ЗАКОН ЗА КИБЕРСИГУРНОСТ

Обн. ДВ. бр.94 от 13 Ноември 2018г., изм. ДВ. бр.69 от 4 Август 2020г., изм. и доп. ДВ. бр.85 от 2 Октомври 2020г., изм. и доп. ДВ. бр.15 от 22 Февруари 2022г., изм. ДВ. бр.25 от 29 Март 2022г.

Проект: 802-01-18/30.05.2018 г.

Глава първа.
ОБЩИ ПОЛОЖЕНИЯ

Предмет

Чл. 1. (1) Този закон урежда дейностите по:

1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността;

2. предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност.

(2) С този закон се определят и правомощията и функциите на компетентните органи в областта на киберсигурността.

Киберсигурност. Мрежова и информационна сигурност

Чл. 2. (1) Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им.

(2) Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана.

(3) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.

Мерки за мрежова и информационна сигурност

Чл. 3. (1) Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите по чл. 4, ал. 1 и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране.

(2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Минималният обхват на мерките за мрежова и информационна сигурност, както и други препоръчителни

мерки, се определят с наредба на Министерския съвет по предложение на министъра на електронното управление. Мерките не може да налагат използването на определен тип технология.

(3) Наредбата по ал. 2 не се прилага за ведомствата и функциите им по чл. 5, т. 2.

(4) Субектите по чл. 4, ал. 1, т. 1 и 2 поддържат система за управление на сигурността на информацията, която включва следните минимални организационни мерки:

1. разпределение на отговорностите за мрежовата и информационната сигурност;

2. прилагане на политика за мрежовата и информационната сигурност;

3. управление на:

а) риска;

б) информационните активи, включително човешките ресурси;

в) инцидентите;

г) достъпите (физически и логически);

д) измененията;

е) непрекъснатостта на дейността и/или услугите (съществени, цифрови);

ж) взаимодействията с трети страни.

Обхват

Чл. 4. (1) С този закон се определят изискванията към:

1. административните органи;

2. операторите на съществени услуги и доставчиците на цифрови услуги - за всеки сектор, подсектор и услуги, посочени в приложения № 1 и 2;

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

4. организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път.

(2) Оператор на съществени услуги е публичен или частен субект от посочените в приложение № 1 категории, който отговаря на следните критерии:

1. да предоставя съществена услуга, и

2. предоставянето на тази съществена услуга да зависи от мрежи и информационни системи, и

3. инцидентите в мрежовата и информационната сигурност да имат значително увреждащо въздействие върху предоставянето на тази услуга.

(3) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1 определят операторите на съществени услуги съгласно критериите по ал. 2 и в съответствие с методика, приета от Министерския съвет, и

уведомяват министъра на електронното управление за това. Методиката се приема по предложение на министъра на електронното управление.

(4) Когато оператор предоставя съществена услуга в две или повече държави - членки на Европейския съюз, административният орган по чл. 16, ал. 1 провежда консултации със съответните държави преди вземането на решение относно определянето на оператора.

(5) Операторите на съществени услуги спазват изискванията за мрежова и информационна сигурност, предвидени в този закон, само по отношение на предоставяните от тях съществени услуги.

(6) Когато в правен акт на Европейския съюз или в закон, който е специален за конкретен сектор или услуга, посочени в приложения № 1 и 2, се предвижда операторите на съществени услуги или доставчиците на цифрови услуги да гарантират мрежовата и информационната си сигурност или да уведомяват за инциденти, се прилагат тези актове, при условие че техните изисквания са най-малкото равностойни като резултат на задълженията, предвидени в този закон.

Изключения

Чл. 5. Този закон не се прилага:

1. за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация;

2. (изм. - ДВ, бр. 69 от 2020 г.) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция "Национална сигурност", Държавна агенция "Разузнаване", Държавна агенция "Технически операции", Служба "Военно разузнаване" и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители;

3. по отношение на предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги по смисъла на Закона за електронните съобщения, с изключение на чл. 14, ал. 5, чл. 15, ал. 6 и чл. 19, ал. 3;

4. за доставчици на удостоверителни услуги по смисъла на чл. 3, т. 19 от Регламент (ЕС) № 910/2014 г. на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.);

5. за доставчици на цифрови услуги, които са микро- и малки предприятия по смисъла на чл. 3, ал. 2 и 3 от Закона за малките и средните предприятия.

Регистър

Чл. 6. (1) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на

електронното управление създава, води и поддържа регистър на съществените услуги по смисъла на този закон, който съдържа:

1. видове съществени услуги;

2. списък на операторите на съществени услуги и предоставяните от тях услуги;

3. сфера на дейност;

4. брой потребители, разчитащи на услугата, предоставяна от оператора;

5. географски обхват на областта, която може да бъде засегната от даден инцидент.

(2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Списъкът по ал. 1, т. 2 се преразглежда и актуализира на всеки две години от съответните административни органи по чл. 16, ал. 1, за което те уведомяват министъра на електронното управление.

(3) Редът за водене, съхраняване и достъп до регистъра се определя с наредбата по чл. 3, ал. 2.

(4) Регистърът по ал. 1 не е публичен.

Система за киберсигурност

Чл. 7. (1) Системата за киберсигурност е част от системата за защита на националната сигурност.

(2) Управлението и организацията на системата за киберсигурност се осъществяват от Министерския съвет. За подпомагане изпълнението на тези дейности към Министерския съвет се създава Съвет по киберсигурността.

(3) Министерският съвет приема с решение Национална стратегия за киберсигурност, а в случаите по чл. 8, ал. 3 - и Национална стратегия за мрежова и информационна сигурност.

Стратегии

Чл. 8. (1) Националната стратегия за киберсигурност е стратегическа рамка на политиката за киберсигурност, която включва:

1. цели, принципи и приоритети;

2. области на действие и мерки:

а) система за киберсигурност;

б) мрежова и информационна сигурност;

в) противодействие на киберпрестъпността;

г) киберотбрана;

д) киберразузнаване;

3. взаимодействие между държава, бизнес и общество;

4. развитие и подобряване на регулаторната рамка;

5. повишаване на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността;

6. международно взаимодействие;

7. кибердипломация;

8. взаимодействие на техническо, оперативно и стратегическо (политическо) ниво.

(2) Националната стратегия за мрежова и информационна сигурност е стратегическа рамка на политиката за мрежова и информационна сигурност, която включва:

1. цели и приоритети относно мрежовата и информационната сигурност;

2. управленска рамка за постигане на целите и приоритетите по т. 1, включително функциите и отговорностите на държавните органи и на други участници;

3. мерки във връзка с подготвеността, реагирането и възстановяването в мрежите и информационните системи, включително сътрудничеството между публичния и частния сектор;

4. съществена информация за образователните и обучителните програми и програмите за повишаване на осведомеността във връзка с мрежовата и информационната сигурност;

5. посочване на плановете за научноизследователска и развойна дейност относно мрежовата и информационната сигурност;

6. план за оценка на риска с цел набелязване на рисковете;

7. списък на различните участници в изпълнението на стратегията.

(3) Национална стратегия за мрежова и информационната сигурност се изготвя, когато Националната стратегия за киберсигурност не съдържа информацията по ал. 2.

Съвет по киберсигурността

Чл. 9. (1) Съветът по киберсигурността е консултативен и координиращ орган към Министерския съвет по въпросите на киберсигурността.

(2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Председател на Съвета по киберсигурността е министърът на електронното управление.

(3) Членове на Съвета по киберсигурността са:

1. министърът на вътрешните работи;

2. министърът на отбраната;

3. министърът на външните работи;

4. министърът на финансите;

5. (изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на транспорта и съобщенията;

6. министърът на енергетиката;

7. министърът на здравеопазването;

8. министърът на околната среда и водите;

8а. (нова - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на електронното управление;

9. началникът на отбраната;

10. главният секретар на Министерството на вътрешните работи;

11. председателят на Държавна агенция "Национална сигурност";

12. председателят на Държавна агенция "Разузнаване";

13. (изм. - ДВ, бр. 69 от 2020 г.) директорът на Служба "Военно разузнаване";

14. началникът на Националната служба за охрана;

15. (отм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.)

16. секретарят на Съвета по киберсигурността;

17. секретарят на Съвета по сигурността към Министерския съвет;

18. представител на президента на републиката, изрично определен от него с указ.

(4) Президентът на републиката, председателят на Народното събрание и министър-председателят може да участват лично в заседанията на Съвета по киберсигурността.

(5) В определени случаи и по отделни въпроси в работата на Съвета по киберсигурността по покана на неговия председател може да участват председатели на постоянни комисии на Народното събрание, народни представители и ръководители на ведомства и организации.

Дейност на Съвета по киберсигурността

Чл. 10. Съветът по киберсигурността:

1. анализира тенденциите на киберзаплахите, рисковете, методите за противодействие и за развитието на необходимия капацитет, приоритетите за изграждането и развитието на човешки, технологични, инфраструктурни, финансови и организационни компоненти и при необходимост предлага решения и действия по отношение на тях;

2. предлага на Министерския съвет Национална стратегия за киберсигурност и пътната карта към нея, както и изготвя периодичната им актуализация;

3. предоставя информация на Съвета по сигурността към Министерския съвет относно състоянието на сигурността в киберпространството за включване в проекта на годишен доклад за състоянието на националната сигурност по чл. 9, т. 7 от Закона за управление и функциониране на системата за защита на националната сигурност;

4. осъществява взаимодействие с компетентните органи в областта на киберсигурността, включително с националните компетентни органи по чл. 16, с Националното единно звено за контакт, с регулаторни органи и с други институции;

5. дава предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото;

6. предлага на Министерския съвет Национален план за управление на киберкризи;

7. взаимодейства със Съвета по сигурността към Министерския съвет.

Национален координатор по киберсигурността

Чл. 11. (1) Министър-председателят определя национален координатор по

киберсигурността, който е и секретар на Съвета по киберсигурността.

(2) Националният координатор по киберсигурността:

1. ръководи изготвянето и актуализирането на Националната стратегия за киберсигурност и пътната карта към нея;

2. участва при изграждането и развитието на Националната координационно-организационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост;

3. участва при създаването и развитието на Националния киберситуационен център, координира действията и комплексната реакция при заплаха от киберкриза и заплахи от хибриден характер;

4. предлага на Съвета по киберсигурността:

а) нива за оценка на заплахата от кибератаки и киберинциденти и критерии за определянето им;

б) степени за определяне нивото на готовност за противодействие на кибератаки и киберинциденти - в зависимост от нивото на заплаха;

в) мерките, които да се предприемат при съответните степени на готовност;

5. при необходимост, в състояние на повишена заплаха от кибер- или от хибриден характер, подпомага сформирането на екипи за анализ, реакция и възстановяване с участието на експерти от различни ведомства и организации;

6. съдейства при планирането, подготовката и провеждането на учения в областта на киберсигурността;

7. осигурява взаимодействие и подпомага дейността на секретаря на Съвета по сигурността към Министерския съвет.

Министър на електронното управление (Загл. изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.)

Чл. 12. (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на електронното управление:

1. провежда държавната политика в областта на мрежовата и информационната сигурност;

2. изготвя и предлага за приемане от Министерския съвет Национална стратегия за мрежова и информационна сигурност в случаите по чл. 8, ал. 3;

3. издава методически указания и координира изпълнението на политиките за мрежова и информационна сигурност;

4. удостоверява съответствието на внедряваните от административните органи информационни системи с изискванията за мрежова и информационна сигурност и упражнява контрол върху администрациите за спазване на тези изисквания;

5. упражнява контрол за спазване на изискванията за мрежова и информационна сигурност на административните органи, с изключение на ведомствата по чл. 5, т. 2;

6. осъществява проверки чрез оправомощени от него лица на информационната сигурност на определена информационна система или на предприетите от административния орган мерки и дава предписания за тяхното подобряване; в обхвата

на проверките не попадат информационни системи на ведомствата по чл. 5, т. 2;

7. разработва методика и правила за извършване на оценка за съответствие с мерките за мрежова и информационна сигурност, определени с наредбата по чл. 3, ал. 2;

8. координира, организира и провежда международни и национални учения и тренировки в областта на мрежовата и информационната сигурност.

Министър на отбраната. Началник на отбраната

Чл. 13. (1) Министърът на отбраната провежда държавната политика за защита и активно противодействие на кибератаки и хибридни въздействия върху системите за управление на отбраната и въоръжените сили. Министърът на отбраната организира подготовката за киберотбрана на системите за управление на страната при положение на война, военно положение и извънредно положение.

(2) Министърът на отбраната:

1. организира изграждането и развиването на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили, включително на център за киберотбрана и тяхното ресурсно осигуряване;

2. организира координацията и взаимодействието във връзка с изпълнението на поети ангажименти за колективна отбрана на споделеното киберпространство с Организацията на Северноатлантическия договор (НАТО) и Европейския съюз;

3. (изм. и доп. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) съвместно с министъра на вътрешните работи, министъра на електронното управление и председателя на Държавна агенция "Национална сигурност":

а) изготвя допълнителни изисквания по отношение на планирането и осъществяването на мероприятията по подготовка на киберотбраната и киберустойчивостта на страната при обявяване на извънредно положение, военно положение или положение на война и организира осъществяването на контрола за тяхното изпълнение;

б) организира изграждането, развиването и поддържането на потенциал за защита и активно противодействие, адекватно на съвременните предизвикателства и заплахи в киберпространството.

(3) Министърът на отбраната определя с наредба условията и реда за изграждане и поддържане на киберрезерв с цел повишаване на капацитета и способностите за киберотбрана във взаимодействие с научноизследователската и образователната общност и индустрията. Киберрезервът участва в съвместни обучения и тренировки и може да бъде включван при необходимост за решаване на практически задачи, свързани с киберотбраната.

(4) Началникът на отбраната:

1. организира поддържането на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили;

2. възлага интегрирането на задачите по киберотбрана като елемент от стратегическото планиране в плановете за изграждане на отбранителни способности и

в плановете за операции на въоръжените сили;

3. организира и координира провеждането на международни или национални занятия, тренировки и учения в областта на киберотбраната.

Министър на вътрешните работи

Чл. 14. (1) Министърът на вътрешните работи провежда държавната политика в областта на противодействието на киберпрестъпността.

(2) Органите на Министерството на вътрешните работи:

1. извършват оперативно-издирвателна дейност за противодействие на киберпрестъпността и произтичащите от нея заплахи за националната сигурност и за опазване на обществения ред;

2. поддържат и развиват способности за киберпревенция и защита, реакция, разследване и правоприлагане при компютърни престъпления;

3. усъвършенстват организационната база и способностите на органите за разкриване и разследване на престъпни дейности в киберпространството и осъществяват взаимодействие с всички заинтересовани страни;

4. осъществяват разследване при извършени компютърни престъпления, от които произтичат заплахи за националната сигурност и за опазване на обществения ред;

5. извършват дейности по повишаване на информираността на обществото за съществуващи и нововъзникващи киберзаплахи и свързания с тях риск от престъпни деяния.

(3) В Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи се изгражда:

1. Център по киберпрестъпност, който осъществява дейности по разкриване, разследване и документиране на компютърни престъпления на национално ниво, и

2. екип за реагиране при инциденти с компютърната сигурност за Министерството на вътрешните работи.

(4) В изпълнение на дейностите по ал. 2 и 3 Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи:

1. поддържа готовност за координирана, съвместна реакция с Националния екип за реагиране при инциденти с компютърната сигурност по чл. 19;

2. подпомага разследващите органи чрез изготвяне на дигитални експертни справки на веществени доказателства;

3. разполага с технически, финансови и човешки ресурси за гарантиране ефективното осъществяване на дейностите по ал. 2 и за изграждането на центъра по ал. 3, т. 1.

(5) При уведомяване от Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, са длъжни незабавно, когато това е технически възможно, да филтрират или преустановят зловредния интернет трафик - източник на кибератака, към мрежи и информационни системи на субектите по чл. 4,

ал. 1.

Държавна агенция "Национална сигурност"

Чл. 15. (1) Държавна агенция "Национална сигурност" изпълнява политиката по защита от киберинциденти в комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност.

(2) (Изм. - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г.) Държавна агенция "Национална сигурност" администрира и ползва Център за мониторинг и реакция на инциденти със значително увреждащо въздействие върху комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност.

(3) (В сила от 31.12.2023 г.) Центърът по ал. 2 изпълнява следните дейности:

1. мониторинг и събиране на информация за събития и инциденти, свързани със сигурността на комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност;

2. подаване на предупреждения за киберзаплахи и информация за киберинциденти към стратегическите обекти и дейности, които са от значение за националната сигурност;

3. оказване на методическо съдействие в процеса на управление на киберинциденти;

4. осигуряване на цялостен анализ на постъпващата информация и оценка на информационната защита на стратегическите обекти и дейности, които са от значение за националната сигурност.

(4) (В сила от 31.12.2023 г.) Центърът по ал. 2 поддържа готовност за координирана съвместна реакция в рамките на Националната координационно-организационна мрежа за киберсигурност при настъпването на инциденти, свързани със сигурността на комуникационните и информационните системи на стратегическите обекти и дейности, които са от значение за националната сигурност.

(5) (В сила от 31.12.2023 г.) Центърът по ал. 2 изпълнява и задачи, свързани с функциите на Държавна агенция "Национална сигурност" по чл. 6, ал. 5 от Закона за Държавна агенция "Национална сигурност".

(6) При уведомяване от Държавна агенция "Национална сигурност" ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности са длъжни незабавно, когато това е технически възможно, да филтрират или преустановят зловредния интернет трафик - източник на кибератака.

(7) (Нова - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г., изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Центърът по ал. 2 се изгражда и поддържа от Министерството на електронното управление.

Национални компетентни органи

Чл. 16. (1) Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи по мрежова и

информационна сигурност за секторите и услугите, посочени в приложения № 1 и 2, когато такива не са създадени със специален закон.

(2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Национален компетентен орган за всички административни органи, както и за лицата и организациите по чл. 4, ал. 1, т. 3 и 4, е Министерството на електронното управление.

(3) Националните компетентни органи:

1. координират и контролират изпълнението на задачите, свързани с мрежовата и информационната сигурност на административните органи, операторите на съществени услуги и доставчиците на цифрови услуги съгласно този закон;

2. (изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) приемат, след съгласуване с Министерството на електронното управление, насоки относно обстоятелствата, при които субектите по чл. 4, ал. 1 са длъжни да уведомяват за инциденти;

3. оценяват дали административните органи, операторите на съществени услуги и доставчиците на цифрови услуги изпълняват задълженията си по глава втора, както и въздействието на това изпълнение върху мрежовата и информационната сигурност и предприемат съответните мерки при неизпълнение;

4. съвместно с Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки по отношение на техническите области, които да се вземат предвид във връзка с използването на европейските или международните стандарти и спецификации от значение за мрежовата и информационната сигурност;

5. със съдействието на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора.

(4) Националните компетентни органи гарантират, че екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 получават уведомления за инциденти по този закон.

(5) Националните компетентни органи имат право да изискват от административните органи и от операторите на съществени услуги:

1. информация, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност, резултати от одити на мрежовата и информационната сигурност, когато са извършени от друг квалифициран одитор, и доказателствата, на които те се основават;

2. доказателства за ефективно изпълнение на препоръките от одити на мрежовата и информационната им сигурност.

(6) В искането по ал. 5 националните компетентни органи посочват целта му и уточняват каква информация или доказателства се изискват.

(7) След оценяването на информацията или на доказателствата по ал. 5 съответният национален компетентен орган дава при необходимост задължителни указания за отстраняване на установените пропуски в изпълнението на изискванията,

предвидени в глава втора.

(8) За целите на глава втора националните компетентни органи имат право да изискват от доставчиците на цифрови услуги да:

1. предоставят информацията, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност;

2. отстранят всеки пропуск в изпълнението на изискванията, предвидени в глава втора.

(9) Когато получи доказателства, че даден доставчик на цифрови услуги не отговаря на изискванията, установени в глава втора, съответният национален компетентен орган предприема действия съгласно правомощията си по ал. 8. Тези доказателства могат да се предоставят от компетентен орган на друга държава - членка на Европейския съюз, в която доставчикът на цифрови услуги предоставя услугата.

(10) Националните компетентни органи имат право да изискват от екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 информация по чл. 17, ал. 4, т. 1 и ал. 7.

(11) Националните компетентни органи оказват съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл. 17, ал. 2, 3, 4 и 7.

(12) Националните компетентни органи си сътрудничат с органите за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни.

(13) Националните компетентни органи трябва да разполагат с технически, финансови и човешки ресурси, за да гарантират, че са в състояние да изпълняват ефективно възложените им задачи в съответствие с този закон.

Национално единно звено за контакт

Чл. 17. (1) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национално единно звено за контакт.

(2) Националното единно звено за контакт координира въпросите, свързани с мрежовата и информационната сигурност, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави - членки на Европейския съюз.

(3) Националното единно звено за контакт предоставя на всеки две години на Европейската комисия информация относно последователността на подходите за определянето на операторите на съществени услуги, която включва:

1. националните мерки, чрез които са определени операторите на съществени услуги;

2. списък на съществените услуги;

3. броя на операторите на съществени услуги, определени за всеки сектор в приложение № 1, и тяхното значение за този сектор;

4. праговете, когато има такива, за определяне на минималното ниво на

доставяните услуги спрямо броя ползватели, разчитащи на тях;

5. значението на конкретния оператор на съществени услуги за поддържане на достатъчно ниво на услугата предвид наличието и на други възможности за предоставяне на тази услуга.

(4) Националното единно звено за контакт уведомява Европейската комисия за:

1. обхвата на задачите на екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19, както и за съществените елементи от тяхната процедура за предприемане на действия при инциденти, след тяхното създаване или при изменение на статута или процедурите им;

2. приетата Национална стратегия за мрежова и информационна сигурност в тримесечен срок от приемането ѝ.

(5) При трансграничен инцидент Националното единно звено за контакт уведомява националното единно звено за контакт на другата засегната държава - членка на Европейския съюз, когато е постъпило искане по чл. 19, ал. 2, т. 9 от Националния екип за реагиране при инциденти с компютърната сигурност.

(6) В случаите по ал. 5 Националното единно звено за контакт запазва търговските интереси на оператора на съществените услуги или на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомленията им, в съответствие с българското законодателство и с правото на Европейския съюз.

(7) Националното единно звено за контакт представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления по чл. 21, ал. 3, чл. 22, ал. 2, чл. 23, ал. 2 и чл. 25, ал. 3, естеството на инцидентите и действията, предприети за разрешаването им.

(8) Националното единно звено за контакт има право да изисква от националните компетентни органи информацията по ал. 3 и ал. 4, т. 1, а от Националния екип за реагиране при инциденти с компютърната сигурност - информацията по ал. 7.

(9) В случай на необходимост националните компетентни органи и Националното единно звено за контакт осъществяват сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни.

Секторни екипи за реагиране при инциденти с компютърната сигурност

Чл. 18. (1) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, включително Министерството на електронното управление, създават секторни екипи за реагиране при инциденти с компютърната сигурност. Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

(2) Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания:

1. да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки момент и да бъдат ясно посочени и добре известни на субектите по чл. 4, ал. 1 и на партньорите;

2. секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони;

3. да осигуряват непрекъснатост на дейността си чрез:

а) подходяща система за управление и разпределяне на заявките;

б) достатъчен персонал, който да е постоянно на разположение;

в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение;

4. изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и с българското законодателство.

(3) Секторните екипи за реагиране при инциденти с компютърната сигурност разполагат с ресурси за ефективно изпълнение на задачите си, които включват най-малко следното:

1. наблюдение на инциденти на национално равнище;

2. подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните субекти;

3. реакция при инциденти и оказване на методологическа помощ при разрешаване на инциденти - при поискване;

4. осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация.

(4) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди.

(5) С цел улесняване на сътрудничеството секторните екипи за реагиране при инциденти с компютърната сигурност насърчават възприемането и използването на общи практики за стандартизация за:

1. процедури за предприемане на действия при инциденти и рискове;

2. схеми за класификация на инциденти, рискове и информация.

(6) Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност, която се изгражда от секторните екипи и от Националния екип по чл. 19.

(7) Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон.

(8) Секторните екипи за реагиране при инциденти с компютърната сигурност

изпращат веднъж на три месеца обобщена статистическа информация до Националния екип за реагиране при инциденти с компютърната сигурност относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност.

(9) Секторните екипи за реагиране при инциденти с компютърната сигурност, обхващащи стратегически обекти и дейности, които са от значение за националната сигурност:

1. изграждат комуникационна свързаност с центъра по чл. 15, ал. 2, която се използва за подпомагане изпълнението на дейностите по чл. 15;

2. (В сила от 31.12.2023 г.) уведомяват незабавно центъра по чл. 15, ал. 2 за настъпилите инциденти.

(10) (В сила от 31.12.2023 г.) В случаите по ал. 9, т. 2 последващите действия на субектите по чл. 4, ал. 1 се координират с центъра по чл. 15, ал. 2 и със съответния секторен екип за реагиране при инциденти с компютърната сигурност.

Национален екип за реагиране при инциденти с компютърната сигурност

Чл. 19. (1) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национален екип за реагиране при инциденти с компютърната сигурност, който отговаря на изискванията на чл. 18, ал. 2.

(2) Националният екип за реагиране при инциденти с компютърната сигурност:

1. действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво;

2. подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност;

3. участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност;

4. обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост;

5. предоставя съвети и препоръки на органите на държавната власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност;

6. оказва експертна подкрепа на административните органи и на други юридически лица при изграждане, внедряване и поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област;

7. участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури;

8. при възникване на инциденти в мрежовата и информационната сигурност дава препоръчителни указания на административните органи, на националните компетентни органи и на секторните екипи за реагиране при инциденти с

компютърната сигурност;

9. информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този закон, и в случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване;

10. участва в международни мрежи за сътрудничество.

(3) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, оказват съдействие на Националния екип за реагиране при инциденти с компютърната сигурност за отстраняване на установени от него киберинциденти в техните мрежи и/или услуги.

Сътрудничество и координация

Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво.

(2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министерството на електронното управление координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция "Национална сигурност", Министерството на вътрешните работи и Министерството на отбраната.

(3) За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят със споразумение за взаимодействие между заинтересованите ведомства.

(4) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление може да създава междуведомствени оперативни групи с участието на ведомства, организации и институции, включително от частния сектор, имащи отношение към тези дейности.

(5) Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност - в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност.

Глава втора.
МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ

Задължения на административните органи по отношение на изискванията за сигурност и уведомяване

за инциденти

Чл. 21. (1) Административните органи осигуряват и отговарят за сигурността на използваните от тях мрежи и информационни системи.

(2) Административните органи предприемат:

1. подходящи и пропорционални мерки, които трябва да осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск;

2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на дейността им;

3. мерките, определени с наредбата по чл. 3, ал. 2.

(3) Административните органи уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност.

(4) Първоначално уведомяване се прави до два часа след констатирането на инцидента. Уведомленията се подават по образец съгласно наредбата по чл. 3, ал. 2 и съдържат информация, която дава възможност на секторния екип да определи евентуалното трансгранично въздействие на инцидента.

(5) В срок до 5 работни дни административният орган предоставя на секторния екип пълната информация за инцидента, определена с наредбата по чл. 3, ал. 2.

(6) При наличие на обосновано предположение, че докладваният инцидент може да се класифицира като компютърно престъпление, секторният екип уведомява Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи.

(7) Секторният екип запазва поверителността на информацията, съдържаща се в уведомленията.

Задължения на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, по отношение на изискванията за сигурност и уведомяване за инциденти

Чл. 22. (1) Лицата и организациите по чл. 4, ал. 1, т. 3 и 4 осигуряват и отговарят за мрежовата и информационната си сигурност при предоставянето на административни услуги по електронен път.

(2) Лицата и организациите по ал. 1 уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път. В тези случаи се прилага съответно чл. 21, ал. 4, 5 и 6.

(3) Секторният екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на лицата и организациите по ал. 1, както и поверителността на информацията, съдържаща се в уведомленията им.

Задължения на операторите на съществени услуги по отношение на изискванията за сигурност и уведомяване за инциденти

Чл. 23. (1) Операторите на съществени услуги предприемат:

1. подходящи и пропорционални мерки, които трябва да осигуряват ниво на

мрежова и информационна сигурност, съответстващо на съществуващия риск;

2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на предоставяните от тях съществени услуги;

3. мерките, определени с наредбата по чл. 3, ал. 2.

(2) Операторите на съществени услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях съществени услуги. В тези случаи се прилагат съответно чл. 21, ал. 4, 5 и 6.

(3) Когато оператор на съществени услуги разчита на доставчик на цифрови услуги, за да предоставя съществена услуга, операторът уведомява доставчика на цифрови услуги за всяко значително увреждащо въздействие върху непрекъснатостта на съществената услуга, дължащо се на инцидент, засягащ доставчика на цифрови услуги.

(4) Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на оператора на съществени услуги, както и поверителността на информацията, съдържаща се в уведомлението му.

Предоставяне на информация

Чл. 24. (1) Съответният екип за реагиране при инциденти с компютърната сигурност при поискване предоставя на подалия уведомление за инцидент административен орган, лице или организация по чл. 4, ал. 1, т. 3 и 4 и оператор на съществени услуги съответната информация във връзка с последващите действия по уведомлението, включително информация, която би спомогнала за предприемането на ефективни действия при инцидента.

(2) След консултация със съответния субект по ал. 1, подал уведомлението, съответният екип за реагиране при инциденти с компютърната сигурност може да информира обществеността за отделни инциденти, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент.

Задължения на доставчиците на цифрови услуги по отношение на изискванията за сигурност и уведомяване за инциденти

Чл. 25. (1) Доставчиците на цифрови услуги предприемат:

1. подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тях при предоставянето на територията на Република България на услугите, посочени в приложение № 2;

2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, върху предоставяните от тях на територията на Република България услуги, посочени в приложение № 2, с цел осигуряване на непрекъснатост на тези

услуги;

3. мерките, определени с наредбата по чл. 3, ал. 2.

(2) Мерките по ал. 1, т. 1 осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск, като са съобразени със:

1. сигурността на системите и съоръженията;

2. действията при инциденти;

3. управление на непрекъснатостта на дейностите;

4. наблюдение, одит и изпитване;

5. спазване на международни стандарти.

(3) Доставчиците на цифрови услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях цифрови услуги. В тези случаи се прилагат съответно чл. 21, ал. 4, 5 и 6.

(4) За определяне на въздействието на даден инцидент като съществено се вземат предвид:

1. броят ползватели, засегнати от инцидента, и по-специално ползвателите, които разчитат на услугата за предоставяне на собствените си услуги;

2. продължителността на инцидента;

3. географският обхват по отношение на областта, засегната от инцидента;

4. степента на нарушаване на функционирането на услугата;

5. степента на въздействие върху стопанските и обществените дейности.

(5) Доставчиците на цифрови услуги подават уведомление по ал. 3 само когато имат достъп до информацията, която е необходима, за да се оцени въздействието на инцидента като съществено съгласно ал. 4.

(6) След консултация със засегнатия доставчик на цифрови услуги съответният секторен екип за реагиране при инциденти с компютърната сигурност и когато е приложимо, органите или екип за реагиране при инциденти с компютърната сигурност на други засегнати държави - членки на Европейския съюз, може да информират обществеността за отделни инциденти или да изискат от доставчика на цифрови услуги да информира за това, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент или когато разкриването на инцидента е в интерес на обществеността поради други причини.

(7) Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомлението му.

Юрисдикция и териториалност по отношение на доставчик на цифрови услуги

Чл. 26. (1) Когато доставчик на цифрови услуги има седалище и адрес на управление или представител в Република България, но неговите мрежи и информационни системи са разположени в една или повече други държави - членки на Европейския съюз, съответният национален компетентен орган и компетентните органи на другите държави си сътрудничат и се подпомагат взаимно, ако е

необходимо. Помощта и сътрудничеството може да включват обмен на информация между съответните компетентни органи и искания за предприемане на действията по чл. 16, ал. 8.

(2) Доставчик на цифрови услуги, който не е установен в държава - членка на Европейския съюз, но предлага в Европейския съюз услугите, посочени в приложение № 2, определя свой представител в Европейския съюз. Представителят трябва да е установен в една от държавите - членки на Европейския съюз, в които се предлагат услугите. Когато представителят е със седалище и адрес на управление в Република България, се приема, че доставчикът на цифрови услуги е под юрисдикцията на Република България.

(3) Определянето на представител от доставчика на цифрови услуги не засяга съдебните производства, които биха могли да бъдат започнати срещу самия доставчик на цифрови услуги.

Уведомяване за инциденти от субекти извън посочените по чл. 4 ал. 1

Чл. 27. (1) Субекти извън посочените по чл. 4, ал. 1 може да уведомяват секторните екипи за реагиране при инциденти с компютърната сигурност за инциденти, които имат въздействие върху непрекъснатостта на предоставяните от тях услуги.

(2) При обработването на уведомленията секторните екипи за реагиране при инциденти с компютърната сигурност действат съгласно съответните разпоредби на тази глава, като уведомленията на субектите по чл. 4, ал. 1 се обработват с предимство пред уведомленията по ал. 1.

(3) Уведомленията по ал. 1 се обработват само когато това не представлява несъразмерна или неоправдана тежест.

Глава трета.
АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ

Отговорност за нарушения, свързани с уведомяване за инциденти

Чл. 28. (1) Административен орган, който не уведоми или уведоми след срока по чл. 21, ал. 4 секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на неговата дейност, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление, се наказва с глоба от 1000 до 10 000 лв.

(2) При повторно нарушение по ал. 1 наказанието е глоба от 2000 до 20 000 лв.

(3) На лице или организация по чл. 4, ал. 1, т. 3 и 4, която не уведоми или уведоми след срока по чл. 21, ал. 4 секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал.

4, изречение второ, в случай че деянието не съставлява престъпление, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

(4) При повторно нарушение по ал. 3 глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв.

(5) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на оператор на съществени услуги, който не уведоми или уведоми след срока по чл. 21, ал. 4 съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от него съществени услуги, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление.

(6) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на доставчик на цифрови услуги, който не уведоми или уведоми след срока по чл. 21, ал. 4 съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има съществено въздействие върху непрекъснатостта на предоставяните от него цифрови услуги, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление.

Отговорност за непредоставяне на информация или неизпълнение на указания

Чл. 29. (1) Административен орган, който не предостави информацията и доказателствата по чл. 16, ал. 5 или не изпълни задължителни указания по чл. 16, ал. 7, се наказва с глоба от 1000 до 10 000 лв.

(2) При повторно нарушение по ал. 1 наказанието е глоба от 2000 до 20 000 лв.

(3) Когато деянието по ал. 1 е извършено от оператор на съществени услуги, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

(4) При повторно нарушение по ал. 3 глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв.

(5) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на доставчик на цифрови услуги, който не предостави информацията по чл. 16, ал. 8, т. 1 или не отстрани пропуск по чл. 16, ал. 8, т. 2.

Отговорност за други нарушения

Чл. 30. (1) Длъжностно лице, което извърши или допусне извършването на друго нарушение по глава втора, се наказва с глоба от 1000 до 10 000 лв., освен ако деянието не съставлява престъпление.

(2) При повторно нарушение по ал. 1 наказанието е глоба от 1500 до 15 000 лв.

(3) На лице, което не изпълни задължение по чл. 14, ал. 5, чл. 15, ал. 6 и чл. 19, ал. 3, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв.

Установяване на нарушенията, издаване, обжалване и изпълнение на наказателните постановления

Чл. 31. (1) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Актовете за установяване на нарушения по този закон, извършени от административни органи, както и за нарушения по чл. 28, ал. 3 и 4 и по чл. 30, ал. 3 във връзка с чл. 19, ал. 3, се съставят от длъжностни лица, определени от министъра на електронното управление.

(2) Актовете за установяване на нарушения по този закон, извършени от оператори на съществени услуги или от доставчици на цифрови услуги, се съставят от длъжностни лица, определени от ръководителите на административните органи по чл. 16, ал. 1.

(3) Актовете за установяване на нарушения по чл. 30, ал. 3 във връзка с чл. 14, ал. 5 се съставят от длъжностни лица, определени от министъра на вътрешните работи.

(4) Актовете за установяване на нарушения по чл. 30, ал. 3 във връзка с чл. 15, ал. 6 се съставят от длъжностни лица, определени от председателя на Държавна агенция "Национална сигурност".

(5) Наказателните постановления се издават от:

1. (изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министъра на електронното управление или от изрично оправомощени от него длъжностни лица - в случаите по ал. 1;

2. ръководителите на административните органи по чл. 16, ал. 1 или от изрично оправомощени от тях длъжностни лица - в случаите по ал. 2;

3. министъра на вътрешните работи или от изрично оправомощени от него длъжностни лица - в случаите по ал. 3;

4. председателя на Държавна агенция "Национална сигурност" или от изрично оправомощени от него длъжностни лица - в случаите по ал. 4.

(6) Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на закона за административните нарушения и наказания.

Допълнителни разпоредби

§ 1. Този закон въвежда изискванията на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.).

§ 2. Този закон предвижда мерки по прилагане на Регламент за изпълнение (ЕС) 2018/151 на Комисията от 30 януари 2018 г. за определяне на правила за прилагане на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета по отношение на допълнителното уточняване на елементите, които трябва да се вземат предвид от доставчиците на цифрови услуги при управлението на рисковете за сигурността на мрежите и информационните системи, както и на показателите за

определяне на това дали даден инцидент има съществено въздействие (ОВ, L 26/48 от 31 януари 2018 г.).

§ 3. По смисъла на този закон:

1. "Административен орган" е понятието по смисъла на § 1, т. 1 от допълнителните разпоредби на закона за електронното управление.

2. "Група за сътрудничество" е групата по смисъла на чл. 11 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.).

3. "Действия при инцидент" са всички процедури, подпомагащи установяването, анализа и ограничаването на инцидент, както и реагирането на такъв инцидент.

4. "Длъжностно лице" е понятието по смисъла на чл. 93, т. 1 от Наказателния кодекс.

5. "Доставчик на DNS услуги" е субект, предоставящ DNS услуги по интернет. DNS (Domain Name System) е Система за имена на домейни, която представлява йерархично разпределена мрежова система за именуване на домейни, разпределяща заявки за имена на домейни.

6. "Доставчик на цифрови услуги" е юридическо лице, предоставящо цифрова услуга.

7. "Зловреден интернет трафик" са аномалии на интернет трафика, предизвикани от хардуерни или софтуерни повреди на интернет пакети със злоумишлено модифицирани опции.

8. "Информационна защита" е комплекс от организационни, юридически, технически и технологични мерки за мониторинг, анализ, активна превенция, намаляване влиянието на уязвимости, споделяне на информация за тях, включително отстраняване на последствията от инциденти.

9. "Инцидент със "значително увреждащо въздействие" се определя, като се вземат предвид следните показатели:

а) брой ползватели, разчитащи на услугите, предоставяни от субекта;

б) зависимост на други сектори - от посочените в приложение № 1, от услугата, предоставяна от субекта;

в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност;

г) пазарният дял на субекта;

д) географският обхват на областта, която би била засегната от даден инцидент;

е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга.

Когато е целесъобразно, се вземат предвид и характерните за сектора показатели, за да се определи дали даден инцидент би имал значително увреждащо

въздействие.

10. "Кибератака" е опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив.

11. "Киберзаплаха" е възможността за злонамерен опит да се повреди или прекъсне компютърната мрежа, системата, услугите и данните.

12. "Киберинцидент" е събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.

13. "Киберинцидент със значителен приоритет" е киберинцидент, който оказва сериозно въздействие върху дейността на правителството, върху предоставянето на съществени услуги на голяма част от българското население или върху икономиката на Република България.

14. "Киберинцидент с висок приоритет" е киберинцидент, който има сериозно въздействие върху голяма организация или върху по-широко/местно управление или който представлява значителен риск за предоставянето на съществените услуги на голяма част от българското население или върху икономиката на Република България.

15. "Киберинцидент със среден приоритет" е киберинцидент, който има сериозно въздействие върху средна организация или който представлява значителен риск за голяма организация или за по-широко/местно управление.

16. "Киберотбрана" е комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност.

17. "Киберпространство" е глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни.

18. "Киберрезерв" е допълнителен ресурс от експерти в областта на киберсигурността, защитата на информацията и информационните технологии с компетентности, свързани с осигуряване на защита и устойчивост на комуникационните и информационните системи.

19. "Компютърна услуга "в облак" е цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно.

20. "Лица, осъществяващи публични функции" е понятието по смисъла на § 1, т. 11 от допълнителните разпоредби на Закона за електронното управление.

21. "Мащабен инцидент" е налице, когато са регистрирани инциденти със среден приоритет в мрежите и информационните системи на повече от 4 от субектите по чл. 4, ал. 1, с висок приоритет в мрежите и информационните системи на повече от два от субектите по чл. 4, ал. 1 и със значителен приоритет на повече от един от

субектите по чл. 4, ал. 1. Класификацията на инциденти в зависимост от типа на атаката се определя по методика на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

22. "Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност" е мрежата по смисъла на чл. 12 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.).

23. "Мрежа и информационна система" е:

а) електронна съобщителна мрежа по смисъла на § 1, т. 15 от допълнителните разпоредби на Закона за електронните съобщения;

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или

в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви "а" и "б", с цел обработване, използване, защита и поддръжка.

24. "Онлайн място за търговия" е цифрова услуга, която дава на потребители или търговци по смисъла на § 13, т. 1 и 2 от допълнителните разпоредби на Закона за защита на потребителите възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия.

25. "Онлайн търсачка" е цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с исканото съдържание.

26. "Организация, предоставяща обществени услуги" е понятието по смисъла на § 1, т. 14 от допълнителните разпоредби на Закона за електронното управление.

27. "Повторно" е нарушението, извършено в срок една година от влизането в сила на наказателното постановление, с което на нарушителя е наложено наказание за същото по вид нарушение.

28. "Представител" е физическо или юридическо лице, установено в държава - членка на Европейския съюз, което е изрично определено да действа от името на доставчик на цифрови услуги, който не е установен в държава - членка на Европейския съюз, и към което национален компетентен орган или екип за реагиране при инциденти с компютърната сигурност може да се обърне вместо към доставчика на цифрови услуги във връзка със задълженията на доставчика на цифрови услуги по този закон.

29. "Регистър на имена на домейни от първо ниво" е субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от

първо ниво (top-level domain - TLD).

30. "Риск" е потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на информационните активи, за да се причини вреда.

31. "Съществени услуги" са услуги, които имат съществено значение за поддържането на особено важни обществени и/или стопански дейности в един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода или цифрова инфраструктура.

32. "Спецификация" е техническа спецификация по смисъла на чл. 2, т. 4 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ, L 316/12 от 14 ноември 2012 г.).

33. "Точка за обмен в интернет (ТОИ)" е мрежово средство, което дава възможност за свързване на повече от две независими автономни системи преди всичко с цел улесняване на обмена на интернет трафик. Чрез ТОИ се осъществява свързване само на автономни системи. Свързването чрез ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин.

34. "Уязвимост" е неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата.

35. "Цифрова услуга" е услуга по смисъла на чл. 1, параграф 1, буква "б" от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ, L 241/1 от 17 септември 2015 г.), от категориите, посочени в приложение № 2.

36. "Цифрова инфраструктура" е инфраструктура, която включва ТОИ, доставчици на DNS услуги и регистри на имената на домейни от първо ниво.

Преходни и Заключителни разпоредби

§ 4. Министерският съвет:

1. в срок до два месеца от влизането в сила на закона определя с решение административните органи по чл. 16, ал. 1 и приема методиката по чл. 4, ал. 3;

2. в срок до 6 месеца от влизането в сила на закона приема наредбата по чл. 3, ал. 2.

§ 5. (1) Административните органи по чл. 16, ал. 1:

1. в срок до два месеца от приемането на решението по § 4, т. 1 създават национални компетентни органи и секторните екипи към тях по чл. 18, ал. 1, както и привеждат устройствените правилници за дейността на администрациите си в съответствие със закона;

2. в срок до 5 месеца от приемането на решението по § 4, т. 1 определят операторите на съществени услуги и уведомяват председателя на Държавна агенция "Електронно управление" за това.

(2) В срок до 4 месеца от влизането в сила на закона Държавна агенция "Електронно управление" създава секторен екип по чл. 18, ал. 1 и привежда в съответствие със закона правилника по чл. 7а, ал. 3 от Закона за електронното управление.

§ 6. В Закона за електронните съобщения (обн., ДВ, бр. 41 от 2007 г.; изм., бр. 109 от 2007 г., бр. 36, 43 и 69 от 2008 г., бр. 17, 35, 37 и 42 от 2009 г.; Решение № 3 на Конституционния съд от 2009 г. - бр. 45 от 2009 г.; изм., бр. 82, 89 и 93 от 2009 г., бр. 12, 17, 27 и 97 от 2010 г., бр. 105 от 2011 г., бр. 38, 44 и 82 от 2012 г., бр. 15, 27, 28, 52, 66 и 70 от 2013 г., бр. 11, 53, 61 и 98 от 2014 г., бр. 14 от 2015 г.; Решение № 2 на Конституционния съд от 2015 г. - бр. 23 от 2015 г.; изм., бр. 24, 29, 61 и 79 от 2015 г., бр. 50, 95, 97 и 103 от 2016 г., бр. 58, 85 и 101 от 2017 г. и бр. 7, 21, 28 и 77 от 2018 г.) в чл. 243б, ал. 4 след думата "съобщенията" се добавя "и Националния екип за реагиране при инциденти с компютърната сигурност по чл. 19, ал. 1 от Закона за киберсигурност".

§ 7. В Закона за електронната търговия (обн., ДВ, бр. 51 от 2006 г.; изм., бр. 105 от 2006 г., бр. 41 от 2007 г., бр. 82 от 2009 г., бр. 77 и 105 от 2011 г. и бр. 57 от 2015 г.) в чл. 16, ал. 3 накрая се поставя запетая и се добавя "като с оглед на бързината и неотложността на кибератака, киберинцидент или киберкриза комуникацията да става по електронен път, достатъчно надеждно защитен".

§ 8. В Закона за електронното управление (обн., ДВ, бр. 46 от 2007 г.; изм., бр. 82 от 2009 г., бр. 20 от 2013 г., бр. 40 от 2014 г., бр. 13, 38, 50, 62 и 98 от 2016 г. и бр. 88 от 2018 г.) се правят следните изменения и допълнения:

1. В чл. 7в:

а) в т. 1 буква "г" се отменя;

б) точка 6 се отменя;

в) в т. 12 думите "мрежова и информационна сигурност" и запетаята преди тях се заличават;

г) създава се т. 27:

"27. осъществява правомощията по Закона за киберсигурност."

2. В чл. 7к, ал. 2 т. 3 се отменя.

3. В чл. 43, ал. 2 думите "и мрежова съвместимост и информационна сигурност" се заменят със "съвместимост".

4. В глава четвърта раздел III с чл. 54, 55 и 55а се отменя.

5. В чл. 56, ал. 1 думите "на този закон" се заличават, а накрая се добавя "по този закон и по Закона за киберсигурност".

6. В чл. 57, ал. 1 думите "и мрежова и информационна сигурност" се заличават.

7. В чл. 60:

а) в заглавието думите "и мрежова и информационна сигурност" се заличават;

б) в ал. 1 думите "мрежова и информационна сигурност и" се заличават;

в) в ал. 2 думите "информационната сигурност и" се заличават.

8. В § 1 от допълнителните разпоредби т. 10 се изменя така:

"10. "Мрежова и информационна сигурност" е понятието по смисъла на чл. 2, ал. 3 от Закона за киберсигурност."

§ 9. В Закона за управление и функциониране на системата за защита на националната сигурност (ДВ, бр. 61 от 2015 г.) в чл. 9, т. 1, буква "ж" думите "информационната сигурност" се заменят с "мрежовата и информационната сигурност".

§ 10. В Закона за изменение и допълнение на Изборния кодекс (обн., ДВ, бр. 39 от 2016 г.; изм., бр. 85 от 2017 г.) в § 145, ал. 14, т. 27 от преходните и заключителните разпоредби думите "чл. 43, ал. 2 от Закона за електронното управление" се заменят с "чл. 3, ал. 2 от Закона за киберсигурност".

§ 11. (В сила от 01.10.2018 г.) В Закона за мерките срещу изпирането на пари (ДВ, бр. 27 от 2018 г.) в § 9 от преходните и заключителните разпоредби навсякъде думите "1 октомври 2018 г." се заменят с "31 януари 2019 г.".

§ 12. Министерският съвет в срок до 31 декември 2018 г. приема правилника за прилагане на Закона за мерките срещу изпирането на пари.

§ 13. Изпълнението на този закон се възлага на Министерския съвет.

§ 14. (Изм. - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г.) Член 15, ал. 3, 4 и 5 и чл. 18, ал. 9, т. 2 и ал. 10 влизат в сила от 31 декември 2023 г., а § 11 влиза в сила от 1 октомври 2018 г.

Законът е приет от 44-то Народно събрание на 31 октомври 2018 г. и е подпечатан с официалния печат на Народното събрание.

Заключителни разпоредби
КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ВОЕННОТО РАЗУЗНАВАНЕ

(ОБН. - ДВ, БР. 69 ОТ 2020 Г.)

§ 36. В Закона за киберсигурност (ДВ, бр. 94 от 2018 г.) навсякъде думите "Служба "Военна информация" се заменят със "Служба "Военно разузнаване".

Преходни и Заключителни разпоредби
КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА МИНИСТЕРСТВОТО НА ВЪТРЕШНИТЕ РАБОТИ

(ОБН. - ДВ, БР. 85 ОТ 2020 Г., В СИЛА ОТ 02.10.2020 Г.)

§ 13. Законът влиза в сила от 1 януари 2021 г. с изключение на:

1. параграфи 1, 3, § 4, т. 1 и § 10, които влизат в сила от 1 ноември 2020 г.;

2. параграф 2, § 4, т. 2 и § 11 и 12, които влизат в сила от деня на обнародването на закона в "Държавен вестник".

Преходни и Заключителни разпоредби
КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

(ОБН. - ДВ, БР. 15 ОТ 2022 Г., В СИЛА ОТ 22.02.2022 Г.)

§ 14. В Закона за киберсигурност (обн., ДВ, бр. 94 от 2018 г.; изм., бр. 69 и 85 от 2020 г.) се правят следните изменения и допълнения:

. . . . . .

4. Навсякъде в закона думите "председателя на Държавна агенция "Електронно управление" и "Държавна агенция "Електронно управление" се заменят съответно с "министъра на електронното управление" и "Министерството на електронното управление", а думите "председателят на Държавна агенция "Електронно управление" се заменят с "министърът на електронното управление".

. . . . . .

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

Преходни и Заключителни разпоредби

КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ПАЗАРИТЕ НА ФИНАНСОВИ ИНСТРУМЕНТИ

(ОБН. - ДВ, БР. 25 ОТ 2022 Г., В СИЛА ОТ 29.03.2022 Г.)

§ 94. Законът влиза в сила от деня на обнародването му в "Държавен вестник", с изключение на § 79, т. 1, 4 и т. 9, буква "а", които влизат в сила от 19 октомври 2022 г.

Приложение № 1 към чл. 4, ал. 1, т. 2

(Изм. - ДВ, бр. 25 от 2022 г., в сила от 29.03.2022 г.)

Списък на секторите и подсекторите по чл. 4, ал. 1, т. 2

Сектор	Подсектор	Категория субект	Съответствие
1. Енергетика	а) електроенергия	- Електроенергийни предприятия по смисъла на чл. 2, т. 35 от Директива 2009/72/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ, L 211/55 от 14 август 2009 г.) са предприятия, които изпълняват функцията "доставка" по смисъла на чл. 2, т. 19 от посочената директива	- "Енергийно предприятие" по смисъла на § 1, т. 24 от допълнителните разпоредби на Закона за енергетиката - "Доставка" по смисъла на § 1, т. 16 от допълнителните разпоредби на Закона за енергетиката
		- Оператори на разпределителна система по смисъла на чл. 2, т. 6 от Директива 2009/72/ЕО на Европейския парламент и на	- "Оператор на разпределителна мрежа" по смисъла на § 1, т. 34б от допълнителните разпоредби на

		Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ, L 211/55 от 14 август 2009 г.)	Закона за енергетиката - "Оператор на съоръжение за втечнен природен газ" по смисъла на § 1, т. 34в от допълнителните разпоредби на Закона за енергетиката - "Оператор на съоръжение за съхранение" по смисъла на § 1, т. 34г от допълнителните разпоредби на Закона за енергетиката
		- Оператори на преносна система по смисъла на чл. 2, т. 4 от Директива 2009/72/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ, L 211/55 от 14 август 2009 г.)	- "Оператор на преносна мрежа" по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката
	б) нефт	- Оператори на нефтопроводи	
		- Оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт	

	в) природен газ	- Предприятия за доставка по смисъла на чл. 2, т. 8 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	- "Краен снабдител" по смисъла на § 1, т. 28а от допълнителните разпоредби на Закона за енергетиката
		- Оператори на газоразпределителна система по смисъла на чл. 2, т. 6 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	- "Оператор на разпределителна мрежа" по смисъла на § 1, т. 34б от допълнителните разпоредби на Закона за енергетиката
		- Оператори на газопреносна система по смисъла на чл. 2, т. 4 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	- "Оператор на преносна мрежа" по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката
		- Оператори на система за съхранение по смисъла на чл. 2, т. 10 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13	- "Оператор на съоръжение за съхранение" по смисъла на § 1, т. 34г от

		юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	допълнителните разпоредби на Закона за енергетиката
		- Оператори на система за втечнен природен газ по смисъла на чл. 2, т. 12 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	- "Оператор на съоръжение за втечнен природен газ" по смисъла на § 1, т. 34в от допълнителните разпоредби на Закона за енергетиката
		- Предприятия за природен газ по смисъла на чл. 2, т. 1 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	- "Производител" по смисъла на § 1, т. 46 от допълнителните разпоредби на Закона за енергетиката
		- Оператори на съоръжения за рафиниране и преработка на природен газ	
2. Транспорт	а) въздушен транспорт	- Въздушни превозвачи по смисъла на чл. 3, т. 4 от Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г.	

		относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ, L 97/72 от 9 април 2008 г.)	
		- Управляващи летищата органи по смисъла на чл. 2, т. 2 от Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 г. относно летищните такси (ОВ, L 70/11 от 14 март 2009 г.) - Летища по смисъла на чл. 2, т. 1 от Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 г. относно летищните такси (ОВ, L 70/11 от 14 март 2009 г.), включително летища, изброени в раздел 2 от приложение II към Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. относно насоките на Съюза за развитието на трансевропейската транспортна мрежа и за отмяна на Решение № 661/2010/ЕС (ОВ, L 348/1 от 20 декември 2013 г.), както и субекти, които експлоатират помощни инсталации, намиращи се в рамките на летището	- "Летищна администрация" по смисъла на § 3, т. 15 от допълнителните разпоредби на Закона за гражданското въздухоплаване - "Летищен оператор" по смисъла на § 3, т. 16 от допълнителните разпоредби на Закона за гражданското въздухоплаване - "Летище" по смисъла на § 3, т. 13 от допълнителните разпоредби на Закона за гражданското въздухоплаване

		- Оператори по контрола на управлението на движението, осъществяващи обслужване по контрол на въздушното движение по смисъла на чл. 2, т. 1 от Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за определяне на рамката за създаването на Единно европейско небе (рамков регламент) (ОВ, L 96/1 от 31 март 2004 г.)	- "Управление на въздушното движение" по смисъла на § 3, т. 44 от допълнителните разпоредби на Закона за гражданското въздухоплаване
	б) железопътен транспорт	- Управители на инфраструктура по смисъла на чл. 3, т. 2 от Директива 2012/34/ЕС на Европейския парламент и на Съвета от 21 ноември 2012 г. за създаване на единно европейско железопътно пространство (ОВ, L 343/32 от 14 декември 2012 г.)	- "Управител на железопътна инфраструктура" по смисъла на § 1, т. 2 от допълнителните разпоредби на Закона за железопътния транспорт
		- Железопътни предприятия по смисъла на чл. 3, т. 1 от Директива 2012/34/ЕС на Европейския парламент и на Съвета от 21 ноември 2012 г. за създаване на единно европейско железопътно пространство (ОВ, L 343/32 от 14 декември 2012 г.), включително оператори на обслужващи съоръжения по смисъла на чл. 3, т. 12 от посочената директива	- "Железопътно предприятие" по смисъла на чл. 48 от Закона за железопътния транспорт - "Оператор на обслужващо съоръжение" по смисъла на § 1, т. 51 от допълнителните разпоредби на Закона за

			железопътния транспорт
	в) воден транспорт	- Предприятия за вътрешноводен, морски и крайбрежен транспорт на пътници и товари по смисъла на приложение I към Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ, L 129/6 от 29 април 2004 г.), с изключение на отделните кораби, експлоатирани от тези предприятия	- "Компания" по смисъла на § 1, т. 12 от допълнителните разпоредби на Наредбата за условията и реда за постигане сигурността на корабите, пристанищата и пристанищните райони (ДВ, бр. 99 от 2014 г.)
		- Управителните органи на пристанища по смисъла на чл. 3, т. 1 от Директива 2005/65/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 г. за повишаване на сигурността на пристанищата (ОВ, L 310/28 от 25 ноември 2005 г.), включително техните пристанищни съоръжения по смисъла на чл. 2, т. 11 от Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ, L 129/6 от 29 април 2004 г.), както и субекти,	- "Пристанище" по смисъла на чл. 92, ал. 1 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България - Чл. 117, ал. 1 и чл. 117а, ал. 1, 2, 3 и 4 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България

		експлоатиращи инсталации и оборудване, разположено в рамките на пристанището	
		- Оператори на службата по морския трафик по смисъла на чл. 3, буква "о" от Директива 2002/59/ЕО на Европейския парламент и на Съвета от 27 юни 2002 г. за създаване на система на Общността за контрол на движението на корабите и за информация и отменяща Директива 93/75/ЕИО на Съвета (ОВ, L 208/10 от 5 август 2002 г.)	- Чл. 244а, ал. 1 и 2 от Кодекса на търговското корабоплаване - Чл. 115м, ал. 1, т. 12, 13, 14 и 15 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България
	г) автомобилен транспорт	- Пътни органи по смисъла на чл. 2, т. 12 от Делегиран регламент (ЕС) 2015/962 на Комисията от 18 декември 2014 г. за допълване на Директива 2010/40/ЕС на Европейския парламент и на Съвета по отношение на предоставянето в целия ЕС на информационни услуги в реално време за движението по пътищата (ОВ, L 157/21 от 23 юни 2015 г.), които отговарят за контрола на управлението на движението	
		- Оператори на интелигентни транспортни системи по смисъла на чл. 4, т. 1 от Директива 2010/40/ЕС на	- "Интелигентни транспортни системи" по смисъла на § 1, т.

		Европейския парламент и на Съвета от 7 юли 2010 г. относно рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и за интерфейси с останалите видове транспорт (ОВ, L 207/1 от 6 август 2010 г.)	40 от допълнителните разпоредби на Закона за автомобилните превози
3. Банково дело		- Кредитни институции по смисъла на чл. 4, параграф 1, т. 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и за изменение на Регламент (ЕС) № 648/2012 (ОВ, L 176/1 от 27 юни 2013 г.)	
4. Инфраструктури на финансовия пазар		- Оператори на местата за търговия по смисъла на чл. 4, параграф 1, т. 24 от Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС (ОВ, L 173/349 от 12 юни 2014 г.)	Закона за пазарите на финансови инструменти
		- Централни контрагенти по смисъла на чл. 2, т. 1 от	

		Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ, L 201/1 от 27 юли 2012 г.)	
5. Здравеопазване	Здравни заведения, включително болници и частни клиники	- Доставчици на здравно обслужване по смисъла на чл. 3, буква "ж" от Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ, L 88/45 от 4 април 2011 г.)	- Чл. 21, ал. 1, 2 и 3 от Закона за здравето - Чл. 2, ал. 1, чл. 5, ал. 1, чл. 8, ал. 1, чл. 9, ал. 1, 2 и 3, чл. 10 от Закона за лечебните заведения
6. Доставка и снабдяване с питейна вода		- Доставчици и снабдители с води, предназначени за консумация от човека по смисъла на чл. 2, § 1, буква "а" от Директива 98/83/ЕО на Съвета от 3 ноември 1998 г. относно качеството на водите, предназначени за консумация от човека (ОВ, L 330/32 от 5 декември 1998 г.), с изключение на снабдителите, за които снабдяването с води, предназначени за консумация от човека, е само част от общата им дейност за снабдяване с блага и стоки, които не се считат за съществени услуги	Допълнителните разпоредби на Наредба № 9 от 2001 г. за качеството на водата, предназначена за питейно-битови цели (ДВ, бр. 30 от 2001 г.)

7. Цифрова инфраструктура	- Точка за обмен в интернет (ТОИ)	
	- Доставчици на DNS услуги	
	- Регистри на имената на домейни от първо ниво	

Приложение № 2 към чл. 4, ал. 1, т. 2

Видове цифрови услуги

1. Онлайн място за търговия.
2. Онлайн търсачка.
3. Компютърни услуги "в облак".

Релевантни актове от Европейското законодателство

Директиви:

ДИРЕКТИВА (ВС) 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

ДИРЕКТИВА (ЕС) № 2015/1535 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество

Регламенти:

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2018/151 НА КОМИСИЯТА от 30 януари 2018 г. за определяне на правила за прилагане на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета по отношение на допълнителното уточняване на елементите, които трябва да се вземат предвид от доставчиците на цифрови услуги при управлението на рисковете за сигурността на мрежите и информационните системи, както и на показателите за определяне на това дали даден инцидент има съществено въздействие

РЕГЛАМЕНТ (ЕС) № 1025/2012 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО,

95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета