НАРЕДБА за минималните изисквания за мрежова и информационна сигурност

Приета с ПМС № 186 от 26.07.2019 г., обн., ДВ, бр. 59 от 26.07.2019 г., в сила от 26.07.2019 г.

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Обхват

Чл. 1. (1) Тази наредба се прилага за следните субекти:

1. административните органи;

2. операторите на съществени услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на съществени услуги;

3. доставчиците на цифрови услуги по смисъла на Закона за киберсигурност относно техните мрежи и информационни системи, използвани при предоставянето на цифрови услуги;

4. лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги по смисъла на Закона за киберсигурност, когато тези лица предоставят административни услуги по електронен път;

5. организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на Закона за киберсигурност, когато тези организации предоставят административни услуги по електронен път.

(2) С наредбата се уреждат:

1. изисквания за минималните мерки за мрежова и информационна сигурност;

2. препоръчителни мерки за мрежова и информационна сигурност;

3. правила за извършване на проверките за съответствие с изискванията на тази наредба;

4. редът за водене, съхраняване и достъп до регистъра на съществените услуги по чл. 6 от Закона за киберсигурност;

5. образец на уведомленията за инциденти.

Принципи

Чл. 2. (1) По своя характер мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на дейността на Субекта и трябва да са подходящи и пропорционални на рисковете за постигането на основните цели на мрежовата и информационната сигурност.

(2) Мерките по ал. 1 гарантират основните цели на мрежовата и информационната сигурност, а именно запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на Субекта.

(3) Мерките по ал. 1 са съобразени с изискванията на националните нормативни актове, регламентите на Европейския съюз и приетите и приложени от Субекта стандарти, като се вземат предвид краткосрочните, основните и общите рискове за сигурността за съответния сектор.

(4) Мерките за мрежова и информационна сигурност се прилагат съобразно указанията на приложимите международни стандарти, посочени в приложение № 1, препоръките на производители и доставчици на софтуер и хардуер, както и с добрите практики, препоръчани от водещи в областта на сигурността организации.

(5) Мерките по ал. 1 трябва да са:

1. разнородни – постигането на всяка от целите на мрежовата и информационната сигурност се реализира с различни по характер и специфика мерки, което създава условие за многослойна защита, или т. нар. "дълбока отбрана";

2. конкретни и лесни за възприемане, за да се гарантира, че мерките действително се прилагат;

3. ефикасни – да имат най-голямо въздействие върху потенциални заплахи, като се избягва ненужен разход на ресурси;

4. пропорционални на рисковете – с оглед на постигане на оптимално съотношение между разходи и ползи при реализиране на целите на мрежовата и информационната сигурност;

5. проверими – гарантират, че Субектът може да предостави на съответния национален компетентен орган по смисъла на чл. 16 от Закона за киберсигурност доказателства за ефективното им прилагане в съответствие с изискването на чл. 16, ал. 3 от същия закон.

(6) Минималните мерки за мрежова и информационна сигурност, посочени в тази наредба, не са обвързани с определени технологии.

Глава втора
МИНИМАЛНИ МЕРКИ ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Раздел I
Управление на мрежовата и информационната сигурност

Разпределение на роли и отговорности

Чл. 3. (1) Административният орган, съответно ръководителят на Субекта по чл. 1, ал. 1, т. 2 – 5:

1. носи пряка отговорност за мрежовата и информационната сигурност в обхвата на наредбата, дори и когато дейността е възложена за изпълнение на трети страни;

2. създава условия за прилагане на комплексна система от мерки за управление на тази сигурност по смисъла на международен стандарт БДС ISO/IEC 27001; системата обхваща всички области на сигурност, които засягат мрежовата и информационната сигурност на Субекта, включително физическата сигурност на информационните и комуникационните системи;

3. осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност в обхвата на наредбата;

4. упражнява контрол върху нивото на мрежовата и информационната сигурност чрез:

а) организиране на одити по смисъла на чл. 35, ал. 1, т. 1 и 3 за доказване на съответствието на предприетите мерки с изискванията на нормативните актове и приетите стандарти;

б) провеждане минимум веднъж в годината на периодичен преглед на мрежовата и информационната сигурност и на адекватността на предприетите мерки;

5. определя, документира и налага отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи, като се спазва принципът, че едно лице не може да контролира собствената си дейност.

(2) Лицето по ал. 1 определя служител или административно звено,

отговарящо за мрежовата и информационната сигурност, като:

1. служителят или звеното, отговарящо за мрежовата и информационната сигурност, е на пряко подчинение на административния орган, съответно на ръководителя на Субекта, по чл. 1, ал. 1, т. 2 – 5 с цел пряко информиране за състоянието и проблемите в мрежовата и информационната сигурност;

2. препоръчителни функции на служителя или на звеното, отговарящо за мрежовата и информационната сигурност, са описани в приложение № 6.

(3) Когато субектът има териториални структури и разпределени информационни системи, за всяка от тези структури се определя служител, отговарящ за мрежовата и информационната сигурност.

Политика за сигурност

Чл. 4. (1) Субектите разработват и приемат собствена политика за мрежова и информационна сигурност, която се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

(2) Политиката съдържа стратегическите цели на Субекта за мрежовата и информационната сигурност и подхода за постигането им в съответствие с общите му стратегически и оперативни цели, нормативните актове и договорите, текущите и потенциалните вътрешни и външни заплахи за постигането на тези цели и за сигурността на информацията.

(3) Политиката има отношение към или включва всички съответни специфични политики за сигурност на информационните и комуникационните системи, като обмен на информация, използване на мобилни устройства, работа от разстояние, използване на криптографски механизми, управление на достъпите и автентикацията, разработване на нови системи, управление на инциденти, взаимоотношение с трети страни, повишаване на квалификацията на служителите и на осведомеността по отношение на мрежовата и информационната сигурност и др.

Документирана информация

Чл. 5. (1) За намаляване на загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, Субектът поддържа следната документация:

1. опис на информационните активи;
2. физическа схема на свързаност;
3. логическа схема на информационните потоци;
4. документация на структурната кабелна система;
5. техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;
6. инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;
7. вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

(2) Документацията по ал. 1 трябва да е:

1. еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
2. поддържана в актуално състояние, като се преразглежда и при необходимост се обновява поне веднъж годишно;
3. одобрена от административен орган, съответно от ръководителя на

Субекта по чл. 1, ал. 1, т. 2 – 5 или от упълномощено от него лице;

4. класифицирана по смисъла на чл. 6;

5. достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

(3) Субектът поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на тази наредба.

(4) Информацията по ал. 3:

1. се поддържа в актуално състояние;

2. е достъпна само за:

а) тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови, служебни или договорни отношения;

б) представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;

в) други организации, оправомощени с нормативен акт или договорни отношения.

Класификация на информацията

Чл. 6. (1) Субектът приема вътрешни правила по смисъла на чл. 5, ал. 1, т. 6 и 7 за класификация на информацията, които указват как да се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага организацията. Препоръчителна класификация е дадена в приложение № 2.

(2) Правилата по ал. 1 гарантират достатъчна, адекватна и пропорционална на заплахите защита на информацията с оглед на нейната важност, чувствителност и на нормативните изисквания към нея.

(3) Класификацията по ал. 1 се прилага и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията, като към тях трябва да се прилагат подходящи механизми за защита, съответстващи на идентифицираните от Субекта заплахи.

(4) Нивото на класификацията трябва да е подходящо нанесено върху документираната информация.

(5) За класификацията по ал. 1 не се допуска използването на нивата на класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация, както и техният гриф.

(6) Информацията без класификация е достъпна за общо ползване при спазване на стандартните правила за авторски права и към нея не се прилагат механизми за защита.

(7) При обмен на информация се използва класификация TLP (traffic light protocol) съгласно приложение № 2.

Управление на риска

Чл. 7. (1) Субектът извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите, влизащи в обхвата на тази наредба.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т. 6, в който са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса.

(3) Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от административния орган, съответно от ръководителя на субекта по чл. 1, ал. 1, т. 2 – 5, и е достъпна за лицата, на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3.

(4) На основание на анализа и оценката на риска Субектът изготвя план за

намаляване на неприемливите рискове, който да включва минимум:

1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

Управление на информационните активи

Чл. 8. (1) Субектът приема вътрешни правила по смисъла на чл. 5, ал. 1, т. 6, регламентиращи процеса на управление на жизнения цикъл на информационните и комуникационните системи и техните компоненти. Вътрешните правила трябва еднозначно да указват условията, начина и реда за придобиване, въвеждане в експлоатация, поддръжка, преместване/изнасяне, извеждане от експлоатация и унищожаване на информационни и комуникационни системи и техните компоненти.

(2) Описът на информационните активи по смисъла на чл. 5, ал. 1, т. 1 съдържа информация, необходима за разрешаването на инциденти, анализ и оценка на риска, управление на уязвимости и управление на измененията, като:

1. еднозначна идентификация, като инвентарен, сериен номер или др.;
2. основни характеристики;
3. услуги, процеси и дейности, в които участва;
4. местоположение;
5. година на производство, където е приложимо;
6. дата на въвеждане в експлоатация, където е приложимо;
7. версия, където е приложимо;
8. местонахождение на свързаната с него документация (техническа, експлоатационна, потребителска и др.);
9. отговорно лице.

Сигурност на човешките ресурси

Чл. 9. (1) За намаляване на риска от инциденти, умишлено или неумишлено предизвикани от служители, Субектът гарантира чрез вътрешни правила и инструкции, че служителите, имащи отношение към процесите и дейностите в обхвата на наредбата, имат подходящата квалификация, знания и умения за изпълнение на отговорностите си.

(2) Вътрешните правила по ал. 1 регламентират:

1. процеса за наемане на работа в съответствие с приложимите закони и подзаконови нормативни актове, професионалната етика и съобразно изискванията, свързани с дейността им – класификацията на информацията, до която имат достъп, и предполагаемите рискове;
2. отговорностите и задълженията по отношение на сигурността на информацията при прекратяване или промяна на служебните/договорните отношения;
3. дисциплинарен процес за лицата по ал. 1, които са извършили нарушение по отношение на политиката и вътрешните правила за мрежова и информационна сигурност.

(3) Отговорностите на лицата по ал. 1 по отношение на сигурността на информацията се документират с ясно определени срокове и задължения.

(4) Субектът обезпечава нивото на мрежова и информационна сигурност посредством:

1. подходящо професионално обучение за повишаване на квалификацията на служителите в съответствие с използваната техника и технологии;
2. периодично инструктиране на служителите за повишаване на вниманието им по отношение на мрежовата и информационната сигурност; инструктажът се прави по утвърден график и се документира по начин, гарантиращ проследяемост.

Управление на взаимодействията с трети страни

Чл. 10. (1) При установяване на взаимоотношения с доставчици на стоки и услуги, наречени "трети страни", Субектът трябва да договори изисквания за мрежова и информационна сигурност, включително:

1. за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активи на Субекта;

2. за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;

3. за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;

4. последици при неспазване на изискванията за сигурност на информацията;

5. отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност;

6. за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент.

(2) Субектът определя служител/служители, отговарящ/отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

(3) Субектът изготвя план за действие в случай на неспазване на уговорените дейности и клаузи с третата страна.

Управление на измененията в информационните активи

Чл. 11. (1) Субектът приема вътрешни правила за управление на измененията във важните за дейността му информационни активи в съответствие с изискването на чл. 5, ал. 1, т. 6 с цел намаляване на риска от инциденти, настъпили в резултат на изменения във важните за дейността му информационни активи, и по-точно в информационните и комуникационните системи и обслужващата ги инфраструктура, в процесите и дейностите, в конфигурациите, в софтуера или във фърмуера.

(2) Преди да се извърши изменението, Субектът трябва да направи анализ и оценка на риска в съответствие с чл. 7.

(3) Измененията се:

1. планират, като се определят срокове и отговорности за всяка дейност, която ще бъде извършена преди, по време на и след изменението;

2. съгласуват предварително с всички страни, имащи отговорности към процесите и дейностите в обхвата на наредбата;

3. одобряват от административния орган, съответно от ръководителя на субекта по чл. 1, ал. 1, т. 2 – 5, или от упълномощено от него лице;

4. оповестяват по подходящ начин на всички страни, които са заинтересовани; информирането на заинтересованите страни трябва да е поне 3 дни преди да се направи изменението;

5. проверяват в тестова среда.

(4) Субектът разработва план за връщане на системите в предишното им състояние, за да се намали продължителността на потенциален инцидент, настъпил в резултат на изменението.

Сигурност при разработване и придобиване на информационни и комуникационни системи

Чл. 12. (1) При разработване на проекти и технически задания Субектът включва адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното

ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.

(2) Субектът въвежда в експлоатация нови информационни и комуникационни системи планирано и след успешно проведени и документирани тестове, доказващи защитата на информацията от загуба на достъпност, интегритет и конфиденциалност.

Раздел II
Защита

Сегрегация

Чл. 13. (1) Субектът поддържа информационна и комуникационна инфраструктура, която гарантира, че информационните и комуникационните системи, изпълняващи различни функции, са разделени и изолирани помежду си физически и/или логически, както и че са разделени и изолирани от информационните и комуникационните системи на трети страни, с цел да се ограничи разпространението на инциденти с мрежовата и информационната сигурност.

(2) В случай че дадена система е съставена от подсистеми, разделянето им трябва да се осъществи на последно физическо или логическо ниво, като уеб сървърът, сървърът с приложния софтуер и сървърът с базата данни на една информационна система трябва да са разположени на различни машини и в различни мрежи.

Филтриране на трафика

Чл. 14. (1) Субектът гарантира, че трафикът между отделните системи и техните подсистеми е контролиран чрез подходящо филтриране (по IP адрес, по протокол, по номер на порт от Transmission Control Protocol (TCP)/Internet Protocol (IP) стека и т. н.) с цел превенция на евентуални атаки и ограничаване на разпространението на инциденти. Филтрирането на трафика трябва да бъде по предварително разписани и одобрени правила, основаващи се на функционалността и сигурността, които трябва да бъдат редовно проверявани за нерегламентирани изменения и да бъдат актуализирани с оглед на нововъзникващи заплахи.

(2) Ненужните портове по протоколи TCP и User Datagram Protocol (UDP трябва да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.

Неоторизирано използване на устройства

Чл. 15. (1) Субектът приема ясно дефинирани политики относно използването на:

1. лични технически средства в мрежата, която контролират;
2. преносими записващи устройства.

(2) Политиките се отразяват във вътрешните правила, като се предприемат подходящи и реципрочни на заплахите мерки за реализирането им.

Криптография

Чл. 16. (1) Субектът разработва политика и вътрешни правила съгласно чл. 5, ал. 1, т. 6 за прилагане на криптографски механизми, които се използват за гарантиране на конфиденциалността и интегритета на чувствителната информация в съответствие с нейната класификация.

(2) Криптографските механизми се съобразяват с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритет и с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.

Администриране на информационните и комуникационните системи

Чл. 17. (1) Субектът прилага следните мерки за защита на профилите с административни права за информационните и комуникационните системи и техните компоненти:

1. преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на информационния актив;

2. администраторските профили са персонални;

3. администраторските профили се използват само за административни цели;

4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);

5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;

6. данните за автентикацията на администраторските акаунти:

а) са различни за всяка система;

б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;

в) се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран представител на Субекта;

7. поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти;

8. при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини правата на административния му акаунт се спират за съответния период;

9. поне веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.

(2) Паролите за автентикация на администраторските профили се сменят задължително:

1. периодично – най-малко веднъж в годината;

2. при прекратяването на договорните отношения със служители или трети страни, на които тези данни са били известни;

3. при пробив в мрежовата и информационната сигурност.

(3) Всички операции, процеси и дейности в информационните и комуникационните системи и техните компоненти, извършени с администраторски права, се документират по смисъла на чл. 5, ал. 3 и 4 за всеки администраторски профил и в съответствие с изискванията на чл. 29, ал. 2, 4, 5 и 6.

(4) В документацията по ал. 3 не се въвеждат и не се съхраняват пароли на административен профил под формата на явен текст или хеш.

Среда за администриране

Чл. 18. (1) Субектът използва отделна, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда трябва да е изолирана от другите информационни и комуникационни системи на Субекта и от интернет и да не се използва за други цели.

(2) В случай че администрирането на информационните и комуникационните системи и техните компоненти не се осъществява през средата по ал. 1, потоците на тази информация трябва да са защитени чрез механизми за удостоверяване и криптиране.

Управление на достъпите

Чл. 19. Субектът е длъжен да дава достъп до информационните и комуникационните си системи на потребител или автоматизиран процес само когато този достъп е строго необходим на потребителя, за да изпълни задълженията си, или на автоматизирания процес да извърши необходимите технически операции. За да гарантира, че достъп до информационните и комуникационните му системи имат само оторизирани потребители, устройства (включително други информационни системи) и автоматизирани процеси, Субектът:

1. във вътрешните си правила по смисъла на чл. 5, ал. 1, т. 6 определя:

а) правата на достъп до конкретни информационни активи на служителите според длъжността им;

б) реда за заявяване, промяна и прекратяване на достъп;

2. прилага задължителни мерки за автентикация, оторизация и одит на компютърните мрежи и системи, които включват и изисквания за определена сложност на данните за автентикация; ако се използват пароли:

а) те следва да съдържат малки и големи букви, цифри и специални символи;

б) дължината им трябва да е не по-малко от 8 символа за потребителските и 12 символа за администраторските профили;

в) паролите на потребителските акаунти трябва да се сменят регулярно на период не по-голям от шест месеца;

3. гарантира, че потребителските профили са индивидуални; в ежедневната работа трябва да се използват профили с най-ниското ниво на достъп, което дава възможност за изпълнение на служебните задължения;

4. гарантира, че лицата, имащи право да заявяват даване, променяне и спиране на достъп, определени във вътрешните правила по т. 1, буква "б", правят редовни прегледи на достъпите, но не по-рядко от веднъж в годината; при тези прегледи се установява дали всички, на които е даден достъп до мрежата, до отделните системи и/или приложения, имат право на него в съответствие със служебните им задължения, дали външни лица имат достъп и какъв е той (бивши служители, представители на трети страни); за целите на прегледите администраторите на съответните информационни и комуникационни системи предоставят на оправомощените във вътрешните правила по т. 1, буква "б" лица списък на всички, които имат достъп до системата и нивото на достъпа, а оправомощените лица документирано потвърждават или дават указания за промяна;

5. ограничава даването на привилегирован достъп (по-високо ниво на достъп или достъп до система, до която лицето не трябва да има достъп в съответствие с вътрешните правила по ал. 1); привилегированият достъп трябва да се дава само за определен период и да се контролират действията с него;

6. гарантира, че достъпът до споделени файлове и принтери е разрешен само от мрежата, контролирана от Субекта.

Защита при отдалечен достъп/работа от разстояние

Чл. 20. При необходимост от достъп до информационни активи извън мрежата, контролирана от Субекта, се спазват изискванията на чл. 19, включително:

1. се използва най-малко двуфакторна автентикация;

2. се използват само канали с висока степен на защита като Virtual Private Network (VPN);

3. не се използват File Transfer Protocol (FTP) и Remote Desktop Connection.

Защита на хардуерни устройства

Чл. 21. (1) За намаляване на риска от инциденти, предизвикани от технически повреди, Субектът:

1. осигурява климатико-механичните условия, указани от производителя;

2. осъществява наблюдение на параметрите на условията по т. 1;

3. провежда планирана регулярна техническа профилактика на устройствата в съответствие с политиката му за жизнения им цикъл.

(2) За намаляване на риска от неоторизиран достъп Субектът е длъжен да разполага устройствата в зони, които са физически и логически защитени в съответствие с класификацията на информацията, с която работят.

Защита на софтуер и фърмуер

Чл. 22. (1) Субектът инсталира и поддържа само версии на използвания в системите му софтуер и фърмуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността.

(2) Административният орган, съответно ръководителят на субекта по чл. 1, ал. 1, т. 2 – 5, одобрява софтуера, който се използва в информационните и комуникационните системи.

(3) Субектът поддържа библиотека с дистрибутиви на използвания софтуер и фърмуер с цел намаляване на времето за възстановяване на дадена система след срив.

(4) Субектът предприема мерки за:

1. недопускане на инсталирането и използването на неодобрен софтуер и фърмуер;

2. контрол върху използвания софтуер и фърмуер, включително неговата актуалност.

(5) Субектът приема вътрешни правила и инструкции за регламентиране на действията по:

1. поддържане на библиотеката с дистрибутиви на използвания софтуер и фърмуер в актуално състояние;

2. управлението на достъпа до нея;

3. проследяване за новооткрити уязвимости в сигурността на използвания в системите му софтуер и фърмуер и за техни актуализации (нови версии, ъпдейти и пачове), които отстраняват тези уязвимости, или мерки за смекчаването им, публикувани от производителите или доставчиците;

4. придобиване и проверка на произхода и целостта на актуализацията преди инсталирането ѝ;

5. прилагането на актуализациите и препоръчаните мерки, които трябва да се извършват съобразно разпоредбите на чл. 11.

(6) Субектът гарантира, че устройствата и системите са конфигурирани в съответствие с препоръките за сигурност на съответния им доставчик или производител, като се приложат и изискванията на приложение № 4.

(7) Субектът съхранява off-line копие от актуалните конфигурационни файлове и/или описание на настройките, като достъпът до тях трябва да е контролиран. Копията трябва да се проверяват регулярно относно качество и годност.

(8) Субектът регулярно прави проверка на конфигурационните файлове и настройките на системи и устройства за нерегламентирани изменения.

Защита от зловреден софтуер

Чл. 23. (1) Субектът прилага в информационната и комуникационната си инфраструктура подходящи мерки за защита от проникване и мерки за откриване и справяне със зловреден софтуер.

(2) Мерките за защита от зловреден софтуер трябва:

1. да са приложени към всички компоненти на информационните и комуникационните системи, където това е възможно;

2. да се поддържат в актуално състояние, за да имат способността да защитават от новооткрити заплахи.

(3) Мерките за защита от зловреден софтуер трябва да позволяват:

1. извършване на пълна проверка за наличие на зловреден софтуер поне веднъж в седмицата, където е приложимо;

2. проверка на електронната поща и файлове, свалени от интернет, както и преносими записващи устройства, преди да бъдат отворени.

(4) Субектът извършва регулярно оценка на ефективността на мерките за защита от зловреден софтуер и при констатирани слабости предприема действия за подобряване на защитата.

Защита на уеб сървъри

Чл. 24. (1) Субектът предприема следните мерки за защита на уеб сървърите:

1. инсталира сертификат на уеб сървърите си, издаден от доверена система за сертифициране (trusted certification authority system); сертификатът трябва:

а) да е издаден за съответния уеб сайт (website) или група сайтове и да е уникален;

б) да използва алгоритъм за криптиране поне SHA2;

в) да е актуален, като сертификатите с изтекъл срок се анулират;

2. за защита на интегритета на информацията, обменяна с потребителите, уеб сайтът (website) трябва да е достъпен само по протокол Hypertext Transfer Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г. или следващи по-нови версии;

3. за криптиране на информацията, обменяна между уеб сървъра и потребителите му, се прилагат изискванията на чл. 16 и като се вземат предвид публикуваните в RFC на IETF забрани за използване на методи за шифриране в криптографските транспортни протоколи;

4. да се приложи подходящ Web Application Firewall (WAP), който наблюдава и филтрира трафика от и към съответното приложение с цел защита на уеб приложенията от кибератаки от типа Cross-Site Request Forgery (CSRF), Cross site Scripting (XSS), file inclusion, SQL injection и др.;

5. да не се позволява вмъкване на данни от страна на потребителя, освен на определените за това места;

6. всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headers на препращащия и потребителски агент, трябва да бъдат валидирани;

7. приложния софтуер да не позволява въвеждане на специални символи, особено такива, които се използват в SQL заявките;

8. всички данни, изпращани от клиента и показвани в уеб страница, трябва да бъдат кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript;

9. за защита от атаки от типа отказ от услуги (DoS):

а) да се наложи ограничение на заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по Url;

б) да се конфигурират типът и размерът на headers, които уеб сървърът ще приеме;

в) да се ограничат времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки;

10. за защита от brute force атаки да се въведе ограничение на броя неуспешни опити за влизане в системата;

11. да не се извежда списък на уеб директориите;

12. бисквитките (cookies) трябва да имат:

а) флаг за защита (security flag) – този флаг инструктира браузъра, че "бисквитката" може да бъде достъпна само чрез защитени SSL канали;

б) флаг HTTP only – инструктира браузъра, че "бисквитката" може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;

13. headers на отговорите на заявки, които трябва да гарантират защита както на клиента, така и на уеб сайта (website), като съдържат опции, посочени в приложение № 5;

14. в главната директория на уеб сайта (website) да се сложи файл robot.txt, който дава указания на уеб роботите (ботове/паяци) колко често да обхождат сайта, както и кои части от него да обхождат и да индексират; ако този файл не съществува, уеб роботите обхождат целия сайт – всяка една негова страница, подстраница, статия, линк и т.н., което крие риск за конфиденциалността на информацията;

15. при използване на Система за управление на съдържанието (CMS) да се промени наименованието по подразбиране на папката за достъп до администраторския панел.

Защита на Domain Name System (DNS)

Чл. 25. Субектът трябва да предприеме следните мерки за защита на DNS:

1. при използване на повече от един DNS сървър, всеки от тях да е разположен в различна мрежа/подмрежа;

2. да прилага DNSSEC (Domain Name System Security Extensions);

3. да минимизира DNS заявките съгласно RFC 7816 на IETF от 2016 г.;

4. да забрани zone-transfers – злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация;

5. в конфигурационния файл да сложи:

а) dmarc (Domain-based Message Authentication, Reporting and Conformance) запис;

б) SPF (Sender Policy Framework) запис.

Физическа сигурност

Чл. 26. (1) Субектът осигурява физическа защита на информационните си активи чрез прилагане на адекватни и пропорционални мерки срещу заплахи от неоторизиран физически достъп до тях. Мерките трябва да гарантират наличността, интегритета и конфиденциалността на информационните активи.

(2) Субектът осигурява защита на информационните си активи от пожар, наводнение, химическа и физическа промяна на въздуха чрез подходящи мерки в съответствие с нормативните актове.

(3) За да гарантира ефикасността на приложените мерки по ал. 1 и 2, Субектът извършва подходящо наблюдение върху тях.

Защита на индустриални системи за контрол

Чл. 27. В случай че Субектът използва индустриални системи за контрол, от функционирането и сигурността на които зависят съществените услуги, които предоставя, той е задължен да приложи подходящи мерки за тяхната защита в съответствие с изискванията на наредбата, ако са приложими.

Наблюдение

Чл. 28. (1) Субектът използва система/системи за автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността му системи, чрез анализ на информационни потоци, протоколи и файлове, преминаващи през ключови устройства, позиционирани така, че да могат да анализират всички потоци, обменяни между собствените им

информационни и комуникационни системи, както и с информационните и комуникационните системи на трети страни.

(2) Субектът организира чрез вътрешни правила и/или инструкции действията за наблюдение и реакция на сигналите от тази/тези система/системи.

Системни записи (logs)

Чл. 29. По отношение на системните записи Субектът гарантира, че:

1. в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;

2. в записите за всяко от тези събития е отбелязано астрономическото време, когато е настъпило събитието;

3. всички компоненти на системите поддържат единно време в съответствие с изискванията на:

а) стандарти БДС ISO 8601-1 "Дата и време. Представяния за обмен на информация. Част 1: Основни правила" и БДС ISO 8601-2 "Дата и време Представяния за обмен на информация. Част 2: Разширения"; времето за настъпването на събития с правно или техническо значение се отчита с точност до година, дата, час, минута и секунда, а при технологична необходимост се допуска и отчитане до милисекунда;

б) за синхронизация на часовниците на компоненти на информационните и комуникационните системи трябва да се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;

4. достъпът до информацията по ал. 1 е ограничен само до лица, имащи задължения за наблюдението по смисъла на чл. 30, за разрешаването на инциденти с мрежовата и информационната сигурност, за разкриването и разследването на тежки престъпления и престъпления по чл. 319а – 319е от Наказателния кодекс в съответствие с чл. 14, ал. 4, т. 2 и чл. 15, ал. 3, т. 3 от Закона за киберсигурност; достъпът до тази информация трябва да е само за четене;

5. информацията по ал. 1 се архивира и се съхранява за период не по-малък от дванадесет месеца при спазване на изискванията на чл. 32;

6. Субектът трябва да е в състояние да извършва корелация на информацията по ал. 1 от различните източници и да правят анализ, за да открият събития, които засягат мрежовата и информационната сигурност.

Управление на инциденти с мрежовата и информационната сигурност

Чл. 30. (1) Във вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 се регламентират всички дейности при обработката на сигнали и реакция при инциденти.

(2) Вътрешните правила по ал. 1 съдържат:

1. реда за подаване на сигнали за настъпили или потенциални събития, оказващи негативно влияние върху мрежовата и информационната сигурност;

2. информация за лицата, отговорни за регистъра на инцидентите;

3. реда за регистриране на сигнала, проверката на неговата достоверност, класифицирането му, приоритизирането му и последващото уведомяване за това на подателя;

4. реда за уведомяване за инцидента (функционална и йерархична ескалация);

5. реда за подаване на информация за начина за разрешаване на инцидента;

6. реда за приключване на инцидента;

7. процеса за събиране, съхраняване и предаване на доказателства, когато инцидентът предполага извършването на процесуални действия срещу лице или организация, включително необходимите за това записи;

8. правата на достъп до регистъра на инцидентите.

(3) Субектът разработва, проверява и поддържа в актуално състояние планове за справяне с инцидентите, които биха имали най-сериозно въздействие върху мрежовата и информационната сигурност. Плановете съдържат информация за:

1. отговорника за организацията при настъпване на инцидент;

2. реда за информиране;

3. мерките, които следва да се предприемат и отговорното за това лице;

4. реда за консултиране;

5. реда за следене на параметрите по време на инцидента;

6. лицето, което ще събира и съхранява необходимата информация, и др.

(4) Субектът разработва стратегия за комуникация, която определя реда за споделяне на информацията за инцидента със служители, партньори, доставчици, клиенти, медии, държавни органи.

Уведомяване за инциденти

Чл. 31. (1) При инцидент с мрежовата и информационната сигурност служителят или административното звено, отговарящо за мрежовата и информационната сигурност по смисъла на чл. 3, ал. 2, уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите в сроковете, посочени в чл. 21, ал. 4 и 5 и чл. 22 от Закона за киберсигурност.

(2) За уведомяването по ал. 1 и по чл. 17, ал. 7 от Закона за киберсигурност се използва формата, посочена в приложение № 7.

(3) При изпълняване на изискването на чл. 17, ал. 8 от Закона за киберсигурност секторните екипи за реагиране при инциденти с компютърната сигурност изпращат обобщената статистическа информация за инциденти към националния екип за реагиране при инциденти с компютърната сигурност, като използват формата, посочена в приложение № 8.

(4) В случай че информацията по ал. 2 и 3 се изпраща по електронна поща, тя трябва да е подходящо защитена от неоторизиран достъп и да е класифицирана съгласно чл. 6, ал. 7.

Раздел III
Устойчивост

Резервиране и архивиране на информация

Чл. 32. (1) Вътрешните правила/инструкции по смисъла на чл. 5, ал. 1, т. 6 се разработват в съответствие с целите и стратегическите насоки, определени в политиката за мрежова и информационна сигурност относно защита на интегритета на информацията в случай на инцидент, засягащ нейната достъпност.

(2) Вътрешните правила/инструкции по ал. 1 регламентират процесите, свързаните с тях дейности и отговорностите по резервиране и архивиране на информация, като в съдържанието им се включва най-малко:

1. информацията (бази данни, конфигурационни файлове, имиджи на системи и др.), която ще се резервира и/или архивира;

2. технологията, която ще се използва за архивиране и резервиране;

3. типът на резервиране (частично, пълно и др.);

4. периодът на извършване на архивирането и резервирането;

5. броят на копията, които ще се правят;

6. времето за съхраняване на всяко копие съгласно изискванията на нормативните актове и оценката на риска;

7. мястото на съхраняване на всяко копие;

8. начинът на защита от неправомерен достъп (физическа и логическа);

9. случаите на използване;

10. лицето, което дава разрешение за използването.

(3) Всички изисквания по ал. 2 се определят от собственика на информацията или с неговото одобрение и трябва да бъдат съобразени с времето, за което тя трябва да се възстанови, за да се гарантира необходимото ниво на наличност на услугата.

(4) При резервирането и/или архивирането на информацията се спазват следните изисквания:

1. да се правят регулярни копия съобразно риска от загуба на информация и динамиката на изменението ѝ;

2. копията на информация да са етикетирани по начин, указващ еднозначно поне каква е информацията, за коя система, какъв метод е използван за създаване на копието, дата и час;

3. копията на чувствителна информация да са в криптиран вид или поне защитени с парола;

4. копията на информацията да се съхраняват на отделна машина и по възможност в друга защитена мрежа;

5. едно от копията на критична за дейността информация се съхранява off-line и по възможност в друга сграда или на отдалечено място;

6. да се прави регулярна проверка на годността на резервните копия, дали те изпълняват целите, за които са създадени, и постига ли се необходимото време за възстановяване.

Резервиране на компоненти на инфраструктурата

Чл. 33. Субектът предприема подходящи и в съответствие с рисковете мерки за гарантиране на нивото на услугите и дейностите, които са в обхвата на наредбата, като:

1. резервиране на системи;

2. резервиране на устройства;

3. балансиране на натоварването на критични устройства или системи;

4. резервиране на центрове за данни.

Планове за непрекъсваемост

Чл. 34. (1) Субектът разработва планове за действия в случай на аварии, природни бедствия или други непредвидени обстоятелства, които биха причинили прекъсване на предоставяната от него услуга в съответствие с изискванията на чл. 5, ал. 1, т. 6.

(2) Плановете по ал. 1 съдържат:

1. обстоятелствата, за които се отнасят;

2. праговете, при които се задействат;

3. лицето, което дава разрешение за задействането им;

4. реда за възстановяване на услугите и дейностите до определено ниво.

(3) Плановете по ал. 1:

1. се проиграват периодично, но не по-рядко от веднъж в годината, с цел да се провери тяхната актуалност и да се тренират лицата, които имат отговорности за изпълнението им;

2. се поддържат в актуално състояние;

3. са достъпни само за лицата, които имат отговорности за тяхното изпълнение;

4. се съхраняват най-малко на две места, едно от които е извън сградата, в

която се намират системите, за които се отнасят.

Глава трета
КОНТРОЛ

Одити

Чл. 35. (1) Контролът за спазване на изискванията на глава втора и приетите стандарти се осъществява чрез:

1. вътрешни одити (от първа страна), които са организирани от Субекта и се извършват от негови служители или от трета страна, но от негово име;

2. външни одити от втора страна, които са организирани от клиенти или доставчици на Субекта;

3. външни одити от трета страна, провеждани от независими организации за одит, като контролни органи на изпълнителната власт или организации, имащи право да извършват акредитация или сертификация.

(2) Одитите по ал. 1, т. 2 и 3 са препоръчителни мерки.

(3) Одитите по ал. 1, т. 1 се извършват в съответствие със стандарт БДС EN ISO 19011 "Указания за извършване на одит на системи за управление", изискванията на стандарт БДС EN ISO/IEC 17020 "Оценяване на съответствието" като се спазва най-малко следното:

1. одитите се провеждат периодично, но не по-рядко от веднъж в годината;

2. одитите се провеждат по документирани и одобрени процедури, годишни програми и планове, които са оповестени на лицата, отговарящи за одитираната област;

3. одитите се извършват от лица, притежаващи квалификация в областта на контрола и имащи необходимите знания и професионален опит в областта на мрежовата и информационната сигурност;

4. одиторът спазва принципите за почтеност, безпристрастност, професионализъм, независимост и конфиденциалност;

5. одиторът не може да одитира собствената си дейност;

6. резултатите от одита се документират и за тях се информира служителят, отговарящ за одитираната област;

7. при несъответствие с изискванията подробно се документира изискването и констатираното състояние и се посочва срок за отстраняването му;

8. резултатите от одита са с класификация TLP-AMBER.

(4) Субектът предоставя резултатите от одитите на съответния национален компетентен орган съгласно чл. 16, ал. 5 от Закона за киберсигурност.

Проверки

Чл. 36. (1) Проверките за съответствие с изискванията на глава втора, осъществявани от председателя на Държавна агенция "Електронно управление" съгласно чл. 12, т. 6 от Закона за киберсигурност, се извършват съобразно стандарт БДС EN ISO 19011 "Указания за извършване на одит на системи за управление" и изискванията на стандарт БДС EN ISO/IEC 17020 "Оценяване на съответствието".

(2) Проверките се провеждат по документирани и утвърдени от председателя на Държавна агенция "Електронно управление" вътрешни правила.

(3) Проверките се извършват по годишна програма, одобрена от председателя на Държавна агенция "Електронно управление", която се публикува на страницата на агенцията до края на предходната година.

(4) Проверки извън одобрената годишна програма се извършват по искане на правоимащ орган, както и по заявка на Субекта, като последните се осъществяват само при наличие на свободен ресурс на оправомощените от председателя на Държавна агенция "Електронно управление" лица.

(5) За всяка проверка оправомощените лица създават план, с който се запознава административният орган или съответно ръководителят на Субекта по чл. 1, ал. 1, т. 2 – 5 – обект на проверката.

(6) Времето за извършване на проверката се съгласува с административен орган или съответно с ръководителя на одитирания Субект по чл. 1, ал. 1, т. 2 – 5 – обект на проверката, не по-късно от седем дни преди началото на проверката.

(7) Оправомощените от председателя на Държавна агенция "Електронно управление" лица трябва да притежават квалификация в областта на контрола и да имат необходимите знания и професионален опит в областта на мрежовата и информационната сигурност.

(8) Оправомощените лица спазват принципите за почтеност, безпристрастност, професионализъм, независимост и конфиденциалност.

(9) Оправомощените лица изготвят доклад с резултатите от проверката в срок не по-късно от 10 дни след приключването на проверката. Докладът се класифицира с TLP-AMBER.

(10) В доклада по ал. 9 се посочва и оценката, получена в съответствие с методиката за извършване на оценка на мрежовата и информационната сигурност, приета от председателя на Държавна агенция "Електронно управление" съгласно чл. 12, т. 7 от Закона за киберсигурност.

(11) В случай на констатирано несъответствие с изискванията в доклада подробно се документира изискването и констатираното състояние, срок за отстраняването му и ако е необходимо, препоръки как да бъде отстранено.

(12) В доклада по ал. 9 може да бъдат включени и препоръки за подобряване на нивото на мрежовата и информационната сигурност.

(13) Председателят на Държавна агенция "Електронно управление" или упълномощено от него лице изпраща доклада по ал. 9 на административния орган, съответно на ръководителя на Субекта, където е направена проверката.

(14) Председателят на Държавна агенция "Електронно управление" или упълномощено от него лице планира действия за последващ контрол за отстраняване на констатираните несъответствия и информира за тях ръководителя на одитираното лице по чл. 1, ал. 1.

Анкети

Чл. 37. (1) За целите на чл. 16, ал. 3, т. 3 от Закона за киберсигурност националните компетентни органи използват и анкети.

(2) Анкетите се отнасят до обхвата на тази наредба, посочен в чл. 1, ал. 2.

(3) В анкетите може да се иска информация относно всички изисквания, посочени в глава втора, отделни раздели от нея или отделни членове, независимо в кой раздел са.

(4) Попълнените анкети са с класификация TLP-AMBER.

Глава четвърта
РЕГИСТЪР НА СЪЩЕСТВЕНИТЕ УСЛУГИ

Идентифициране на съществените услуги и на операторите на съществени услуги

Чл. 38. (1) Административните органи, определени с решение на Министерския съвет съгласно чл. 16, ал. 1 от Закона за киберсигурност, идентифицират и регистрират съществените услуги в съответните сектори и подсектори и операторите, които ги предоставят.

(2) За целите на ал. 1 административните органи прилагат методиката, приета с решение на Министерския съвет.

(3) Административните органи по ал. 1 регулярно, но не по-малко от веднъж на две години, правят преглед на:

1. адекватността на специфичните за съответния сектор критерии и

евентуални прагове за определяне на съществените услуги, дефинирани в методиката по ал. 2;

2. съществените услуги в съответните сектори и подсектори и операторите, които ги предоставят.

Класификация на информацията в регистъра на съществените услуги

Чл. 39. Информацията, събрана по чл. 38, е с класификация TLP-RED.

Поддръжка на информацията в регистъра на съществените услуги

Чл. 40. (1) Административните органи по чл. 38, ал. 1 предават на председателя на Държавна агенция "Електронно управление" информацията за съществените услуги в съответните сектори и подсектори и за операторите, които ги предоставят, посочена в чл. 6, ал. 1 от Закона за киберсигурност, и информацията, събрана в резултат на изпълнение на чл. 38, ал. 2 по защитени комуникационни канали.

(2) Министърът на транспорта, информационните технологии и съобщенията предава по защитени комуникационни канали на председателя на Държавна агенция "Електронно управление" информацията за всички цифрови услуги съгласно рецитал 57 от 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 194/1 от 19 юли 2016 г.), разпределени по видове съгласно приложение № 2 към чл. 4, ал. 1, т. 2 към Закона за киберсигурност, и за доставчиците, които ги предоставят.

Администриране

Чл. 41. Оправомощени от председателя на Държавна агенция "Електронно управление" служители администрират регистър на съществените услуги и въвеждат информацията, получена по чл. 38.

Защита на регистъра на съществените услуги

Чл. 42. Към регистъра на съществените услуги се прилагат адекватните и приложими минимални мерки за мрежова и информационна сигурност, посочени в глава втора, раздел II с уточненията, посочени в чл. 19, и раздел III.

Управление на достъпа до регистъра на съществените услуги

Чл. 43. (1) Достъп до регистъра на съществените услуги имат упълномощени представители на:

1. Националния екип за реагиране при инциденти с компютърната сигурност по смисъла на чл. 19, ал. 1 от Закона за киберсигурност за изпълнение на функциите му по чл. 19, ал. 2, т. 1 и 10, като достъпът е до цялата информация и дава право само за четене;

2. секторните екипи за реагиране на инциденти с компютърната сигурност по смисъла на чл. 18, ал. 1 от Закона за киберсигурност за изпълнение на функциите му по чл. 18, ал. 3 и 7 от Закона за киберсигурност, като достъпът е само до информацията за съответния сектор и дава право само за четене;

3. Националното единно звено за контакт по смисъла на чл. 17, ал. 1 от Закона за киберсигурност за изпълнение на функциите му по чл. 17, ал. 2, 3, 4 и 7 от Закона за киберсигурност, като достъпът е до цялата информация и дава право само за четене;

4. националните компетентни органи по смисъла на чл. 16, ал. 1 от Закона за киберсигурност за изпълнение на функциите им по чл. 16, ал. 11 от Закона за киберсигурност, като достъпът е само до информацията за съответния сектор и дава право на четене и редактиране само до полета "лице за контакт" и "контактни точки".

(2) Достъпът до регистъра е индивидуален, като за целта административните органи по чл. 38, ал. 1 подават списък на упълномощените

служители, които изпълняват функции в съответния национален компетентен орган и секторен екип за реагиране при инциденти с компютърната сигурност.

(3) При промяна или прекратяване на служебните правоотношения административният орган по чл. 38, ал. 1 информира писмено в рамките на един работен ден председателя на Държавна агенция "Електронно управление" или упълномощено от него лице за настъпилите промени за коригиране на достъпа до регистъра на съществените услуги.

(4) Достъп до регистъра се дава след одобрение от председателя на Държавна агенция "Електронно управление" или упълномощено от него лице.

(5) Служителите по чл. 41, които администрират регистъра на съществените услуги, най-малко веднъж в годината инициират преглед на правата за достъп по смисъла на чл. 19, т. 4.

(6) За достъп до регистъра се използва поне двуфакторна автентикация.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. Наредбата е съобразена със:

1. Групата стандарти БДС (EN) ISO/IEC 2700x – Информационни технологии – Методи за сигурност – Системи за управление на сигурността на информацията.

2. Други международни стандарти в областта на информационните технологии и сигурността на информацията, посочени в приложение № 1.

3. Препоръките на Групата за сътрудничество по мрежова и информационна сигурност към Европейската комисия от февруари 2018 г. относно мерките за сигурност за операторите на основни услуги.

4. Добри практики в областта на информационните и комуникационните технологии, препоръчани от водещи в областта на мрежовата и информационната сигурност организации.

§ 2. По смисъла на наредбата:

1. DNSSEC (Domain Name System Security Extensions) е набор от разширения към DNS системата, чрез които се добавя начин за верифициране на автентичността на публикуваната DNS информация за даден домейн. Чрез DNSSEC се удостоверява истинността на DNS информацията за даден домейн, като по този начин индиректно се защитава автентичността на всички услуги от този домейн, а също и потребителите на тези услуги.

2. Dmark (Domain-based Message Authentication, Reporting and Conformance) – запис, указващ политиките за валидиране, разпространение и отчетност на електронната поща в рамките на домейна, съгласно RFC 7489 на IETF.

3. SPF (Sender Policy Framework) – запис, указващ метода за удостоверяване на електронна поща, съгласно RFC 7208 на IETF от 2014 г. Записът трябва да бъде във формат DNS TXT (type 16) Resource Record (RR) съгласно RFC 1035 на IETF.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 3. В срок 4 месеца от влизането в сила на наредбата субектите по чл. 1, ал. 1 привеждат дейността си в съответствие с глава втора.

§ 4. Наредбата се приема на основание чл. 3, ал. 2 от Закона за киберсигурност.

Приложение № 1 към чл. 2, ал. 4

СПИСЪК НА СТАНДАРТИ В ОБЛАСТТА НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

Стандарти за управление на сигурността на информацията

БДС EN ISO/IEC 27000 – Информационни технологии – Методи за сигурност – ***Системи за управление на сигурността на информацията – Общ преглед и речник***

БДС EN ISO/IEC 27001 – Информационни технологии – Методи за сигурност – ***Системи за управление на сигурността на информацията – Изисквания***

БДС EN ISO/IEC 27002 – Информационни технологии – Методи за сигурност – ***Кодекс за добра практика за управление на сигурността на информацията***

БДС ISO/IEC 27003 – Информационни технологии – Методи за сигурност – ***Указания за внедряване на системи за управление на сигурността на информацията***

БДС ISO/IEC 27004 – Информационни технологии – Методи за сигурност – ***Управление на сигурността на информацията – Наблюдение, измерване, анализ и оценяване***

ISO/IEC 27009 – ***Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements*** (Информационни технологии – Техники за сигурност – ***Специфично за секторите прилагане на ISO/IEC 27001 – Изисквания***)

БДС ISO/IEC 27013 – Информационни технологии – Методи за сигурност – ***Указания за съвместно внедряване на ISO/IEC 27001 и ISO/IEC 20000-1***

ISO/IEC 27014 – Information technology – Security techniques – ***Governance of information security*** (Информационни технологии – Методи за сигурност – ***Управление на сигурността на информацията***)

ISO/IEC 27017 – Information technology – Security techniques – ***Code of practice for information security controls based on ISO/IEC 27002 for cloud services*** (Информационни технологии – Методи за сигурност – ***Кодекс за добра практика за контрол на сигурността на информацията за облачни услуги, базиран на ISO/IEC 27002***)

ISO/IEC 29146 – Information technology – Security techniques – ***A framework for access management*** (Информационни технологии – Методи за сигурност – ***Рамка за управление на достъпа***)

БДС ISO/IEC 27018 – Информационни технологии – Методи за сигурност – ***Кодекс за добра практика за защита на лични данни (personally identifiable information PII) в обществени облаци, действащи като администратори на PII***

Стандарти за управление на риска

БДС ISO/IEC 27005 – Информационни технологии – Методи за сигурност – ***Управление на риска за сигурността на информацията***

БДС ISO 31000 – Управление на риска – ***Указания***

БДС EN 31010 – Управление на риска – ***Методи за оценяване на риска***

ETSI TS 102 165-1 – CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA) (КИБЕР; ***Методи и протоколи***; Част 1: Методика и професионална форма на заплаха, уязвимост, анализ на риска (Threat, Vulnerability, Risk Analysis (TVRA)

Стандарти за идентификация и автентикация

ISO/IEC 11770-1 – Information technology – Security techniques – ***Key management*** – Part 1: Framework (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 1: Рамка)

ISO/IEC 11770-2 – Security techniques – ***Key management*** – Part 2: Mechanisms using symmetric techniques (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 2: Механизми, използващи симетрични техники)

ISO/IEC 11770-3 – Information technology – Security techniques – ***Key management*** – Part 3: Mechanisms using asymmetric techniques (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 3:Споразумение за невидими Diffie-Hellman ключове)

ISO/IEC 11770-4 – Information technology – Security techniques – ***Key management*** – Part 4: Mechanisms based on weak secrets (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 4: Механизми, основани на слаби тайни)

ISO/IEC 11770-5 – Information technology – Security techniques – ***Key management*** – Part 5: Group key management (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 5: Управление на групови ключове)

ISO/IEC 11770-6 – Information technology – Security techniques – ***Key management*** – Part 6: Key derivation (**Информационни технологии** – Методи за сигурност – ***Управление на ключовете*** – Част 6: Деривация на ключове)

ISO/IEC 20889 – Privacy enhancing data de-identification terminology and classification of techniques (Технологии за защита на личните данни от де-идентификация, терминология и класификация на техниките)

ISO/IEC 24760-1 – Information technology – Security techniques – ***A framework for identity management*** – Part 1: Terminology and concepts (**Информационни технологии** – Методи за сигурност – ***Рамка за управление на идентичността*** – Част 1: Терминология и понятия)

ISO/IEC 24760-2 – Information technology – Security techniques – ***A framework for identity management*** – Part 2: Reference architecture and requirements (Информационни технологии – Методи за сигурност – ***Рамка за управление на идентичността*** – Част 2: Препоръчителна архитектура и изисквания)

ISO/IEC 24760-3 – Information technology – Security techniques – ***A framework for identity management*** – Part 3: Practice (Информационни технологии – Методи за сигурност – ***Рамка за управление на идентичността*** – Част 3: Прилагане)

ISO/IEC 29115 – Information technology – Security techniques – ***Entity authentication assurance framework*** (Информационни технологии – Методи за сигурност – ***Рамка за гарантиране на автентичността на субекти***)

ISO/IEC 29151 – Information technology – Security techniques – **Code of practice for personally identifiable information protection** (Информационни технологии – Техники за сигурност – ***Кодекс на практики за защита на личната информация***)

ISO/IEC 29191 – Information technology – Security techniques – ***Requirements for partially anonymous, partially unlinkable authentication*** (Информационни технологии – Техники за защита – ***Изисквания за частично анонимно удостоверяване, частична псевдоминизация***)

ISO/IEC 18370-1 – Information technology – Security techniques – ***Blind digital signatures*** – Part 1: General (**Информационни технологии** – Методи за сигурност – ***Невидими цифрови подписи*** – Част 1: Общи положения)

ISO/IEC 18370-2 – Information technology – Security techniques – ***Blind digital signatures*** – Part 2: Discrete logarithm based mechanisms (Информационни технологии – Методи за сигурност – ***Невидими цифрови подписи*** – Част 2: Механизми, базирани на дискретни логаритми)

ISO/IEC 20008-1 – Information technology – Security techniques – ***Anonymous digital signatures*** – Part 1: General (Информационни технологии – Методи за сигурност – ***Анонимни цифрови подписи*** – Част 1: Общи положения)

ISO/IEC 20008-2 – Information technology – Security techniques – ***Anonymous digital signatures*** – Part 2: Mechanisms using a group public key (Информационни технологии – Методи за сигурност – ***Анонимни цифрови подписи*** – Част 2: Механизми с използване на групов публичен ключ)

ISO/IEC 20009-1 – Information technology – Security techniques – ***Anonymous entity authentication*** – Part 1: General (Информационни технологии – Методи за сигурност – ***Идентификация на анонимни обекти*** – Част 1: Общи положения)

ISO/IEC 20009-2 – Information technology – Security techniques – ***Anonymous entity authentication*** – Part 2: Mechanisms based on signatures using a group public key (Информационни технологии – Методи за сигурност – ***Идентификация на анонимни обекти*** – Част 2: Механизми, основани на подписи с използване на групов публичен ключ)

ISO/IEC 20009-4 – Information technology – Security techniques – ***Anonymous entity authentication*** – Part 4: Mechanisms based on weak secrets (Информационни технологии – Методи за сигурност – ***Идентификация на анонимни обекти*** – Част 4: Механизми, основани на слаби тайни)

Стандарти за криптиране

ISO/IEC 18033-1 – Information technology – Security techniques – ***Encryption algorithms*** – Part 1: General (Информационни технологии – Методи за сигурност – ***Алгоритми за криптиране*** – Част 1: Общи

положения)

ISO/IEC 18033-2 – Information technology – Security techniques – ***Encryption algorithms*** –Part 2: Asymmetric ciphers (Информационна технология – Методи за сигурност – ***Алгоритми за криптиране*** – Част 2: Асиметрични шифри)

ISO/IEC 18033-4 – Information technology – Security techniques – ***Encryption algorithms*** – Part 3: Block ciphers (Информационни технологии – Методи за сигурност – ***Алгоритми за криптиране*** – Част 3: Блокови шифри)

ISO/IEC 18033-4 – Information technology – Security techniques – ***Encryption algorithms*** – Part 4: Stream ciphers (Информационни технологии – Методи за сигурност – ***Алгоритми за криптиране*** – Част 4: Поточни шифри)

ISO/IEC 18033-5 – Information technology – Security techniques – ***Encryption algorithms*** – Part 5: Identity-based ciphers (Информационни технологии – Методи за сигурност – ***Алгоритми за криптиране*** – Част 5: Шифри, базирани на идентичност)

Стандарти за одити

ISO/IEC 27006 – Information technology – Security techniques – ***Requirements for bodies providing audit and certification of information security management systems*** (Информационни технологии – Методи за сигурност – ***Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията***)

ISO/IEC 27007 – Information technology – Security techniques – ***Guidelines for information security management systems auditing*** (Информационни технологии – Методи за сигурност – ***Указания за одит на системи за управление на сигурността на информацията – допълнение към насоките, съдържащи се в стандарт ISO 19011***)

БДС EN ISO 19011– *Указания за извършване на одит на системи за управление*

БДС EN ISO/IEC 17020 – Оценяване на съответствието – ***Изисквания за дейността на различни видове органи, извършващи контрол***

Стандарти за оценка на сигурността

ISO/IEC 15408-1 – Information technology – Security techniques – ***Evaluation criteria for IT security*** – Part 1: Introduction and general model (Информационни технологии – Методи за сигурност – ***Критерии за оценка на ИТ сигурността*** –
Част 1: Въведение и общ модел)

ISO/IEC 15408-2 – Information technology – Security techniques – ***Evaluation criteria for IT security*** – Part 2: Security functional components (Информационни технологии – Методи за сигурност – ***Критерии за оценка на ИТ сигурността*** –
Част 2: Функционални компоненти за сигурност)

ISO/IEC 15408-3 – Information technology – Security techniques – ***Evaluation criteria for IT security*** – Part 3: Security assurance components (Информационни технологии – Методи за сигурност – ***Критерии за оценка на ИТ сигурността*** –
Част 3: Компоненти за осигуряване на сигурност)

ISO/IEC 18045 – Information technology – Security techniques – ***Methodology for IT security evaluation*** (Информационни технологии – Методи за сигурност – ***Методология за оценка на ИТ сигурността***)

ISO/IEC TS 19608 – ***Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 (Указания за разработване на функционални изисквания за сигурност и неприкосновеност, основани на ISO/IEC 1540)***

ISO/IEC TR 20004:2015 – Information technology – Security techniques – ***Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*** (Информационни технологии – Методи за сигурност – ***Усъвършенстване на анализа на софтуерните уязвимости в съответствие с ISO/IEC 15408 и ISO/IEC 18045***)

ISO/IEC 29134 – Information technology – Security techniques – ***Guidelines for privacy impact assessment*** (Информационни технологии – Методи за сигурност – ***Указания за оценка на въздействието върху неприкосновеността на личните данни***)

ISO/IEC 29190 – Information technology – Security techniques – ***Privacy capability assessment model*** (Информационни технологии – Методи за сигурност – ***Модел за оценка на способността за защита на личните данни***)

Стандарти за сигурност, които са в етап на разработване през 2019 г.

ISO/IEC CD 20009-3 – Information technology – Security techniques – **Anonymous entity authentication** – Part 3: Mechanisms based on blind signatures concepts (Информационни технологии – Методи за сигурност – ***Идентификация на анонимни обекти*** – Част 3: Механизми, основани на концепции за скрити подписи)

ISO/IEC 27551 – Information technology – Security techniques – ***Requirements for attribute-based unlinkable entity authentication*** (Информационни технологии – техники за сигурност – ***Изисквания за удостоверяване на субекти на базата на несвързващи атрибути***)

ISO/IEC PDTR 27550 – Information technology – Security techniques – ***Privacy engineering*** (Информационни технологии – Техники за сигурност – ***Инженеринг на лични данни***)

ISO/IEC DIS 27552 – Security techniques – ***Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*** – Requirements and guidelines (Методи за сигурност – ***Разширяване на ISO/IEC 27001 и ISO/IEC 27002 за управление на личната информация*** – Изисквания и насоки)

ISO/IEC 27030 – Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT) (Информационни технологии – Методи за сигурност – ***Указания за сигурност и неприкосновеност на личните данни в Интернет на нещата (IoT)***

ISO/IEC 29184 – Information technology – ***Online privacy notices and consent*** (Информационни технологии – ***Съобщения и съгласие за поверителност в интернет***)

Забележка. Номерата на стандартите са уникални и еднозначно свързани с техните имена. Пред номера на стандарта се изписват абревиатурите на организациите, които са го одобрили. След номера на стандарта се изписва годината, в която той е приет. Общото изписване е от вида ISO/IEC 27001:2013 или БДС ISO/IEC 27001:2018, като в случая става въпрос за един и същ стандарт.
Стандартите се преглеждат от съответните организации и при необходимост се актуализират на всеки пет години, като новата версия отменя действието на предишната. За да се постигне относителна устойчивост на тази наредба и независимост от цикъла за преразглеждане на стандартите, в наредбата не се посочват годините на издаване на стандартите.

Приложение № 2
към чл. 6, ал. 1 и 7

КЛАСИФИКАЦИИ НА ИНФОРМАЦИЯТА

С цел да се гарантира достатъчна, адекватна и пропорционална на заплахите защита на информацията, се прави преценка на важността и чувствителността ѝ, както и на нормативните изисквания към нея. Въз основа на тази преценка информацията се разделя в няколко категории. Когато е приложимо, тази класификация се пренася и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето, разпространението и унищожаването на информацията, и към тях се прилагат подходящи мерки за защита, съответстващи на заплахите.

1. TLP (traffic light protocol) – използва се при обмен на информация

[TLP-RED] – Само за определени получатели: в контекста на една среща например информацията се ограничава до присъстващите на срещата. В повечето случаи тази информация се предава устно или лично.
[TLP-AMBER] – Ограничено разпространение: получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът "необходимост да се знае". Често практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.
[TLP-GREEN] – Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.
[TLP-WHITE] – Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

2. Препоръчителна класификация на информацията и изисквания към информационните и

комуникационните системи за осигуряване на достъп до информацията:
2.1. "Ниво 0" обхваща открита и общодостъпна информация (например публикувана на интернет страниците); предполага анонимно ползване на информацията и липса на средства за защита на конфиденциалността ѝ; отговаря на **TLP-WHITE**;
2.1.1. оповестяването на информация с класификация "**Ниво 0**" не е ограничено;
2.1.2. източниците могат да използват класификация "**Ниво 0**", когато информацията носи минимален или никакъв предвидим риск от злоупотреба, в съответствие с приложимите правила и процедури за публично оповестяване;
2.1.3. при спазване на стандартните правила за авторски права информация с класификация "**Ниво 0**" може да се разпространява без ограничения.
2.2. "Ниво 1"
2.2.1. споделянето на информация с класификация "**Ниво 1**" е ограничено само до дадена общност; отговаря на **TLP-GREEN**;
2.2.2. източниците могат да използват класификация "**Ниво 1**", когато информацията е полезна за информираността на всички участващи организации, както и за партньори от широката общност или сектор;
2.2.3. получателите могат да споделят информация с класификация "**Ниво 1**" с партньорски организации в рамките на своя сектор или общност, но не и чрез обществено достъпни канали; информацията в тази категория може да се разпространява широко в дадена общност, но не и извън нея;
2.2.4. изисквания към **информационните и комуникационните системи:**
2.2.4.1. достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;
2.2.4.2. 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;
2.2.4.3. идентифициращата информация трябва да бъде защитена от нерегламентиран достъп;
2.2.4.4. доверителната изчислителна система, т. е. функционалността на информационната система, която управлява достъпа до ресурсите, трябва да поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи хода на работата;
2.2.4.5. информационната система трябва да разполага с технически и/или програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;
2.2.4.6. защитните механизми трябва да са преминали тест, който да потвърди, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.
2.3. "Ниво 2"
2.3.1. разпространението на информация с класификация "**Ниво 2**" е разрешено само в рамките на организациите на участниците, обработващи, съхраняващи или обменящи информацията; отговаря на **TLP-AMBER** с допълнително уточнение за ограничение на достъпа;
2.3.2. източниците могат да използват класификация "**Ниво 2**", когато информацията изисква защита, за да бъде ефективно обменена, и носи риск за неприкосновеността на личния живот, репутацията или операциите, ако се споделя извън съответните организации;
2.3.3. получателите могат да споделят информация с класификация "**Ниво 2**" с членове на собствената си организация и с потребители или клиенти, които трябва да са запознати с нея, за да се защитят или да предотвратят допълнителни щети; източниците имат правото да определят допълнителни планирани граници на споделянето, които трябва да се спазват;
2.3.4. изисквания към **информационните и комуникационните системи** – в допълнение към изискванията към предишното ниво:
2.3.4.1. 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;
2.3.4.2. при издаване на удостоверението издаващият орган проверява съществените данни за личността на ползвателя, без да е необходимо личното му присъствие;
2.3.4.3. доверителната изчислителна система трябва да осигури реализация на принудително управление на достъпа до всички обекти;
2.3.4.4. доверителната изчислителна система трябва да осигури взаимна изолация на процесите чрез разделяне на адресните им пространства.
2.4. "Ниво 3"
2.4.1. информация с класификация **"Ниво 3"** не е за оповестяване и разпространението ѝ е ограничено само до участниците, обработващи, съхраняващи или обменящи информацията; отговаря на **TLP-RED**;
2.4.2. източниците могат да използват класификация **"Ниво 3"**, когато информацията не може да бъде ефективно обменяна с други страни и би могла да доведе до въздействия върху неприкосновеността на личния живот, репутацията или операциите на дадена страна, ако с нея бъде злоупотребено;
2.4.3. получателите не могат да споделят информация, маркирана с **"Ниво 3"**, с която и да е страна извън конкретния обмен, обработка или съхранение; достъпът до информацията с класификация **"Ниво 3"** е ограничен само до лицата, участващи в обработката ѝ; в повечето случаи информация с класификация **"Ниво 3"** трябва да се предава лично;
2.4.4. изисквания към ИКТ системите – в допълнение към изискванията към предишното ниво:
2.4.4.1. като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;
2.4.4.2. при издаване на удостоверението да е гарантирана физическата идентичност на лицето;

2.4.4.3. доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;
2.4.4.4. комуникацията между потребителя и системата да се осъществява по криптирани канали, използващи протокол Transport Layer Security (TLS) поне 1.2, като минималната дължина на криптиращия ключ трябва да е поне 256 бита;
2.4.4.5. доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

Приложение № 3
към чл. 7, ал. 3

АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

I. ВЪВЕДЕНИЕ
Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност.
По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

II. ОПРЕДЕЛЕНИЯ
Конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
Интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
Наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

III. ЦЕЛИ
1. Цел на процеса за управление на риска
Да минимизират загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях.
2. Цел на методиката за анализ и оценка на риска
Методиката има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от различните администрации, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:
2.1. регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
2.2. определяне на критериите;
2.3. определяне на приоритетите на риска.

ПРЕПОРЪЧИТЕЛНА МЕТОДИКА

I. ЕТАПИ НА АНАЛИЗ И ОЦЕНКА НА РИСКА

Анализът и оценката на риска са част от процеса за управлението му и се обосновават на познаване на всички компоненти, имащи отношение към целите.
За целите на управлението на сигурността на мрежите и информационните системи трябва:
а) да се познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на тази наредба (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация, поддържащите ги системи (електрозахранващи, климатизиращи и др.), оперативни процеси/дейности, служители и външни организации), наричани за краткост "информационни активи";
б) да се идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
в) да се оцени вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимости) на информационните активи и мерките, които са предприети за справяне с тях;
г) да се оцени въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
д) да се оцени рискът за сигурността;
е) да се набележат мерки за смекчаване на рисковете с висок приоритет.
При анализ и оценка на риска се използва регистър на рисковете (риск-регистър). Примерен регистър на рисковете е даден в края на това приложение.
1. Идентифициране на информационните активи
В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на тази наредба:
а) информационни системи;

б) хардуерни устройства, с които са реализирани информационните системи;
в) софтуери, с които са реализирани информационните системи;
г) бази данни, включително лични данни по смисъла на GDPR;
д) записи за събитията (логове, журнали) на информационните системи;
е) документация на информационните системи (експлоатационна и потребителска);
ж) комуникационни системи;
з) хардуерни устройства, с които са реализирани комуникационните системи;
и) фърмуерът на тези устройства;
к) софтуери на комуникационните системи;
л) записи за събитията (логове, журнали);
м) документация (експлоатационна и потребителска);
н) поддържащи системи (електрозахранващи, климатични);
о) системи за контрол на физическия достъп и на околната среда;
п) процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
р) документация на тези процеси и дейности;
с) служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
т) външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
у) друго.

2. Идентифициране на заплахите

За всеки от информационните активи в риск-регистъра се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията. Трябва да се разгледат всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.
Примерни заплахи са посочени в края на това приложение.
В риск-регистъра за всяка заплаха се вписва какви мерки са предприети срещу нея.

3. Оценка на въздействието

В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които дадена заплаха може да причини, ако се реализира.
За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.

4. Оценка на вероятността

Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:
а) за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
б) за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.
В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.
За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:
1 – вероятността от реализирането на заплахата е под 10 %;
2 – вероятността от реализиране на заплахата е от 10 % до 30 %;
3 – вероятността от реализиране на заплахата е от 30 % до 50 %;
4 – вероятността от реализиране на заплахата е от 50 % до 70 %;
5 – вероятността от реализиране на заплахата е над 70 %.

5. Оценка на риска

За получаване на оценката на риска се използва следната формула:
(Оценка на въздействие x Оценка на вероятност) = Оценка на риска

6. Приоритизация на рисковете

С цел прилагане на пропорционални на заплахите механизми за защита се прави приоритизация на рисковете на база на тяхната оценка и следните прагове:

Приоритет на риска	Оценка на риска
1	от 17 до 25
2	от 8 до 17
3	от 1 до 8

7. Смекчаване на рисковете

Приема се, че за рискове с приоритет 3 не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.
За рисковете с приоритет 2 се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят

отговорно лице и срок за прилагане на тези мерки.
За всички рискове с приоритет 1 се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

II. ПОСЛЕДВАЩИ ДЕЙСТВИЯ

Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.
Ръководството на администрацията организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

ПРЕПОРЪЧИТЕЛЕН РЕГИСТЪР НА РИСКОВЕТЕ

№ по ред	Информационен актив	Заплахи/ нежелани събития	Приложени мерки за защита	Оценка на въздействието (от 1 до 5)	Оценка на вероятността (от 1 до 5)	Оценка на риска	Приоритет на риска (от 1 до 3)

ВЕРОЯТНИ ЗАПЛАХИ

- Влошаване на средствата за съхраняване
- Грешка при техническото обслужване
- Грешки при предаването
- Електромагнитна радиация
- Зловреден програмен код
- Злоупотреба с ресурси
- Използване на неразрешени програми и данни
- Кражба
- Маскиране на потребителска идентификация (нелегално проникване)
- Неоторизиран достъп до компютри, данни, услуги и приложения
- Неоторизиран достъп до средствата за съхраняване
- Неправилна (погрешна) маршрутизация/пренасочване на съобщения
- Отричане (доказуемост)
- Повреда на комуникационното оборудване и услугите
- Подслушване
- Пожар, наводнение

•Потребителска грешка

•Администраторска грешка

•Прекъсване/повреда на захранването (електричество и климатизация)

•Претоварване на трафика

•Природни бедствия

•Кибератака

•Софтуерни проблеми

•Техническа повреда (мрежа, системен хардуер)

Приложение № 4
към чл. 22, ал. 6

ИЗИСКВАНИЯ ЗА КОНФИГУРИРАНЕ

1. Да се забрани macros в office пакетите.
2. Да се забрани pop-up в браузерите.
3. Auto play функцията да се конфигурира винаги да иска потвърждение на потребителя.
4. User Account Control да се конфигурира до най-високо ниво, така че винаги да издава предупреждения.
5. При споделянето на файлове и принтери да не се използва настройка Everyone, а да се указва кои акаунти точно да имат право на достъп до тях.
6. Да се забрани TRACE/TRACK методът.
7. Да се забрани anonymous authentication.
8. Да се използва Unicast Reverse-Path Forwarding (uRPF) за предпазване от използването на фалшиви IP адреси и rate-limiting за ограничаване на броя на заявките по IP адрес.
9. Да се забрани TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия.
10. Съобщенията за грешки в системите да не дават излишна информация.
11. Да не се използва AutoComplete.
12. Да се използват приложения (add-ons) към браузърите за блокиране на рекламно съдържание.

Приложение № 5
към чл. 24, т. 13

ИЗИСКВАНИЯ КЪМ HEADERS НА ОТГОВОРИТЕ НА ЗАЯВКИ ЗА УЕБ САЙТОВЕТЕ

1. Headers на отговорите на заявките да не съдържат информация за платформите и версиите на използвания софтуер.
2. Headers на отговорите на заявките да съдържат следните опции:
а) HTTP Strict Transport Security (HSTS) – политика съгласно RFC 6797 на IETF от 2012 г., която принуждава уеб браузъра на клиента да се свърже директно чрез HTTPS при преразглеждане на уеб сайта; препоръчителна стойност на периода на валидност на кеша на HSTS (max-age) е поне шест месеца;
б) X-Content-Type-Options – инструктира потребителския браузър да следва стриктно типа MIME, дефиниран в Content header; единствената валидна стойност за този хедър е "X-Content-Type-Options-nosniff";
в) X-XSS-Protection – настройва конфигурацията за XSS филтъра, вграден в повечето браузъри, което предотвратява някои категории XSS атаки; препоръчителна стойност "X-XSS-Protection: 1; mode=block";
г) X-Frame-Options – дава указания на браузъра да не вкарва уеб страницата във frame/iframe на други уеб страници; препоръчителна стойност "x-frame-options: SAMEORIGIN";
д) Content-Security-Policy – предотвратява широк спектър от атаки, включително Cross-site scripting и други cross-site injections;
е) Referrer-Policy Header – позволява на сайта да контролира колко информация с навигация да се включва в браузъра извън документа;
ж) Feature-Policy Header – позволява на сайта да контролира кои функции и приложни програмни интерфейси (API) могат да се използват в браузъра;
з) HTTP Public Key Pinning (HPKP) – защитен механизъм, който позволява на HTTPS уеб сайтовете да се противопоставят на имитация от страна на атакуващите, използвайки неправилно издадени или лъжливи сертификати.

Приложение № 6
към чл. 3, ал. 2, т. 2

ПРЕПОРЪЧИТЕЛНИ ФУНКЦИИ НА СЛУЖИТЕЛЯ/ЗВЕНОТО, ОТГОВАРЯЩ/О ЗА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност, и целите, заложени в политиката на Субекта по чл. 4.
2. Участва в изготвянето на политиките и документираната информация.
3. Следи за спазването на вътрешните правила по смисъла на чл. 5, ал. 1, т. 6 и прилагането на законите, подзаконовите нормативни актове, стандартите, политиките и правилата за мрежовата и информационната сигурност.
4. Консултира ръководството на Субекта във връзка с информационната сигурност.
5. Ръководи периодичните оценки на рисковете за мрежовата и информационната сигурност.
6. Периодично (не по-малко от веднъж в годината) изготвя доклади за състоянието на мрежовата и информационната сигурност в административното звено и ги представя на ръководителя.
7. Координира обученията, свързани с мрежовата и информационната сигурност.
8. Организира проверки за актуалността на плановете за справяне с инцидентите и плановете за действия в случай на аварии, природни бедствия или други форсмажорни обстоятелства. Анализира резултатите от тях и организира изменение на плановете, ако е необходимо.
9. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност.
10. Следи за акуратното водене на регистъра на инцидентите.
11. Уведомява за инциденти съответния секторен екип за реагиране на инциденти с компютърната сигурност в съответствие с изискването на чл. 31, ал. 1 (уведомяване за инциденти) от тази наредба.
12. Организира анализ на инцидентите с мрежовата и информационната сигурност за откриване на причините за тях и предприемане на мерки за отстраняването им с цел намаляване на еднотипните инциденти и намаляване на загубите от тях.
13. Следи за актуализиране на използвания софтуер и фърмуер.
14. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.
15. Организира тестове за откриване на уязвимости в информационните и комуникационните системи и предлага мерки за отстраняването им.
16. Организира и сътрудничи при провеждането на одити, проверки и анкети и при изпращането на резултатите от тях на съответния национален компетентен орган.
17. Предлага санкции за лицата, нарушили мерките за мрежовата и информационната сигурност.

Приложение № 7
към чл. 31, ал. 2

УВЕДОМЛЕНИЕ ЗА ИНЦИДЕНТ към секторния ЕРИКС

Необходима информация	Детайли	Данни
(до 2 часа)		
Лице, подаващо уведомлението	Име, фамилия	
Вашият телефонен номер	(GSM)	
Вашата електронна поща		
Организация	Наименование на организацията, засегната от инцидента	
Лице за контакт (за целите на разрешаването на инцидента)	Име, телефонен номер и електронна поща на компетентно лице от предприятието, което при необходимост може да подаде допълнителна информация	
Дата и час	Вписват се датата и часът на възникване на инцидента, ако не е възможно – датата и часът на откриването му	
Тип на инцидента		□ Virus □ Trojan □ Botnet □ Dos/DDos □ Malware □ Port Scan □ Spam □ Phishing □ Pharming

Необходима информация	Детайли	Данни
		□ Probe □ Crack □ Copyright □ Ransomware □ Defacement □ Exploiting known Vulnerabilities □ Application Compromise □ Login Attempts □ SQL injections □ Unknown □ Other
Кратко описание на инцидента	Вписва се кратко описание на инцидента, като се включва всяка практическа/техническа информация (тази информация се предоставя, в случай че е налична)	
Трансгранично въздействие	• Вписва се информация за евентуално трансгранично въздействие и се посочват държавите • Вписва се информация за услугите, които са засегнати	
Въздействие върху други съществени услуги	Вписва се информация на кои други съществени услуги евентуално ще окаже въздействие	
Засегната система (попълва се, ако е налична информацията)	IP Address: DNS: Operating System:	
Източник на атаката (попълва се, ако е налична информацията)	IP Address: DNS:	
Предприети действия	Описват се първоначалните действия, предприети до момента – до 2 часа от засичането на инцидента	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	
до 5 работни дни		
Механизъм на атаката	Описва се механизмът на атаката	
Предприети действия	Описват се подробно действията, предприети за разрешаване на инцидента	
Необходимост от коригиращи действия	Има ли необходимост от промяна в настройките на защитните стени, WAF или др. Промяна на политиката за сигурност, ако се налага Обучение на персонала	
Анализ на артефаки	Описват се резултатите от анализа на артефактите, ако има установени такива, и инструментите, използвани за това. Изпраща се копие от артефактите	
Публично оповестяване	Съгласно комуникационна стратегия на администрацията	

Забележка. Попълва се допълнителна информация в случай на необходимост.

Приложение № 8
към чл. 31, ал. 3

ОБОБЩЕНА СТАТИСТИЧЕСКА ИНФОРМАЦИЯ ЗА ИНЦИДЕНТИ от секторния ЕРИ

	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Получени сигнали		
Засегнати IP адреси		
Изпратени мейли		
Регистрирани на сайта		

Не всички сигнали се регистрират като инциденти

Приоритет на регистрираните инциденти	I/II/ III/IV тримесечие за текущата година	Общо за текущата година
Висок		
Среден		
Нисък		
Общо	0	0

Определянето на приоритета на инциденти се извършва съгласно приложение № 7

Видове инциденти	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Fraud		
Malicious code		
Abusive Content (Spam)		
Availability (DDoS)		
Intrusion Attempts		
Information Gathering		
Intrusions		
Information Security		
Vulnerable		
Other		
Botnet		
Общо:	0	0

Класификацията на инцидентите се извършва съгласно таксономията на ENISA, посочена в приложение № 7

Засегнати IP адреси по видове инциденти	I/II/III/IV тримесечие за текущата година	Общо за текущата година
Fraud		
Malicious code		
Spam		
Botnet		
Availability (DDoS)		
Intrusion Attempts		
Information Gathering		
Intrusions		
Vulnerable		
Other		
Засегнати IP адреси	0	0

Приложение № 9

КЛАСИФИКАЦИЯ НА ИНЦИДЕНТИТЕ И ПРИОРИТЕТ

Клас	Тип на инцидента	Приоритет	Описание/пример
Abusive Content	Spam	Нисък	"Нежелана електронна поща". Използването на среда за електронни комуникации (интернет) за масово изпращане на нежелани съобщения. Spam съобщенията се изпращат като част от по-голяма колекция от съобщения, всички с идентично съдържание.
	Harassment	Нисък	Компромати или дискриминация спрямо някой (пр. cyberstalking).
	Child/sexual/violence/...	Висок	Детската порнография, прослава на насилието, ...
Malicious Code	Virus	Среден	Софтуер, който преднамерено се инсталира в системите с вредни цели. Необходимо е действие на потребителя, за да се активира кодът.
	Worm	Среден	
	Trojan	Среден	
	Spyware	Среден	
	Dialer	Среден	

Клас	Тип на инцидента	Приоритет	Описание/пример
Information Gathering	Scanning	Среден	Атаки, които изпращат заявки към дадена система с цел да открият слаби места. Това включва също и някои видове тестове с цел да се събере информация за хостове, услуги и сметки. Примери: fingerd, DNS заявки, ICMP, SMTP (EXPN, RCPT, ...).
	Sniffing	Нисък	Наблюдение и записване на мрежовия трафик (wiretapping)
	Social engineering	Нисък	Събиране на информация от индивиди без използване на технически средства (например, лъжи, трикове, подкупи или заплахи).
Intrusion Attempts	Exploiting known vulnerabilities	Среден	Опит да се компрометира система или да се наруши целостта на услуга, като се използва уязвимост със стандартизиран идентификатор, като CVE име (например, buffer overflow, backdoors, cross site scripting, и т.н.).
	Login attempts	Среден	Множество опити за логване в система (пр. guessing/cracking of passwords, brute force).
	New attack signature	Нисък	Опит за атака, използващ нови техники.
Intrusions	Privileged account compromise	Среден	Успешен пробив в система или приложение (услуга). Това може да е причинено дистанционно чрез използване на известна или нова уязвимост, както и локално от неоторизирано лице.
	Unprivileged account compromise	Среден	
	Application compromise	Среден	
Availability	DoS	Висок	В този вид атака системата се бомбардира с толкова много пакети, че процесите се забавят или системата блокира. Примери за отдалечен DoS са SYN- и PING-flooding, бомбардиране на електронна поща и др. (DDoS: TFN, Trinity и др.) Въпреки това наличността на услугите може да бъде засегната и от действия на локално ниво (унищожаване, прекъсване на електро-захранването и др.)
	DDoS	Висок	
	Sabotage	Висок	
Information Security	Unauthorized access to information	Среден	Освен локални злоупотреби с данни и системи, сигурността на информацията може да бъде застрашена и от успешно компрометиране на акаунти и приложения. В допълнение на това са възможни и атаки, които прихващат и достъпват информация по време на нейното предаване (подслушване, подправяне или прихващане).
	Unauthorized modification of information	Среден	
Fraud	Unauthorized use of resources	Среден	Използване на ресурси за непозволени цели, включително парично облагодетелстване (например, използването на електронна поща за участие в незаконно разпращане на писма с цел облагодетелстване или участие в пирамидални схеми за източване на данни и средства).
	Copyright	Нисък	Продажба и инсталиране на нелицензирани копия на търговски софтуер или други защитени с права търговски материали (Warez).
	Masquerade	Висок	Видове атаки, в които едно лице незаконно приема самоличността на друго, за да се възползва от него.
	Phishing	Висок	Атака, при която е създадено копие на легитимна WEB страница, през която жертвите са подмамвани да въвеждат лични данни или друга конфиденциална информация. Въведените данни се използват по-нататък за незаконни дейности.
Other	Всички останали	Нисък	За всички инциденти, които не попадат в по-горната класификационна схема.