет от 23 юли 2010 г. за изменение и

допълнение на нормативни актове на Министерския съвет

(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".

.....

ПОСТАНОВЛЕНИЕ № 311

на Министерския съвет от 20 декември 2010 г. за изменение

и допълнение на нормативни актове на Министерския съвет

(ДВ, бр. 102 от 2010 г.)

.....

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 на Министерския съвет от 18 май 2013 г.

за изменение и допълнение на Наредбата за общите изисквания за

оперативна съвместимост и информационна сигурност

(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.

.....

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

към Постановление № 3 на Министерския съвет от 9 януари 2017 г.

за приемане на Наредба за общите изисквания към информационните системи,

регистрите и електронните административни услуги

(ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.)

.....

§ 4. 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. и доп., бр. 58 и 102 от 2010 г. и бр. 48 от 2013 г.), се правят следните изменения и допълнения:

.....

12. Навсякъде в наредбата думите "оперативна съвместимост" и "оперативна съвместимост и" се заличават, пред думите "информационна сигурност" се добавя "мрежова и", а думите "министъра на транспорта, информационните технологии и съобщенията" се заменят с "председателя на Държавна агенция "Електронно управление".

.....

§ 11. В срок 12 месеца от влизането в сила на постановлението председателят на Държавна агенция "Електронно управление" изготвя и представя на Министерския съвет проект на изменение на Наредбата за обмена на документи в администрацията, с който регулираните с нея процеси се привеждат в съответствие с изискванията на ISO 15489: Information and Documentation – Records management.

§ 12. В срок два месеца след влизането в сила на постановлението Съветът по вписванията и Съветът по

стандартите за оперативна съвместимост и информационна сигурност се закриват.

.....

Приложение 1

към чл. 25, ал. 2

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

Общи стратегии за мрежова и информационна сигурност

(Загл. доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.)

1. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Политиката за мрежова и информационна сигурност е набор от нормативни документи, правила и норми за поведение, които определят как организацията защищава обработката, съхранението и разпространението на информацията.

2. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) 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 мрежовата и 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", обезпечаваща 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 запушване" - 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
(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

Функции на служителя (звеното) по мрежова и информационна сигурност

(Загл. доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.)

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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Следи за прилагането на стандартите, политиките и правилата за мрежова и информационна сигурност и управление на риска в администрацията.

3. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Консултира ръководството на администрацията във връзка с мрежовата и информационната сигурност.

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

5. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Периодично (не по-малко от два пъти годишно) изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на ръководителя.

6. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Координира обучението на ръководителите и служителите в административното звено във връзка с мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Участва в изготвянето на политиките, целите, процедурите и метриката за оценка на мрежовата и информационната сигурност.

10. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Поддържа връзки с други администрации, организации и експерти, работещи в областта на мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Следи за изпълнението на утвърдените от

ръководителя на администрацията инструкции и процедури, свързани с мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Изготвя доклади и анализи за настъпили инциденти, засягащи мрежовата и 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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) При възникване на какъвто и да е инцидент, свързан с мрежовата и информационната сигурност, го документира и информира незабавно ръководителя на съответната администрация и Националния център за действие при инциденти по отношение на мрежовата и информационната сигурност в информационните системи на административните органи.

20. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Разработва и предлага иновативни решения и архитектури за подобряване на мрежовата и 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

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Заплахите за мрежовата и информационната

сигурност се класифицират по следните критерии:

а) по елементите на мрежовата и 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 цикличен 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 авариите 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

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

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 използваните 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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) При проверка на идентичността чрез криптографски модули информационната система трябва да прилага методи, отговарящи на стандартите, вписани в раздел "Мрежова и 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) документирани 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

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

Управление на експлоатационните процеси

1. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Като основно средство за управление на експлоатационните процеси в информационните системи на администрациите за осигуряване на мрежова и 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 Инструкция за резервиране и архивиране на данни и файлове;

в) да се осигури редовно изготвяне на резервни копия на базите данни и файловете във файловите 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 файловите 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) (доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) достъпът до резервни и архивни копия се извършва под контрола на служителя по мрежова и информационна сигурност.

Приложение 8

към чл. 37

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

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 роботи;

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. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) 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 мрежова и информационна сигурност, специалисти от Националния център за действие при инциденти по отношение на мрежовата и 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 PFC 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 идентифициращa 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 (дискови устройства, системни платки, софтуер и др.).

Приложение 12

към чл. 48

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

Управление на инциденти, свързани с мрежовата и информационната сигурност

(Загл. доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.)

1. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) Планирането на дейността по управление на инциденти, свързани с мрежовата и 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

(Доп. – ДВ, **бр. 5 от 2017 г.** ,

в сила от 1.03.2017 г.)

Мерки за постигане сигурност по отношение на персонала

1. (Доп. – ДВ, **бр. 5 от 2017 г.**, в сила от 1.03.2017 г.) За постигане на мрежова и 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 преминат 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.,
отм., **бр. 5 от 2017 г.** ,
в сила от 1.03.2017 г.)

Приложение 15
към чл. 103, ал. 2
(Ново - ДВ, бр. 48 от 2013 г.,
отм., **бр. 5 от 2017 г.** ,
в сила от 1.03.2017 г.)

Приложение 16
към чл. 104, ал. 2
(Ново - ДВ, бр. 48 от 2013 г.,
отм., **бр. 5 от 2017 г.** ,
в сила от 1.03.2017 г.)