ЗАКОН за киберсигурност

Обн. - ДВ, бр. 94 от 13.11.2018 г.; изм., бр. 69 от 04.08.2020 г.; изм. и доп., бр. 85 от 02.10.2020 г., в сила от 02.10.2020 г.; изм. и доп., бр. 15 от 22.02.2022 г., в сила от 22.02.2022 г.; изм., бр. 25 от 29.03.2022 г., в сила от 29.03.2022 г.; изм. и доп., бр. 17 от 13.02.2026 г.

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Предмет

Чл. 1. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Този закон урежда дейностите по:

1. (изм. - ДВ, бр. 17 от 2026 г.) организацията, управлението и контрола на киберсигурността, координация и сътрудничество в областта на киберотбраната и противодействието на киберпрестъпността;

2. (изм. - ДВ, бр. 17 от 2026 г.) предприемане на необходимите мерки за постигане на високо общо ниво на киберсигурност в Република България.

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

Киберсигурност. Мрежова и информационна сигурност

Чл. 2. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Киберсигурност означава дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и на други лица, засегнати от киберзаплахи.

(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 високо общо ниво на киберсигурност

Чл. 3. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Мерките за високо общо ниво на киберсигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите по чл. 4 и 4а и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране.

(2) (Изм. - ДВ, бр. 17 от 2026 г.) Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4 и 4а с изключение на посочените в чл. 4, т. 3, буква „а", 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) (Изм. - ДВ, бр. 17 от 2026 г.) Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4, т. 3, букви „а" и „б" и приложение II, т. 1 се определят с наредба на Министерския съвет по предложение на Комисията за регулиране на съобщенията и на министъра на електронното управление. Мерките не може да налагат използването на определен тип технология.

(4) (Изм. - ДВ, бр. 17 от 2026 г.) Наредбите по ал. 2 и 3 не се прилагат за ведомствата по чл. 5, т. 2.

Обхват

Чл. 4. (Изм. - ДВ, бр. 17 от 2026 г.) С този закон се определят изискванията към:

1. административните органи;

2. публични и частни субекти от видовете, посочени в приложение I или II, които отговарят на критериите за средни предприятия съгласно чл. 3, ал. 1 от Закона за малките и средни предприятия или надхвърлят определената в него горна граница за

средни предприятия и които предоставят своите услуги или извършват дейности в рамките на Европейския съюз; при установяване размера на предприятието не се прилага чл. 4, ал. 9 от Закона за малките и средните предприятия;

3. субекти от видовете, посочени в приложение I или II, независимо от размера на предприятието, когато:

а) услугите се предоставят от доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги;

б) услугите се предоставят от доставчици на удостоверителни услуги;

в) услугите се предоставят от регистри на имена на домейни от първо ниво и доставчици на системни услуги за имена на домейни;

г) субектът е единствен доставчик на услуга, която е от съществено значение за поддържането на критични обществени и икономически дейности;

д) смущение (за определено време) в предоставяната от субекта услуга би могло да окаже значително въздействие върху обществената безопасност, обществената сигурност или общественото здраве;

е) смущение в предоставяната от субекта услуга би могло да предизвика значителен системен риск, по-специално за секторите, в които такова смущение би могло да има трансгранично въздействие;

ж) субектът е критичен поради своята специфична значимост на национално или регионално равнище за конкретния сектор или вид услуга или за други взаимозависими сектори в Република България;

4. субекти, установени като критични субекти съгласно Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ L 333/164 от 27 декември 2022 г.), наричана по нататък „Директива (ЕС) 2022/2557";

5. субекти, предоставящи услуги за регист-рация на имена на домейни;

6. образователни институции, когато извършват научноизследователски дейности от критично значение в секторите по приложение I и приложение II;

7. лицата, осъществяващи публични функции, които не са определени като съществени или важни субекти на друго основание, когато предоставят административни услуги по електронен път;

8. организациите, предоставящи обществени услуги, които не са съществени или важни субекти на друго основание, когато предоставят административни услуги по електронен път;

9. органите на съдебната власт.

Съществени и важни субекти

Чл. 4а. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* За целите на закона съществени субекти са:

1. субекти от видовете, посочени в приложение I, които надхвърлят горната граница за средни предприятия, установени в чл. 3, ал. 1 от Закона за малките и средните предприятия;

2. доставчици на квалифицирани удостоверителни услуги и регистри на имена на домейни от първо ниво, както и доставчици на DNS услуги, независимо от техния размер;

3. доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги, които отговарят на критериите за средни предприя-тия по смисъла на чл. 3, ал. 1 от Закона за малките и средните предприятия;

4. субектите по чл. 4, т. 1;

5. всички други субекти от видовете, посочени в приложение I или II, които са установени като съществени субекти съгласно чл. 4, т. 3, букви „г" - „ж";

6. субектите, посочени в чл. 4, т. 4;

7. определените като оператори на съществени услуги към датата на влизане в сила на настоящия закон.

(2) За целите на закона субектите от видовете, посочени в приложение I или II, които не отговарят на критериите за съществени субекти съгласно ал. 1, се считат за важни субекти. В това число се включват субекти, установени като важни субекти съгласно чл. 4, т. 3, букви „г" - „ж".

Изключения

Чл. 5. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) 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. и доп. - ДВ, бр. 17 от 2026 г.) за мрежите и информационните системи на Министерството на отбраната и структурите на пряко подчинение на министъра на отбраната и Българската армия, Министерството на вътрешните работи, Държавна агенция „Национална сигурност", Държавна агенция „Разузнаване", Държавна агенция „Технически операции", Комисията за противодействие на корупцията 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. (отм. - ДВ, бр. 17 от 2026 г.);

4. (отм. - ДВ, бр. 17 от 2026 г.);

5. (отм. - ДВ, бр. 17 от 2026 г.);

Регистър

Чл. 6. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Министърът на електронното управление създава, води и поддържа регистър на субектите по чл. 4 и 4а, който съдържа следната информация:

1. наименованието на субекта;

2. адрес и актуални данни за контакт, включително адреси на електронната поща и телефонни номера;

3. IP обхвати;

4. когато е приложимо, съответния сектор, подсектор и вид субект, както е посочено в приложение I или II;

5. когато е приложимо, списък на държавите членки, в които те предоставят услуги, попадащи в обхвата на този закон;

6. когато е приложимо, данни за контакт на представителя, определен съгласно чл. 27а, ал. 2.

(2) Доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, субектите, предоставящи услуги за регистриране на имена на домейни, доставчиците на компютърни услуги в облак, доставчиците на услуги на центрове за данни, доставчиците на мрежи за предоставяне на съдържание, доставчиците на управлявани услуги, доставчиците на управлявани услуги за сигурност, както и доставчиците на онлайн места за търговия, на онлайн търсачки и на платформи на услуги за социални мрежи предоставят на националните компетентни органи по чл. 16 информация за адреса на основното място на установяване и на останалите законови места на установяване на територията на Европейския съюз или, при липсата на място на установяване в Европейския съюз, на неговия представител, определен съгласно чл. 27а, ал. 2, до два месеца от възникването им.

(3) Субектите, посочени в ал. 1 и 2, уведомяват съответния национален компетентен орган по чл. 16 за всяка настъпила промяна в данните, предоставени съгласно ал. 1 и 2, в срок до две седмици от датата на промяната. Националните компетентни органи препращат получената информация на министъра на електронното управление и Националното единно звено за контакт в срок до една седмица от постъпването ѝ.

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

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

Специални закони за сектора

Чл. 6а. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Когато в специален закон съществува изискване съществените или важните субекти да приемат мерки за управление на риска в областта на киберсигурността или да уведомяват за значителни инциденти и когато тези изисквания имат най-малко равностоен ефект на предвидените в закона задължения, съответните разпоредби на закона, включително разпоредбите относно надзора и правоприлагането, не се прилагат за такива субекти. Когато в специален закон не са обхванати всички субекти в конкретен сектор, попадащ в обхвата на настоящия закон, съответните му разпоредби продължават да се прилагат по отношение на субектите, които не са обхванати от тези специални закони.

(2) Изискванията, посочени в ал. 1, се считат за равностойни по ефект на задълженията, предвидени в този закон, когато:

1. мерките за управление на риска в областта на киберсигурността са най-малкото равностойни по сила на мерките, определени в чл. 22, или

2. в специален закон се предвижда незабавен, по целесъобразност автоматичен и пряк достъп до уведомленията за инциденти на екипа за реагиране при инциденти с компютърната сигурност (ЕРИКС), националните компетентни органи или единните звена за контакт съгласно настоящия закон и когато изискванията за уведомяване за значителни инциденти са най-малко равностойни на предвидените в чл. 24.

Система за киберсигурност

Чл. 7. (Изм. - ДВ, бр. 17 от 2026 г.) *(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) (Изм. - ДВ, бр. 17 от 2026 г.) Министерският съвет приема с решение Национална стратегия за киберсигурност.

Стратегии

Чл. 8. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Националната стратегия за киберсигурност е стратегическа рамка на политиката за киберсигурност, която предвижда стратегическите цели, необходимите ресурси за постигане на тези цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на киберсигурност. Националната стратегия за киберсигурност включва:

1. целите и приоритетите, като се обхващат по-специално секторите, посочени в приложения I и II;

2. рамка за управление за постигане на целите и приоритетите, посочени в т. 1, включително посочените в ал. 2 политики;

3. рамка за управление, в която се изясняват ролите и отговорностите на съответните заинтересовани страни на национално равнище и която е в основата на сътрудничеството и координацията на национално равнище между националните компетентни органи, единните звена за контакт и ЕРИКС съгласно закона, както и координацията и сътрудничеството между тези органи и националните компетентни органи съгласно специфичните европейски правни актове;

4. механизъм за установяване на относимите активи и оценка на риска на ниво държава;

5. мерките, гарантиращи подготвеността, реагирането и възстановяването при инциденти, включително сътрудничеството между публичния и частния сектор;

6. списък с различните органи и заинтересовани страни, които участват в прилагането на Националната стратегия за киберсигурност;

7. рамка на политика за засилена координация между националните компетентни органи съгласно закона и компетентни органи съгласно Директива (ЕС) 2022/2557 - за целите на обмена на информация за рискове, киберзаплахи и инциденти, както и за несвързани с киберпространството рискове, заплахи и инциденти, и упражняването на надзорни задачи, по целесъобразност;

8. план, включващ необходимите мерки за укрепване на общото равнище на осведоменост на гражданите относно киберсигурността.

(2) Като част от Националната стратегия за киберсигурност министърът на електронното управление провежда политиките:

1. за киберсигурността по веригата за доставки на ИКТ продукти и услуги, използвана от субектите за предоставянето на техните услуги;

2. относно включването и посочването на изискванията, свързани с киберсигурността за ИКТ продуктите и ИКТ услугите, при възлагането на обществени поръчки, включително във връзка със сертифициране в областта на киберсигурността, криптиране и използване на продукти за киберсигурност с отворен код;

3. по управление на уязвимостите, включващо насърчаването и улесняването на координираното оповестяване на уязвимости съгласно Европейската база данни за уязвимости на Агенцията на Европейския съюз за киберсигурност (ENISA);

4. свързани с поддържането на общата наличност, цялостност и поверителност на общественото ядро на отворения интернет, включително, когато е целесъобразно, киберсигурността на подводните комуникационни кабели;

5. свързани с насърчаване на разработването и внедряването на съответните авангардни технологии, насочени към прилагане на най-съвременни мерки за управление на риска в областта на киберсигурността;

6. свързани с насърчаване и развитие на образованието и обучението в областта на киберсигурността, уменията, повишаването на осведомеността и инициативите за научноизследователска и развойна дейност в областта на киберсигурността, както и насоки за добри практики и механизми за контрол в областта на киберхигиената, насочени към гражданите, заинтересованите страни и субектите;

7. по подпомагане на академичните и научноизследователските институции за разработване, подобряване и насърчаване на внедряването на инструменти за киберсигурност и сигурна мрежова инфраструктура;

8. по включване на съответни процедури и подходящи инструменти за обмен на информация, подпомагащи доброволния обмен на информация за киберсигурността между субектите;

9. по укрепване на киберустойчивостта и основните параметри за киберхигиена на малките и средните предприятия, по-специално на тези, които са изключени от обхвата на този закон, чрез предоставяне на леснодостъпни насоки и помощ за техните специфични нужди;

10. по насърчаване на активна киберзащита.

(3) Националната стратегия за киберсигурност се актуализира на всеки пет години въз основа на ключови показатели за ефективност.

Съвет по киберсигурността

Чл. 9. (Изм. и доп. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.; доп., бр. 17 от 2026 г.) *(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;

8б. (нова - ДВ, бр. 17 от 2026 г.) министърът на регионалното развитие и благоустройството;

8в. (нова - ДВ, бр. 17 от 2026 г.) министърът на земеделието и храните;

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. 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. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) 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. (доп. - ДВ, бр. 17 от 2026 г.) дава предложения към Министерския съвет за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото;

6. (изм. - ДВ, бр. 17 от 2026 г.) предлага на Министерския съвет Национален план за реакция при мащабни киберинциденти и кризи;

7. взаимодейства със Съвета по сигурността към Министерския съвет.

Национален координатор по киберсигурността

Чл. 11. (Изм. - ДВ, бр. 17 от 2026 г.) *(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. (изм. - ДВ, бр. 17 от 2026 г.) участва при изграждането и развитието на Националната координационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост;

3. (изм. - ДВ, бр. 17 от 2026 г.) участва в 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

Чл. 12. (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.; изм. и доп., бр. 17 от 2026 г.) Министърът на електронното управление:

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

2. (отм. - ДВ, бр. 17 от 2026 г.);

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. (изм. - ДВ бр. 17 от 2026 г.) осъществява проверки чрез оправомощени от него лица на информационната сигурност по смисъла на този закон и на предприетите от административния орган мерки според правомощията, описани в глава втора „в" и в глава трета, и дава задължителни предписания за тяхното подобряване; в обхвата на проверките не попадат информационни системи на ведомствата по чл. 5;

7. (изм. и доп. - ДВ бр. 17 от 2026 г.) разработва методика и правила за извършване на проверки за съответствие с мерките за мрежова и информационна сигурност, определени с наредбата по чл. 3, ал. 2 и 3;

8. (изм. - ДВ бр. 17 от 2026 г.) координира, организира и провежда международни и национални учения и тренировки в областта на киберсигурността.

9. (нова - ДВ, бр. 17 от 2026 г.) осъществява проверки на предоставените годишни одити от националните компетентни органи с цел анализ и съответствие с изискванията по този закон;

10. (нова - ДВ, бр. 17 от 2026 г.) определя ограничения за използване на приложения и интернет страници на служебните устройства, използвани от служителите в държавната администрация, от които произтича висок риск за информационните системи и мрежи на държавната администрация;

11. (нова - ДВ, бр. 17 от 2026 г.) издава задължителни разпореждания до националните компетентни органи относно спазването на изискванията на закона.

Министър на отбраната. Началник на отбраната

Чл. 13. (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) *(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. - 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. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) *(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) (Изм. и доп. - ДВ, бр. 17 от 2026 г.) 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. 4а. Министерството на вътрешните работи представя на ресорната комисия в Народното събрание доклад за извършените действия по преустановяване на интернет трафик веднъж на всеки 6 месеца.

Държавна агенция „Национална сигурност"

Чл. 15. (Изм. и доп. - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г.; изм. и доп., бр. 17 от 2026 г.) *(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.; изм., бр. 17 от 2026 г.) В Държавна агенция „Национална сигурност" се администрира, ползва и развива 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 01.01.2022 г.; влизане в сила изменено на 31.12.2023 г., бр. 85 от 2020 г., в сила от 02.10.2020 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 01.01.2022 г.; влизане в сила изменено на 31.12.2023 г., бр. 85 от 2020 г., в сила от 02.10.2020 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 01.01.2022 г.; влизане в сила изменено на 31.12.2023 г., бр. 85 от 2020 г., в сила от 02.10.2020 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) (Нова - ДВ, бр. 17 от 2026 г.) При настъпване на инцидент с критични системи на стратегическите обекти и дейностите от значение за националната сигурност ръководителите на субектите незабавно уведомяват центъра по ал. 2 по реда на чл. 23.

(7) (Предишна ал. 6 - ДВ, бр. 17 от 2026 г.) 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.

(8) (Нова - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г.; предишна ал. 7, изм., бр. 17 от 2026 г.) Ръководителите на стратегически обекти и възлагащите и извършващите стратегически дейности от значение за националната сигурност предприемат действия по осигуряване на автоматизиран обмен на данни между информационните системи за сигурност на ръководените от тях обекти и дейности и центъра по ал. 2.

Национални компетентни органи

Чл. 16. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Министерският съвет определя с решение административните органи, които изпълняват функциите на национални компетентни органи по киберсигурност за секторите и услугите, посочени в приложения I и II, когато такива не са създадени със специален закон.

(2) (Изм. - ДВ, бр. 17 от 2026 г.) Национален компетентен орган за всички административни органи, както и за лицата и организациите по чл. 4, т. 7 и 8, е Министерството на електронното управление.

(3) Националните компетентни органи:

1. (изм. - ДВ, бр. 17 от 2026 г.) координират и контролират изпълнението на задачите, свързани с киберсигурността на административните органи, и на всички други субекти съгласно този закон;

2. (изм. - ДВ, бр. 17 от 2026 г.) приемат, след съгласуване с Министерството на електронното управление, насоки относно обстоятелствата, при които субектите по чл. 4 и 4а са длъжни да уведомяват за инциденти;

3. (изм. - ДВ, бр. 17 от 2026 г.) оценяват дали административните органи, съществените и важните субекти по този закон изпълняват задълженията си по глава втора, както и въздействието на това изпълнение върху киберсигурността и предприемат съответните мерки при неизпълнение;

4. (изм. - ДВ, бр. 17 от 2026 г.) 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 киберсигурността;

5. (изм. - ДВ, бр. 17 от 2026 г.) изготвят препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора.

6. (нова - ДВ, бр. 17 от 2026 г.) изготвят ежегодна оценка на риска и икономическия и социалния ефект за прилежащия им сектор, която докладват на Националното единно звено за контакт;

7. (нова - ДВ, бр. 17 от 2026 г.) уведомяват Европейската комисия за идентификационните данни на секторния екип за реагиране при инциденти с компютърната сигурност (СЕРИКС) по чл. 18, ал. 1;

8. (нова - ДВ, бр. 17 от 2026 г.) определят съществените и важните субекти съгласно чл. 4а 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) 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) (Изм. - ДВ, бр. 17 от 2026 г.) Секторните екипи за реагиране при инциденти с компютърната сигурност към НКО си сътрудничат ефективно, ефикасно и сигурно чрез Националния екип за реагиране при инциденти с компютърната сигурност (НЕРИКС).

(6) (Отм. - ДВ, бр. 17 от 2026 г.).

(7) (Отм. - ДВ, бр. 17 от 2026 г.).

(8) (Отм. - ДВ, бр. 17 от 2026 г.).

(9) (Отм. - ДВ, бр. 17 от 2026 г.).

(10) (Изм. - ДВ, бр. 17 от 2026 г.) Националните компетентни органи 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. 9.

(11) (Изм. - ДВ, бр. 17 от 2026 г.) Националните компетентни органи оказват съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл. 17, ал. 2, 3, 4 и 9.

(12) (Изм. - ДВ, бр. 17 от 2026 г.) Националните компетентни органи си сътрудничат с Комисията за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни.

(13) (Изм. - ДВ, бр. 17 от 2026 г.) Националните компетентни органи:

1. участват в състава на надзорния форум по смисъла на чл. 32, параграф 4, буква „д" от Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ, L 333/1 от 27 декември 2022 г.), наричан по-нататък „Регламент (ЕС) 2022/2554";

2. оказват съдействие на компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554 и предоставят относими технически становища по тяхно искане;

3. сключват споразумения за сътрудничество с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554, чрез които се създават механизми за координация, включително за координиране на надзорните дейности по отношение на съществените или важните субекти, по смисъла на този закон, които са определени като трети страни, критични доставчици на услуги в областта на ИКТ, съгласно чл. 31 от същия регламент;

4. провеждат в съответствие с националното право проверки на място на трети страни, критични доставчици на услуги в областта на ИКТ, съгласно чл. 31 от Регламент (ЕС) 2022/2554, съвместно с компетентните органи по чл. 46 от същия регламент;

5. обменят информация с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554.

Национално единно звено за контакт

Чл. 17. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) *(1)* Към Министерството на електронното управление се създава Национално единно звено за контакт.

(2) (Изм. - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт координира въпросите, свързани с киберсигурността, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави - членки на Европейския съюз.

(3) (Изм. - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт организира и координира дейността по предоставяне на информацията по чл. 6, ал. 3 на всеки две години.

(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. (изм. - ДВ, бр. 17 от 2026 г.) приетата Национална стратегия за киберсигурността в тримесечен срок от приемането ѝ.

(5) (Нова - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт препраща информацията, посочена в чл. 6, ал. 1, с изключение на информацията по чл. 6, ал. 1, т. 3, на Агенцията на Европейския съюз за киберсигурност (ENISA).

(6) (Нова - ДВ, бр. 17 от 2026 г.) При получаване на информация за транс-граничен инцидент от Националното единно звено за контакт (НЕЗК) на друга държава членка НЕЗК уведомява съответните национални компетентни органи (НКО)/СЕРИКС и координира дейностите по разрешаване на инцидента на национално ниво, както и докладва резултатите на уведомяващия НЕЗК.

(7) (Предишна ал. 5 - ДВ, бр. 17 от 2026 г.) 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.

(8) (Предишна ал. 6, доп. - ДВ, бр. 17 от 2026 г.) В случаите по ал. 5 и 7 Националното единно звено за контакт запазва търговските интереси на съществените и важни субекти, както и поверителността на информацията, съдържаща се в уведомленията им, в съответствие с българското законодателство и с правото на Европейския съюз.

(9) (Предишна ал. 7, изм. - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления от съществените и важните субекти за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях услуги, естеството на инцидентите и действията, предприети за разрешаването им.

(10) (Предишна ал. 8, изм. - ДВ, бр. 17 от 2026 г.) 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. 9.

(11) (Нова - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт изготвя годишен обобщен доклад за оценка на риска, базиран на получените анализи от националните компетентни органи.

(12) (Нова - ДВ, бр. 17 от 2026 г.) Националното единно звено за контакт при целесъобразност обменя информация с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554.

(13) (Предишна ал. 9 - ДВ, бр. 17 от 2026 г.) 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.

Национални рамки за управление на кризи в областта на киберсигурността

Чл. 17а. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Компетентният орган, отговарящ за управлението на мащабните киберинциденти и кризи, е Съветът по киберсигурността.

(2) Съветът по ал. 1 приема национален план за реакция при мащабни киберинциденти и кризи, в който се определят целите, условията и редът за управлението на мащабни киберинциденти и кризи. По-конкретно в плана се установяват:

1. целите на националните мерки и дейности за подготвеност;

2. задачите и отговорностите на органите за управление на киберкризи;

3. процедурите за управление на киберкризи, включително тяхното интегриране в общата рамка за управление на кризи на национално равнище, и канали за обмен на информация;

4. националните мерки за подготвеност, включително дейности по учения и обучения;

5. съответните заинтересовани страни от публичния и частния сектор и съответната инфраструктура;

6. националните процедури и договорености между съответните национални органи и служби за осигуряване на ефективно участие и подкрепа за координираното управление на мащабни киберинциденти и кризи на равнището на Европейския съюз.

Секторни екипи за реагиране при инциденти с компютърната сигурност

Чл. 18. (Изм. - ДВ, бр. 85 от 2020 г., в сила от 02.10.2020 г.; изм. и доп., бр. 17 от 2026 г.) *(1)* (Изм. и доп. - ДВ, бр. 17 от 2026 г.) Административните органи по чл. 16, ал. 1 създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за киберсигурност (ENISA).

(2) (Нова - ДВ, бр. 17 от 2026 г.) Секторните екипи за реагиране при инциденти с компютърната сигурност:

1. си сътрудничат и, когато е подходящо, обменят относима информация в съответствие с чл. 27г със секторни и междусекторни общности на съществените и важните субекти;

2. участват в партньорски проверки, организирани в съответствие с чл. 20а;

3. могат да установяват отношения на сът-рудничество с НЕРИКС на трети държави, сътрудничество с цел ефективен, ефикасен и сигурен обмен на информация с тези НЕРИКС на трети държави, като използват съответните протоколи за обмен на информация, включително протокола за обмен на информация с цветен код за поверителност (Traffic Light Protocol); секторните екипи за реагиране при инциденти с компютърната сигурност могат да обменят съответна информация с НЕРИКС на трети държави, включително лични данни, в съответствие с правото на Европейския съюз в областта на защитата на данните;

4. при целесъобразност предоставят на компетентните органи, определени или създадени в съответствие с Регламент (ЕС) 2022/2554, експертна помощ в областта на разрешаване на киберинцидентите.

(3) (Предишна ал. 2, изм. и доп. - ДВ, бр. 17 от 2026 г.) 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) (изм. - ДВ, бр. 17 от 2026 г.) разполагат с достатъчно персонал, за да гарантират предоставянето по всяко време на техните услуги;

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

4. (изм. - ДВ, бр. 17 от 2026 г.) 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 киберсигурност (ENISA) и с българското законодателство.

(4) (Предишна ал. 3, изм. - ДВ, бр. 17 от 2026 г.) 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; наблюдение и анализ на киберзаплахи, уязвимости и 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;

5. извършване на проактивно неинвазивно сканиране на публично достъпни мрежови и информационни системи на съществени и важни субекти.

(5) (Предишна ал. 4 - ДВ, бр. 17 от 2026 г.) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди.

(6) (Предишна ал. 5, изм. - ДВ, бр. 17 от 2026 г.) С цел улесняване на сътрудничеството СЕРИКС 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.

(7) (Предишна ал. 6, изм. - ДВ, бр. 17 от 2026 г.) 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 НЕРИКС по чл. 19.

(8) (Предишна ал. 7 - ДВ, бр. 17 от 2026 г.) 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.

(9) (Предишна ал. 8, изм. - ДВ, бр. 17 от 2026 г.) Секторните екипи за реагиране при инциденти с компютърната сигурност изпращат всеки месец обобщена статистическа информация до НЕРИКС относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност.

(10) (Предишна ал. 9 - ДВ, бр. 17 от 2026 г.) 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 01.01.2022 г.; влизане в сила изменено на 31.12.2023 г., бр. 85 от 2020 г., в сила от 02.10.2020 г.) уведомяват незабавно центъра по чл. 15, ал. 2 за настъпилите инциденти.

(11) (В сила от 01.01.2022 г.; влизане в сила изменено на 31.12.2023 г., бр. 85 от 2020 г., в сила от 02.10.2020 г.; предишна ал. 10, изм., бр. 17 от 2026 г.) В случаите по ал. 10, 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. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Национален екип за реагиране при инциденти с компютърната сигурност отговаря на изискванията на чл. 18, ал. 1 - 6.

(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. (изм. - ДВ, бр. 17 от 2026 г.) при възникване на киберинциденти 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.

(4) (Нова - ДВ, бр. 17 от 2026 г.) Националният екип за реагиране при инциденти с компютърната сигурност осъществява функциите на координатор за целите на координираното оповестяване на уязвимости:

1. действа като доверен посредник, улес-няващ при необходимост взаимодействието между физическото или юридическото лице, докладващо за уязвимост, и производителя или доставчика на ИКТ продукти или ИКТ услуги, които са потенциално уязвими, при поискване от която и да е от страните;

2. задачите на координатора включват:

а) идентифициране и установяване на контакт със засегнатите субекти;

б) подпомагане на физическите или юридическите лица, докладващи за уязвимост, и

в) договаряне на срокове за оповестяване и управление на уязвимостите, които засягат множество субекти;

3. координираното оповестяване на уязвимости ще се извършва по утвърдена процедура от министъра на електронното управление.

Сътрудничество и координация

Чл. 20. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) *(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) 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) (Изм. - ДВ, бр. 17 от 2026 г.) 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.

(4) (Изм. и доп. - ДВ, бр. 17 от 2026 г.) За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление създава междуведомствена оперативна група с участието на ведомства, организации и институции, включително от частния и академичния сектор, имащи отношение към тези дейности.

(5) (Изм. - ДВ, бр. 17 от 2026 г.) Сътрудничеството на международно ниво се осъществява чрез:

1. Групата за сътрудничество;

2. Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност;

3. Европейската мрежа за връзка на организациите при киберкризи;

4. партньорски проверки;

5. по друг начин, предвиден в закон или международен договор, ратифициран със закон.

Партньорски проверки

Чл. 20а. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Министърът на електронното управление може да изпрати искане до Групата за сътрудничество и Агенцията на Европейския съюз за киберсигурност (ENISA) за извършването на партньорска проверка по Методика на Агенцията на Европейския съюз за киберсигурност (ENISA), която да обхваща един или повече от следните параметри:

1. степента на прилагане на мерките за управлението на риска в областта на киберсигурността и задълженията за докладване, предвидени в глава втора;

2. равнището на способностите, включително наличните финансови, технически и човешки ресурси, както и ефективността от изпълнението на задачите на националните компетентни органи;

3. оперативните способности на ЕРИКС;

4. степента на прилагане на взаимопомощта по чл. 27о, касаеща взаимопомощ и трансгранично сътрудничество;

5. степента на прилагане на договоренос-тите за обмен на информация в областта на киберсигурността, посочени в глава втора „б";

6. специфични въпроси от трансгранично или междусекторно естество.

(2) Преди започването на партньорската проверка проверяваният субект може да извърши самооценка на проверяваните аспекти и да предостави тази самооценка на експертите, определени да извършат партньорската проверка.

(3) Ръководителите на СЕРИКС и НЕРИКС могат да предложат на министъра на електронното управление да изпрати искане по реда на ал. 1.

Глава втора
МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА И ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ
(Загл. изм. - ДВ, бр. 17 от 2026 г.)

Управление

Чл. 21. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Управителните органи на съществените и важните субекти и административните органи одобряват мерките за управление на риска в областта на киберсигурността, предприети от тези субекти с цел спазване на чл. 22, и следят за прилагането им.

(2) Членовете на управителните органи на съществените и важните субекти са длъжни на всеки две години да преминават през обучение за придобиване на достатъчно познания и умения, което да им позволи да идентифицират рискове и да оценяват практиките за управление на риска в областта на киберсигурността и тяхното въздействие върху услугите, предоставяни от субекта.

(3) Членовете на управителните органи на съществените и важните субекти са длъжни да предлагат и организират обученията по ал. 2 и за своите служители.

Мерки за управление на риска в областта на киберсигурността

Чл. 22. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Съществените и важните субекти предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи в основната си дейност или при предоставяне на своите услуги. При спазване на принципа за технологична неутралност и като се вземат предвид последните постижения в тази област и, когато е приложимо, съответните европейски и международни стандарти, както и разходите за прилагането им, чрез мерките за управление на риска се гарантира ниво на сигурност на мрежовите и информационните системи, съответстващо на риска. При оценката на пропорционалността на тези мерки надлежно се вземат предвид степента на излагане на рискове на субекта, размерът на субекта и вероятността от възникване на инциденти, както и тяхната значимост, включително тяхното обществено и икономическо въздействие.

(2) Мерките по ал. 1 се основават на подход, обхващащ всички опасности, които имат за цел да защитят мрежовите и информационните системи и физическата среда на тези системи от инциденти, и включват следното:

1. политики за анализ на риска и сигурност на информационните системи;

2. действия при инцидент;

3. непрекъснатост на стопанската дейност, като управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи;

4. сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите преки снабдители или доставчици на услуги;

5. сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им;

6. политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността;

7. основни киберхигиенни практики и обучение в областта на киберсигурността;

8. политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране;

9. сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи;

10. използване на многофакторни решения за удостоверяване на автентичността или непрекъснато удостоверяване на автентичността, защитени гласови, видео- и текстови съобщения и защитени системи за спешна комуникация в рамките на субекта, когато е целесъобразно;

11. управление на измененията на информационните активи;

12. мерки за управление на риска в областта на киберсигурността и задължения за докладване за субекти от вида, посочен в приложение I или II, както и за субекти, установени като критични съгласно Директива (ЕС) 2022/2557.

(3) При разглеждане на въпросите кои мерки по ал. 2, т. 4 са подходящи, от субектите се изисква да вземат предвид уязвимостите, специфични за всеки пряк снабдител или доставчик на услуги, както и цялостното качество на продуктите и практиките в областта на киберсигурността на своите снабдители и доставчици на услуги, включително техните процедури за сигурно разработване. При определяне кои мерки от посочените в ал. 2, т. 4 са подходящи, от субектите се изисква да вземат предвид резултатите от координираните оценки на риска за сигурността на критичните вериги на доставка, извършени в съответствие с чл. 23.

(4) При установен пропуск в спазването на мерките, предвидени в ал. 2, субектите предприемат всички необходими, подходящи и пропорционални коригиращи мерки за отстраняването му.

Задължения за докладване

Чл. 23. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Съществените и важните субекти уведомяват СЕРИКС за всеки значителен инцидент по образец съгласно наредбите по чл. 3 при условията и по реда на ал. 5. Уведомяването не води до повишена отговорност за уведомяващия субект.

(2) Засегнатите субекти уведомяват, когато е подходящо и без ненужно забавяне, получателите на техните услуги за значителни инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги. При изключителни обстоятелства, когато уведомяването им може да изложи на риск разследването на значителния инцидент, на субектите се разрешава, след получаване на съгласие от страна на съответния национален компетентен орган, да забавят уведомяването на получателите, докато националният компетентен орган счете, че е възможно да уведоми за нарушаването на сигурността на лични данни в съответствие с настоящия член.

(3) В случай че СЕРИКС установи информация за наличие на трансграничен или междусекторен значителен инцидент, СЕРИКС изпраща незабавно информацията на националното единно звено за контакт.

(4) Съществените и важните субекти съобщават на получателите на техните услуги, които са потенциално засегнати от значителна киберзаплаха, всички мерки или средства

за защита, които тези получатели могат да предприемат. Когато е целесъобразно, субектите уведомяват получателите на техните услуги и за вида на значителна киберзаплаха.

(5) За целите на уведомяването по ал. 1 засегнатите субекти подават до СЕРИКС:

1. до 24 часа след установяването на значителен инцидент - ранно предупреждение, в което, когато е приложимо, се посочва дали се предполага, че значителният инцидент се дължи на незаконосъобразни или злонамерени действия и дали би могъл да има трансгранично въздействие;

2. до 72 часа след установяването на значителния инцидент - уведомление за инцидент, в което, когато е приложимо, се актуализира информацията по т. 1 и се посочва първоначална оценка на значителния инцидент, включително неговата тежест и въздействие, както и, когато има такава, техническа информация за инцидента; за доставчиците на удостоверителни услуги срокът по изречение първо е 24 часа;

3. по искане на СЕРИКС - междинен док-лад, съдържащ актуализирана информация за инцидента;

4. окончателен доклад не по-късно от един месец след подаването на уведомлението за инцидента по т. 2, включващ:

а) подробно описание на инцидента, включително неговите обхват и въздействие;

б) вида на заплахата или причината, която вероятно е породила инцидента;

в) приложените и текущите мерки за ограничаване на инцидента;

г) когато е приложимо, трансграничното въздействие на инцидента;

5. в случай че до изтичане на срока по т. 4 субектът не се е справил с инцидента, същият представя междинен доклад, съдържащ, доколкото е приложимо, информацията по т. 4 за справянето с инцидента. Субектите представят окончателен доклад в срок до един месец от справянето с инцидента.

(6) След получаването на ранното предупреждение по ал. 5, т. 1 СЕРИКС връща отговор на уведомяващия субект и му предоставя първоначална информация за значителния инцидент и при поискване от субекта предоставя насоки или оперативни съвети за прилагането на възможни мерки за ограничаване или допълнителна техническа подкрепа. Отговорът по изречение първо се изпраща не по-късно от 24 часа, освен ако по обективни причини срокът не може да бъде спазен, в които случаи отговорът се изпраща във възможно най-кратък срок.

(7) Когато има основания да се смята, че значителният инцидент представлява или е свързан с извършване на престъпление, СЕРИКС уведомява Главна дирекция „Борба с организираната престъпност" на Министерството на вътрешните работи за значителния инцидент и є предоставя цялата налична при него информация.

(8) Когато значителният инцидент засяга критична информационна система на стратегически обект или дейност от значение за националната сигурност или има основание да се смята, че значителният инцидент е свързан с намеса на чужда държава или инфраструктура, разположена извън страната, СЕРИКС незабавно уведомява Държавна агенция „Национална сигурност" за значителния инцидент и є предоставя цялата налична при него информация.

(9) Когато значителният инцидент засяга две или повече държави членки, Националното единно звено за контакт информира другите засегнати държави членки и Агенцията на Европейския съюз за киберсигурност (ENISA) за значителния инцидент, като запазват сигурността и търговските интереси на субекта, както и поверителността на предоставената информация в съответствие с приложимото законодателство. Уведомлението включва информация, получена по реда на ал. 5.

(10) С цел предотвратяване на значителен инцидент или справяне с текущ значителен инцидент или когато е в обществен интерес по друга причина, НЕРИКС, след като се консултира със засегнатия субект, може да оповести публично информация за значителния инцидент или да изиска от субекта да направи оповестяването.

(11) По искане на НЕРИКС Националното единно звено за контакт предава уведомленията, получени съгласно ал. 1, на единните звена за контакт на други засегнати държави членки.

(12) Предоставянето на други държави на информация за значителни инциденти, засягащи стратегически обект или дейност от значение за националната сигурност и свързани с намеса на чужда държава или инфраструктура, разположена извън страната, се извършва след съгласуване с Държавна агенция „Национална сигурност".

(13) На всеки три месеца Националното единно звено за контакт представя на Агенцията на Европейския съюз за киберсигурност (ENISA) обобщаващ доклад, включващ анонимизирани и обобщени данни за значителните инциденти, за инцидентите, киберзаплахите и ситуациите, близки до инциденти, за които е изпратено уведомление в съответствие с ал. 1 от настоящия член или доброволно уведомление по реда на чл. 27д.

(14) Националният екип за реагиране при инциденти с компютърната сигурност предоставя на определените за компетентни органи съгласно Директива (ЕС) 2022/2557 информация относно значителните инциденти, инцидентите, киберзаплахите и ситуациите, близки до инциденти, за които е подадено уведомление в съответствие с ал. 1 или доб-роволно уведомление по реда на чл. 27д от субектите, установени като критични съгласно Директива (ЕС) 2022/2557.

Сертифициране на киберсигурността

Чл. 24. (Изм. - ДВ, бр. 17 от 2026 г.) За да се докаже съответствие с конкретни изисквания по чл. 22, Министерският съвет с постановление, прието по предложение на Съвета по киберсигурността, може да създаде изисквания към съществените и важни субекти да използват конкретни, доказано подходящи в оперативно и икономическо отношение ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени от тях или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ, L 151/15 от 7 юни 2019 г.), наричан по-нататък „Регламент (ЕС) 2019/881". Националният компетентен орган насърчава съществените и важните субекти да използват квалифицирани удостоверителни услуги.

Стандартизация

Чл. 25. (Изм. - ДВ, бр. 17 от 2026 г.) Без да се налага употребата на определен тип технология и/или с цел хармонизираното прилагане на чл. 22, Съветът по киберсигурността насърчава използването на европейски и международни стандарти и технически спецификации от значение за сигурността на мрежовите и информационните системи.

Координирана на равнището на Европейс-кия съюз оценка на риска за сигурността на критични вериги за доставка

Чл. 26. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Министърът на електронното управление или оправомощено от него лице може да предлага на групата за сътрудничество конкретни критични ИКТ услуги, ИКТ системи или ИКТ продукти, по отношение на които да бъде извършена Координирана на равнището на Европейския съюз оценка на риска за сигурността на критични вериги за доставка съгласно чл. 22 от Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ, L 333/164 от 27 декември 2022 г.).

(2) Министърът на електронното управление представя на Съвета по киберсигурността резултати от всички координирани оценки по чл. 22 от Директива (ЕС) 2022/2555 в 30-дневен срок от извършването им.

Ограничаване на използването на рискови технологии

Чл. 27. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Въз основа на предоставената информация по чл. 26, ал. 2 Съветът по киберсигурността изготвя мотивирано предложение до Министерския съвет за приемане на постановление за ограничаване на използването от субектите по чл. 4 и 4а на конкретни технологии или на критични вериги за доставка на ИКТ услуги и ИКТ продукти, доколкото с това не се засягат императивни разпоредби на правото на Европейския съюз или на действащото българско законодателство и не се влиза в противоречие с координираните оценки на риска в рамките на Европейския съюз.

(2) В случай че субектите по чл. 4 и 4а вече използват технология, която е ограничена с постановлението по ал. 1, те следва да преустановят използването є в тригодишен срок от приемането на постановлението. В случай на висок риск за националната сигурност в постановлението по ал. 1 се определя по-кратък срок.

Глава втора „а"
(Нова - ДВ, бр. 17 от 2026 г.)
ЮРИСДИКЦИЯ И РЕГИСТРАЦИЯ

Юрисдикция и териториалност

Чл. 27а. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Субектите, попадащи в обхвата на този закон, се считат за попадащи под юрисдикцията на държавата, в която са установени, освен в случай на:

1. доставчици на обществени електронни съобщителни мрежи или доставчици на обществено достъпни електронни съобщителни услуги, за които се счита, че попадат под юрисдикцията на държавата членка, в която предоставят своите услуги;

2. доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, субектите, предоставящи услуги за регистриране на имена на домейни, доставчиците на компютърни услуги в облак, доставчиците на услуги на центрове за данни, доставчиците на мрежи за предоставяне на съдържание, доставчиците на управлявани услуги, доставчиците на управлявани услуги за сигурност, както и доставчиците на онлайн места за търговия, на онлайн търсачки или на платформи на услуги за социални мрежи, за които се счита, че попадат под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Европейския съюз съгласно ал. 2.

(2) Ако субект по ал. 1, т. 2 не е установен в Европейския съюз, но предлага услуги в него, той предоставя информация за своя представител в Европейския съюз в срока по чл. 6, ал. 2. Представителят трябва да е установен в една от държавите членки, в които се предлагат услугите. При липсата на представител в Европейския съюз, определен съгласно настоящата алинея, субект, който предлага услуги на територията на Република България, се счита под юрисдикцията на Република България.

Представителство и взаимопомощ

Чл. 27б. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Определянето на представител от страна на субект по чл. 27а, ал. 1, т. 2 не засяга правните действия, които биха могли да се предприемат срещу самия субект.

(2) При получаване на искане за взаимопомощ по отношение на субект, посочен в чл. 27а, ал. 1, т. 2, националните компетентни органи могат да предприемат подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или който притежава мрежова и информационна система.

База данни с регистрационни данни на имена на домейни

Чл. 27в. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на такива имена на домейни, събират и поддържат точни и пълни данни за регистрацията на имената на домейни в поддържани от тях регистри при спазване на изискванията в областта на защитата на личните данни.

(2) В регистрите по ал. 1 се съхранява следната информация, необходима за установяване и осъществяване на връзка с притежателите на имена на домейни и точките за контакт, администриращи имената на домейните в домейни от първо ниво:

1. името на домейна;

2. датата на регистрация;

3. името, адреса на електронната поща и телефонния номер за контакт на регистранта;

4. адреса на електронната поща и телефонния номер за контакт на звеното за контакт, администриращо името на домейна, в случай че те са различни от тези на регистранта.

(3) След всяка регистрация на име на домейн субектите по ал. 1 публикуват незабавно данните за регистрацията при спазване на изискванията в областта на защитата на личните данни.

(4) Субектите по ал. 1 са длъжни да оказват съдействие на националните компетентни органи, СЕРИКС, НЕРИКС и органите на досъдебното производство, като предоставят в срок до 72 часа достъп до конкретни данни за регистрация по ал. 2 при наличие на обосновано и законосъобразно искане и в съответствие с приложимото право в областта на защитата на личните данни.

(5) Субектите по ал. 1 създават и поддържат политики и процедури, включително процедури за проверка и разкриване на информация, които осигуряват спазването на изискванията на ал. 1, 2 и 4. Политиките и процедурите са публични.

(6) Спазването на задълженията, предвидени в ал. 1 - 5, не следва да води до дублиране на събирането на данни за регистрация на имена на домейни. За тази цел изискването е регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да си сътрудничат.

Глава втора „б"
(Нова - ДВ, бр. 17 от 2026 г.)

Споразумения за обмен на информация в областта на киберсигурността

Чл. 27г. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Субектите, попадащи в обхвата на този закон, както и други субекти, които не попадат в обхвата, могат да обменят на доброволна основа относима информация за киберсигурността, включително такава относно киберзаплахи, ситуации, близки до инциденти, уязвимости, техники и процедури, признаци за нарушена сигурност, злонамерени тактики, специфична за източника на заплахата информация, предупреждения във връзка с киберсигурността и препоръки за конфигуриране на инструменти за киберсигурност за откриване на кибератаки, когато този обмен на информация:

1. има за цел предотвратяване, откриване, реагиране или възстановяване от инциденти или смекчаване на тяхното въздействие;

2. подобрява нивото на киберсигурност, по-специално посредством повишаване на осведомеността във връзка с киберзаплахи, ограничаване или възпрепятстване на способността за разпространение на такива зап-лахи, поддържане на набор от отбранителни способности, отстраняване и оповестяване на уязвимости, техники за откриване, ограничаване и предотвратяване на заплахи, стратегии за ограничаване или етапи за реакция или възстановяване, или насърчаване на съвместни научни изследвания относно киберзаплахите между публични и частни субекти.

(2) Обменът на информация се осъществява в рамките на общности на съществените и важните субекти, и, когато е относимо, на техните снабдители или доставчици на услуги. Този обмен се осъществява чрез споразумения за обмен на информация в областта на киберсигурността с оглед на потенциално чувствителния характер на споделяната информация.

(3) Националните компетентни органи улесняват създаването на споразумения за обмен на информация в областта на киберсигурността, посочени в ал. 2. Тези

споразумения може да уточняват оперативните елементи, включително използването на специално предназначени ИКТ платформи и инструменти за автоматизиране, съдържанието и условията по споразуменията за обмен на информация. Когато определят подробностите за участието на административните органи в такива споразумения, националните компетентни органи могат да налагат условия по отношение на информацията, предоставяна от компетентните органи или ЕРИКС. Националните компетентни органи оказват помощ при прилагането на такива споразумения в съответствие с политиките, посочени в чл. 8, ал. 2, т. 8.

(4) Съществените и важните субекти уведомяват националните компетентни органи за своето участие в споразуменията за обмен на информация в областта на киберсигурността по ал. 2 при присъединяването в такива споразумения или при прекратяването им.

Доброволно уведомяване за относима информация

Чл. 27д. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Извън задължението за уведомяване, предвидено в чл. 23, се създава възможността за подаване на уведомления до СЕРИКС/НЕРИКС или, когато е приложимо, до националните компетентни органи на доброволна основа:

1. от съществени и важни субекти по отношение на инциденти, киберзаплахи и ситуации, близки до инциденти;

2. от субекти, различни от посочените в т. 1, независимо дали попадат в обхвата на настоящия закон, по отношение на значителни инциденти, киберзаплахи и ситуации, близки до инциденти.

(2) Уведомленията по ал. 1 се обработват в съответствие с процедурата, предвидена в чл. 23. Националните компетентни органи обработват задължителните уведомления с предимство пред доброволните уведомления.

(3) При необходимост ЕРИКС или националните компетентни органи предоставят на единното звено за контакт информацията относно уведомленията, получени съгласно настоящия член, като същевременно гарантират поверителността и подходящата защита на информацията, предоставена от уведомяващия субект. Без да се засягат предотвратяването, разследването, разкриването и наказателното преследване на престъпления, доброволното докладване не води до налагането на никакви допълнителни задължения за уведомяващия субект.

Глава втора „в"
(Нова - ДВ, бр. 17 от 2026 г.)
КОНТРОЛ

Органи

Чл. 27е. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Контролът за спазване на изиск-ванията по този закон се осъществява от:

1. националните компетентни органи по чл. 16;

2. Министерството на отбраната;

3. Министерството на вътрешните работи;

4. Държавна агенция „Национална сигурност".

(2) За осъществяване на контрол по този закон органите по ал. 1 оправомощават със заповед длъжностни лица от съответната администрация.

Правомощия при осъществяване на контрола

Чл. 27ж. (Нов - ДВ, бр. 17 от 2026 г.)*(1)* При осъществяване на своите правомощия по отношение на съществените субекти органите по чл. 27е имат право да:

1. извършват проверки - планови и извънпланови, на място или дистанционни, извършвани от компетентни оправомощени длъжностни лица;

2. извършват редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган;

3. извършват извънпланови одити, когато са обосновани поради значителен инцидент или нарушение на този закон от страна на съществения субект;

4. извършват проверки за сигурност, основани на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска, при необходимост, със съдействието на съответния субект;

5. изискват информация, необходима за оценка на мерките за управление на риска в областта на киберсигурността, приети от съответния субект, включително документирани политики в областта на киберсигурност, както и изпълнение на задълженията за изпращане на информация на националните компетентни органи съгласно чл. 27в (Регистъра на ENISA);

6. им бъде предоставен достъп до данни, документи и всякаква информация, необходими за осъществяването на техните надзорни задачи;

7. изискват и да им бъдат предоставени доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.

(2) При осъществяване на своите правомощия, по отношение на важните субекти, органите по чл. 27е имат право да:

1. извършват проверки на място и последващ дистанционен надзор, извършвани от компетентни оправомощени длъжностни лица;

2. извършват целеви одити на сигурността, извършвани от независим орган или компетентен орган;

3. извършват проверки за сигурност, основани на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска, при необходимост, със съдействието на съответния субект;

4. изискват информация, необходима за последваща оценка на мерките за управление на риска в областта на киберсигурността, приети от съответния субект, включително документирани политики за киберсигурност, както и съответствие със задълженията за изпращане на информация до националните компетентни органи съгласно чл. 27в;

5. изискват достъп до данни, документи и информация, необходими за изпълнението на надзорните им задачи;

6. изискват доказателства за изпълнението на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.

(3) При упражняване на своите правомощия по ал. 1, т. 5, 6 и 7, съответно ал. 2, т. 4, 5 и 6, националните компетентни органи заявяват целта на своето искане и поясняват исканата информация.

Целеви одити на сигурността

Чл. 27з. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Целевите одити на сигурността, посочени в чл. 27ж, се основават на оценки на риска, извършени от компетентния орган или одитирания субект, или на друга налична информация, свързана с риска.

(2) Резултатите от всеки целеви одит на сигурността се предоставят на националните компетентни органи по чл. 16, ал. 1.

(3) Разходите за такъв целеви одит на сигурността, извършен от независим орган, се заплащат от одитирания субект, освен в надлежно обосновани случаи, когато националният компетентен орган реши друго.

Предупреждения, задължителни предписания и разпореждания

Чл. 27и. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* При осъществяване на своите правомощия органите по чл. 27е издават:

1. предупреждения;

2. задължителни предписания или разпореждания, с които се изисква от засегнатите субекти да отстранят установените пропуски или нарушения на този закон,

а за съществените субекти - и предписания относно мерките, необходими за предотвратяване на възникването на инцидент или за справяне с него, за изпълнение на задължение за док-ладване, както и да определят срокове за изпълнение на такива мерки;

3. разпореждания за преустановяване на поведение, което нарушава закона, и за въздържане от повтаряне на такова поведение;

4. разпореждания за гарантиране, че мерките за управление на риска в областта на киберсигурността са в съответствие с чл. 22, или че са изпълнени задълженията за докладване по чл. 23 по конкретен начин, за което да е определен срок;

5. разпореждания към засегнатите субекти да уведомяват физическите или юридическите лица, на които предоставят услуги или по отношение на които извършват дейности и които са потенциално засегнати от значителна киберзаплаха, за естеството на заплахата, както и за възможните защитни или коригиращи мерки, които могат да предприемат в отговор на тази заплаха;

6. разпореждания към засегнатите субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността, като определят за това разумен срок;

7. разпореждания към засегнатите субекти да обявят публично извършеното от тях нарушение, като определят подходящ начин за това.

(2) По отношение на съществените субекти органите по чл. 27е могат да определят длъжностно лице по надзор за спазването на чл. 22 и 23 от засегнатите субекти, както и на неговите конкретни задачи и срок за изпълнение.

Принудителни мерки

Чл. 27к. (Нов - ДВ, бр. 17 от 2026 г.)*(1)* За непредприемане на действията, определени по реда на чл. 27и, ал. 1, т. 1 - 4 и т. 6, акт за временно спиране на действието на лиценз, регистрация, сертификат или разрешение относно всички или част от съответните предоставени услуги или дейностите, извършвани от съществения субект, се издава от:

1. националния компетентен орган, в случаите, в които той е издал лиценза, сертификата или разрешението или е извършил регистрацията, или

2. съд или съответния компетентен административен орган, по искане на националния компетентен орган.

(2) За непредприемане на действията, определени по реда на чл. 23, чл. 27и, ал. 1, т. 1 - 4 и т. 6, националният компетентен орган по чл. 27е може да изиска от съд или от друг държавен орган налагането на временна забрана спрямо всяко физическо лице, изпълняващо управленски функции, или законен представител на съществен субект да упражнява управленски функции в него.

(3) Компетентният административен орган за временно спиране на лиценз, регистрация, сертификат или разрешение по ал. 1 се произнася с индивидуален административен акт, който може да бъде обжалван по реда на Административнопроцесуалния кодекс.

(4) Алинеи 1 и 2 не се прилагат по отношение на съществени субекти, които са административни органи.

(5) Всяко физическо лице, отговорно за съществен или важен субект или действащо като негов законен представител въз основа на правомощие да го представлява, да взема решения от негово име или да упражнява контрол върху него, има необходимите правомощия, за да осигури спазването на закона. За тези лица се прилагат всички мерки, предвидени в закона и могат да бъдат подведени под отговорност за неизпълнението на своите задължения.

Задължение за информиране

Чл. 27л. (Нов - ДВ, бр. 17 от 2026 г.) Органите по чл. 16 информират съответните компетентни органи съгласно Директива (ЕС) 2022/2557, когато упражняват своите правомощия, имащи за цел да гарантират спазването на настоящия закон от съществен

субект, установен като критичен субект съгласно Директива (ЕС) 2022/2557. Когато е целесъобразно, компетентните органи съгласно Директива (ЕС) 2022/2557 могат да поискат от националните компетентни органи по чл. 16 да упражняват своите правомощия във връзка със съществен субект, който е установен като критичен съгласно Директива (ЕС) 2022/2557.

Сътрудничество и взаимодействие

Чл. 27м. (Нов - ДВ, бр. 17 от 2026 г.) Компетентните органи съгласно този закон си сътрудничат със съответните компетентни органи на засегнатата държава членка съгласно Регламент (ЕС) 2022/2554. Компетентните органи съгласно закона информират надзорния форум, установен съгласно член 32, параграф 1 от Рег-ламент (ЕС) 2022/2554, когато упражняват своите надзорни и правоприлагащи правомощия, целящи гарантиране на спазването на закона от страна на съществен или важен субект, който е определен като трета страна критичен доставчик на услуги в областта на ИКТ, в съответствие с член 31 от Регламент (ЕС) 2022/2554.

Нарушения в сигурността на личните данни

Чл. 27н. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Органите по чл. 16 уведомяват незабавно Комисията за защита на личните данни, когато при осъществяване на своите правомощия установят извършено нарушение от съществен или важен субект, което би могло да доведе до нарушаване на сигурността на личните данни съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ, L 119/1 от 4 май 2016 г.), наричан по-нататък „Регламент (ЕС) 2016/679" и Закона за защита на личните данни.

(2) Когато надзорните органи, посочени в член 55 или член 56 от Регламент (ЕС) 2016/679, наложат имуществена санкция съгласно чл. 58, параграф 2, буква „и" от същия регламент, компетентните органи по този закон не налагат имуществена санкция съгласно чл. 27л по отношение на ал. 1, произтичащо от същото деяние, което е било предмет на имуществена санкция съгласно член 58, параграф 2, буква „и" от Регламент (ЕС) 2016/679. В тези случаи компетентните органи по този закон могат да налагат само мерките, предвидени в чл. 27л.

(3) Когато надзорният орган, компетентен съгласно Регламент (ЕС) 2016/679, е установен в държава членка, различна от тази на компетентния орган по този закон, компетентният орган уведомява Комисията за защита на личните данни относно възможното нарушаване на сигурността на данните, посочено в ал. 1.

Взаимопомощ

Чл. 27о. (Нов - ДВ, бр. 17 от 2026 г.) *(1)* Когато субект предоставя услуги на територията на Република България и в друга държава членка и неговите мрежови и информационни системи са разположени на територията на Република България и в други държави членки, компетентните органи по този закон си сътрудничат и се подпомагат взаимно с компетентните органи на засегнатите държави членки, ако е необходимо. Това сътрудничество включва най-малко следното:

1. националните компетентни органи посредством единното звено за контакт уведомяват и се консултират с компетентните органи в другите засегнати държави членки относно предприетите надзорни и правоприлагащи мерки;

2. национален компетентен орган може да поиска от друг компетентен орган в друга държава членка да предприеме надзорни или правоприлагащи мерки;

3. когато национален компетентен орган получи обосновано искане от друг компетентен орган, включително от друга държава членка, той му оказва взаимопомощ, пропорционална на собствените му ресурси, така че надзорните и правоприлагащите мерки да могат да бъдат приложени по ефективен, ефикасен и последователен начин.

(2) Взаимопомощта, посочена в ал. 1, т. 3, може да обхваща искания за информация и надзорни мерки, включително искания за провеждане на проверки на място или дистанционен надзор, или целеви одити на сигурността. Национален компетентен орган, към когото е отправено искане за помощ, не отхвърля това искане, освен ако не бъде установено, че не е компетентен да предостави исканата помощ, поисканата помощ не е пропорционална на надзорните задачи на националния компетентен орган или искането се отнася до информация или включва дейности, които, ако бъдат оповестени или извършени, биха противоречили на националната сигурност, обществената сигурност или отбраната. Преди да отхвърли такова искане, националният компетентен орган се консултира с другите засегнати компетентни органи както и, по искане на една от засегнатите държави членки - с Европейската комисия и Агенцията на Европейския съюз за киберсигурност (ENISA).

(3) Когато е подходящо и при общо съгласие, компетентните органи могат да извършват общи надзорни действия с компетентни органи от други държави членки.

Глава трета
АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ

Отговорност за неизпълнение на принудителни административни мерки

Чл. 28. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Съществен или важен субект, който не изпълни принудителна административна мярка по смисъла на чл. 27и, ал. 1, т. 2 - 7, се наказва с глоба или имуществена санкция в размер от 2500 до 12 000 евро.

(2) При повторно нарушение по ал. 1 наказанието е глоба или имуществена санкция в размер от 5000 до 25 000 евро.

Глоби и имуществени санкции

Чл. 29. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* Глобите и имуществените санкции се налагат независимо от която и да е от мерките, посочени в чл. 27и, ал. 1, т. 2 - 7 и чл. 27к.

(2) На съществен субект, който не изпълнява задълженията си по чл. 22 и 23, се налага имуществена санкция в размер до 10 000 000 евро или до две на сто от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи същественият субект, която от двете суми е по-висока, но не по-малко от 25 000 евро.

(3) На важен субект, който не изпълни задълженията по чл. 22 и 23, се налага имуществена санкция в размер до 7 000 000 евро или до 1,4 на сто от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важният субект, която от двете суми е по-висока, но не по-малко от 12 500 евро.

(4) При нарушение на чл. 21 на ръководителите на административните органи, управителите или членовете на управителните органи на съществените и важните субекти се налага глоба в размер от 500 до 5000 евро.

(5) Алинея 2 не се прилага по отношение на съществените субекти, които са административни органи.

Смекчаващи вината обстоятелства

Чл. 29б. (Нов - ДВ, бр. 17 от 2026 г.) При прилагане на принудителна мярка по чл. 27и и/или налагане на наказание глоба или имуществена санкция по чл. 28 или 29 органите по чл. 27е вземат предвид следните обстоятелства:

1. степента на обществена опасност на извършеното нарушение;

2. повторност на нарушението;

3. дали нарушението е извършено умишлено или по непредпазливост;

4. неуведомяване или липса на реакция от страна на нарушителя при възникване на значителни инциденти;

5. причинените имуществени или неимуществени вреди от извършеното нарушение и неговото въздействие върху други услуги и брой на засегнатите потребители;

6. възпрепятстване от страна на нарушителя на одити или дейности по мониторинг след установяване на нарушението;

7. предоставяне от страна на нарушителя на невярна или непълна информация във връзка с мерките за управление на риска в областта на киберсигурността или задълженията за докладване;

8. всички предприети от нарушителя мерки за предотвратяване или ограничаване на имуществените или неимуществените вреди.

Отговорност за други нарушения

Чл. 30. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Длъжностно лице, което извърши или допусне извършването на друго нарушение по глава втора, се наказва с глоба от 500 до 10 000 евро, освен ако деянието не съставлява престъпление.

(2) (Изм. - ДВ, бр. 17 от 2026 г.) При повторно нарушение по ал. 1 наказанието е глоба от 750 до 15 000 евро.

(3) (Изм. - ДВ, бр. 17 от 2026 г.) На лице, което не изпълни задължение по чл. 14, ал. 5, чл. 15, ал. 5, се налага глоба от 500 до 7500 евро или имуществена санкция 750 до 15 000 евро.

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

Чл. 31. (Изм. - ДВ, бр. 17 от 2026 г.) *(1)* (Изм. - ДВ, бр. 17 от 2026 г.) Актовете за установяване на нарушения по този закон, извършени от административни органи, се съставят от длъжностни лица, определени от министъра на електронното управление.

(2) (Изм. - ДВ, бр. 17 от 2026 г.) Актовете за установяване на нарушения по този закон, извършени от съществени и важни субекти, 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) (Изм. - ДВ, бр. 17 от 2026 г.) Актовете за установяване на нарушения по чл. 30, ал. 3 във връзка с чл. 15, ал. 7 се съставят от длъжностни лица, определени от председателя на Държавна агенция „Национална сигурност".

(5) Наказателните постановления се издават от:

1. 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. (Изм. - ДВ, бр. 17 от 2026 г.) Този закон въвежда изисквания на Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Рег-ламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ, L 333/80 от 27 декември 2022 г.).

§ 2. (Изм. - ДВ, бр. 17 от 2026 г.) Този закон предвижда мерки по прилагане на „Приложение към заключенията на Съвета относно сигурността на веригата за доставки на ИКТ, одобрени от Съвета на заседанието му от 17 октомври 2022 г.

§ 2а. (Нов - ДВ, бр. 17 от 2026 г.) Този закон предвижда мерки по прилагане на Насоки на Комисията за прилагане на член 3, параграф 4 от Директива (ЕС) 2022/2555 (Директива МИС 2) (2023/C 324/02).

§ 3. (Изм. и доп. - ДВ, бр. 17 от 2026 г.) По смисъла на този закон:

1. (Изм. - ДВ, бр. 17 от 2026 г.) „Административен орган" е орган, който принадлежи към системата на изпълнителната власт.

2. (Изм. - ДВ, бр. 17 от 2026 г.) „Група за сътрудничество" е групата по смисъла на чл. 14 от Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

2а. (Нова - ДВ, бр. 17 от 2026 г.) „Национална стратегия за киберсигурност" е съгласувана рамка на държавата, съдържаща стратегически цели и приоритети в областта на киберсигурността и управленските методи за постигането им.

3. (Изм. - ДВ, бр. 17 от 2026 г.) „Действия при инцидент" са всякакви действия и процедури, имащи за цел предот-вратяването, установяването, анализа, ограничаването или реагирането на инцидент и възстановяването от него.

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

4а. (Нова - ДВ, бр. 17 от 2026 г.) „Система за имена на домейни" или „DNS" е йерархична разпределена система за именуване, която позволява идентифициране на интернет услуги и ресурси, позволявайки на устройствата на крайните ползватели да използват интернет маршрутизация и услуги за свързване, за да достигнат до тези услуги и ресурси.

5. (Изм. - ДВ, бр. 17 от 2026 г.) „Доставчик на DNS услуги" е субект, предоставящ:

а) публично достъпни рекурсивни услуги за преобразуване на имена на домейни за крайни интернет ползватели, или

б) услуги за овластено преобразуване на имена на домейни за използване от трета страна с изключение на базови сървъри за имена.

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. (Изм. - ДВ, бр. 17 от 2026 г.) „Ситуация, близка до инцидент" е събитие, което е могло да засегне отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи, чието случване (чиято активност е била предодвратена) е било успешно предотвратено или което не се е осъществило.

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

11. (Изм. - ДВ, бр. 17 от 2026 г.) „Киберзаплаха" е всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, върху ползвателите на такива мрежи и системи и други лица.

11а. (Нова - ДВ, бр. 17 от 2026 г.) „Значителна киберзаплаха" е киберзаплаха, за която въз основа на техническите є характеристики може да се предположи, че има

потенциал да окаже сериозно въздействие върху мрежовите и информационните системи на даден субект или върху ползвателите на услугите на субекта, като причини значителни материални или нематериални вреди.

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.

12а. (Нова - ДВ, бр. 17 от 2026 г.) „Инцидент" е събитие, което засяга отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи.

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.

15а. (Нова - ДВ, бр. 17 от 2026 г.) „Мащабен киберинцидент" е инцидент, който причинява степен на смущение, надхвърляща способността на държавата да реагира на него, или който има значително въздействие върху най-малко две държави членки.

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. (Изм. - ДВ, бр. 17 от 2026 г.) „Компютърна услуга „в облак" е цифрова услуга, която дава възможност за администриране при поискване и широк отдалечен достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно, включително когато тези ресурси са разпределени на няколко места.

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

21. (Изм. - ДВ, бр. 17 от 2026 г.) „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 киберсигурност (ENISA).

22. (Изм. - ДВ, бр. 17 от 2026 г.) „Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност" е мрежата по смисъла на чл. 15 от Директива (ЕС)

2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

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. (Изм. - ДВ, бр. 17 от 2026 г.) „Онлайн място за търговия" е услуга, която чрез използване на софтуер, включително уебсайт, част от уебсайт или приложение, управлявани от търговеца или от негово име, позволява на потребителите да сключват договори от разстояние с други търговци или потребители.

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.

27а. (Нова - ДВ, бр. 17 от 2026 г.) „ИКТ продукт" е ИКТ продукт съгласно определението в член 2, точка 12 от Регламент (ЕС) 2019/881.

27б. (Нова - ДВ, бр. 17 от 2026 г.) „ИКТ услуга" е ИКТ услуга съгласно определението в член 2, точка 13 от Регламент (ЕС) 2019/881.

27в. (Нова - ДВ, бр. 17 от 2026 г.) „ИКТ процес" е ИКТ процес съгласно определението в член 2, точка 14 от Регламент (ЕС) 2019/881.

28. (Изм. - ДВ, бр. 17 от 2026 г.) „Представител" е установено в Съюза физическо или юридическо лице, изрично определено да действа от името на доставчик на DNS услуги, регистър на имена на домейни от първо ниво, субект, предоставящ услуги за регистрация на имена на домейни, доставчик на компютърни услуги „в облак", доставчик на услуги на център за данни, доставчик на мрежи за предоставяне на съдържание, доставчик на управлявани услуги, доставчик на управлявани услуги за сигурност или доставчик на онлайн места за търговия, на онлайн търсачки или на платформи на услуги за социални мрежи, което не е установено в Съюза, и към което, по отношение на задълженията на даден субект съгласно настоящата директива, компетентен орган или ЕРИКС може да се обръща вместо към самия субект.

29. (Изм. - ДВ, бр. 17 от 2026 г.) „Регистър на имена на домейни от първо ниво" е субект, на който е поверен конкретен домейн от първо ниво и който е отговорен за администрирането на този домейн, включително за регистрацията на имена на домейни на нива под домейна от първо ниво и техническото функциониране на този домейн, включително функционирането на неговите сървъри за имена, поддръжката на неговите бази данни и разпределението на файловете на зоните на домейна от първо ниво в сървърите за имена, независимо дали която и да е от тези операции се извършва от субекта, или е възложена на външни изпълнители, като обаче се изключват ситуациите,

при които имената на домейни от първо ниво са използвани от регистър единствено за собствено ползване.

29а. (Нова - ДВ, бр. 17 от 2026 г.) „Субект, предоставящ услуги за регистрация на имена на домейни" е регистратор или агент, действащ от името на регистратори, като например доставчик или препродавач на услуги за поверителност или прокси услуги.

30. (Изм. - ДВ, бр. 17 от 2026 г.) „Риск" е потенциалната загуба или потенциалното смущение в резултат на даден инцидент и трябва да се изразява като комбинация от мащаба на загубата или смущението и вероятността от настъпване на инцидента.

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.

31а. (Нова - ДВ, бр. 17 от 2026 г.) „Удостоверителна услуга" е удостоверителна услуга съгласно определението в член 3, точка 16 от Регламент (ЕС) № 910/2014.

31б. (Нова - ДВ, бр. 17 от 2026 г.) „Доставчик на удостоверителна услуга" е доставчик на удостоверителна услуга съгласно определението в член 3, точка 19 от Регламент (ЕС) № 910/2014.

31в. (Нова - ДВ, бр. 17 от 2026 г.) „Квалифицирана удостоверителна услуга" е квалифицирана удостоверителна услуга съгласно определението в член 3, точка 17 от Регламент (ЕС) № 910/2014.

31г. (Нова - ДВ, бр. 17 от 2026 г.) „Доставчик на квалифицирана удостоверителна услуга" е доставчик на квалифицирана удостоверителна услуга съгласно определението в член 3, точка 20 от Регламент (ЕС) № 910/2014.

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.).

32а. (Нова - ДВ, бр. 17 от 2026 г.) „Стандарт" е стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета.

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. (Изм. - ДВ, бр. 17 от 2026 г.) „Уязвимост" е слабост, предразположеност или недостатък на ИКТ продукти или ИКТ услуги, които могат да бъдат използвани при киберзаплаха.

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. (Изм. - ДВ, бр. 17 от 2026 г.) „Цифрова инфраструктура" е инфраструктурата, която включва категориите, посочени в приложение № 1, т. 8.

37. (Нова - ДВ, бр. 17 от 2026 г.) „Услуга на център за данни" е услуга, включваща конструкции или групи конструкции, предназначени за централизирано разполагане, свързване и експлоатация на ИТ и мрежово оборудване, предоставяща услуги за

съхранение, обработване и пренос на данни, заедно с всички съоръжения и инфраструктури за електроразпределение и контрол на околната среда.

38. (Нова - ДВ, бр. 17 от 2026 г.) „Мрежа за доставяне на съдържание" е мрежа от географски разпределени сървъри с цел да се осигури висока степен на наличност, достъпност или бързо доставяне на цифрово съдържание и услуги на интернет потребителите от страна на доставчиците на съдържание и услуги.

39. (Нова - ДВ, бр. 17 от 2026 г.) „Платформа на услуги за социална мрежа" е платформа, позволяваща на крайните ползватели да се свързват, споделят, откриват и общуват помежду си посредством множест-во устройства, по-специално чрез чатове, публикации, видеоклипове и препоръки.

40. (Нова - ДВ, бр. 17 от 2026 г.) „Обществена електронна съобщителна мрежа" е обществена електронна съобщителна мрежа по смисъла на § 1, т. 39 от допълнителните разпоредби на Закона за електронните съобщения.

41. (Нова - ДВ, бр. 17 от 2026 г.) „Електронна съобщителна услуга" е електронна съобщителна услуга по смисъла на § 1, т. 17 от допълнителните разпоредби на Закона за електронните съобщения.

42. (Нова - ДВ, бр. 17 от 2026 г.) „Субект" е всяко физическо или юридическо лице, създадено и признато за такова съгласно националното право в своето място на установяване, което може, като действа от свое име, да упражнява права и да бъде обект на задължения.

43. (Нова - ДВ, бр. 17 от 2026 г.) „Доставчик на управлявани услуги" е субект, който предоставя услуги, свързани с инсталирането, управлението, експлоатацията или поддръжката на ИКТ продукти, мрежи, инфраструктура, приложения или всякакви други мрежови и информационни системи, чрез оказване на помощ или активно администриране или в помещенията на клиентите, или от разстояние.

44. (Нова - ДВ, бр. 17 от 2026 г.) „Доставчик на управлявани услуги за сигурност" е доставчик на управлявани услуги, който извършва или предоставя помощ за дейности, свързани с управлението на риска в областта на киберсигурността.

45. (Нова - ДВ, бр. 17 от 2026 г.) „Разузнавателни сведения за заплахи" е информация, която е обобщена, обработена, анализирана, разтълкувана или обогатена, за да се осигури необходимият контекст с оглед на вземането на решения и за да се създадат условия за адекватно и достатъчно разбиране с оглед на ограничаването на последствията от инцидент с ИКТ или от киберзаплаха, включително техническите белези на дадена кибератака, отговорните за нея лица и техния начин на действие и мотивация.

46. (Нова - ДВ, бр. 17 от 2026 г.) „Уязвимо място" е слабост, тенденция или недостатък на актив, система, процес или контролна функция, които могат да бъдат използвани.

47. (Нова - ДВ, бр. 17 от 2026 г.) „Тестване за проникване (TLPT)" е симулиране на тактиката, техниките и процедурите на реални източници на заплаха, за които се счита, че представляват истинска киберзаплаха. Тази симулация представлява контролиран, специално разработен и опиращ се на разузнавателни сведения (червен екип) тест на критичните оперативни производствени системи на финансовия субект.

48. (Нова - ДВ, бр. 17 от 2026 г.) „Риск в областта на ИКТ, пораждан от трета страна" е риск в областта на ИКТ, който може да възникне за финансов субект във връзка с използваните от него услуги в областта на ИКТ, предоставяни от трета страна доставчик на такива услуги или от нейни поддоставчици, включително чрез споразумения за възлагане на дейности на външни изпълнители.

49. (Нова - ДВ, бр. 17 от 2026 г.) „Трета страна - доставчик на услуги в областта на ИКТ" е предприятие, което предоставя услуги в областта на ИКТ.

50. (Нова - ДВ, бр. 17 от 2026 г.) „Вътрешногрупов доставчик на услуги в областта на ИКТ" е предприятие, което е част от финансова група и предоставя предимно услуги

в областта на ИКТ на финансови субекти от същата група или на финансови субекти, които са част от една и съща институционална защитна схема, включително на техните предприятия майки, дъщерни предприятия, клонове или други субекти, намиращи се в обща собственост или под общ контрол.

51. (Нова - ДВ, бр. 17 от 2026 г.) „Услуги в областта на ИКТ" са цифрови услуги и услуги за данни, предоставяни непрекъснато чрез системите на ИКТ на един или повече вътрешни или външни ползватели, включително хардуер като услуга и хардуерни услуги, което включва техническа поддръжка чрез актуализации на софтуер или фърмуер от доставчика на хардуер и изключва традиционните аналогови телефонни услуги.

52. (Нова - ДВ, бр. 17 от 2026 г.) „Критична или важна функция" е функция, чието смущение би намалило съществено финансовите резултати на даден финансов субект или стабилността или непрекъснатостта на неговите услуги и дейности, или функция, чието прекъсване, неизправност или срив би намалило съществено възможността на даден финансов субект да продължи да изпълнява условията и задълженията, свързани с неговия лиценз, или останалите си задължения съгласно приложимото право в областта на финансовите услуги.

53. (Нова - ДВ, бр. 17 от 2026 г.) „Трета страна - критичен доставчик на услуги в областта на ИКТ" е трета страна, която е доставчик на услуги в областта на ИКТ, определен като имащ критично значение в съответствие с чл. 27з.

54. (Нова - ДВ, бр. 17 от 2026 г.) „Трета страна - доставчик на услуги в областта на ИКТ, установен в трета държава" е трета страна - доставчик на услуги в областта на ИКТ, който е установено в трета държава юридическо лице, което е сключило договорно споразумение с финансов субект за предоставяне на услуги в областта на ИКТ.

55. (Нова - ДВ, бр. 17 от 2026 г.) „Дъщерно предприятие" е дъщерно предприятие по смисъла на член 2, точка 10 и член 22 от Директива 2013/34/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно годишните финансови отчети, консолидираните финансови отчети и свързаните доклади на някои видове предприятия и за изменение на Директива 2006/43/ЕО на Европейския парламент и на Съвета и за отмяна на директиви 78/660/ЕИО и 83/349/ЕИО на Съвета (ОВ, L 182/19 от 29 юни 2013 г.).

56. (Нова - ДВ, бр. 17 от 2026 г.) „Основни стопански дейности" са дейностите по смисъла на § 1, т. 44 от допълнителните разпоредби на Закона за възстановяване и преструктуриране на кредитни институции и инвестиционни посредници.

57. (Нова - ДВ, бр. 17 от 2026 г.) „Значителен инцидент" е инцидент, който е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект, или е засегнал, или е в състояние да засегне други физически или юридически лица, причинявайки значителни материални или нематериални вреди.

58. (Нова - ДВ, бр. 17 от 2026 г.) „Основното място на установяване" на субектите по чл. 27а, ал. 1, т. 2 е в държавата членка, в която преимуществено се вземат решенията относно мерките за управление на риска в областта на киберсигурността. Ако такава държава членка не може да бъде определена или ако такива решения не се вземат в Европейския съюз, се счита, че основното място на установяване се намира в държавата членка, в която се извършват операциите в областта на киберсигурността. Ако такава държава членка не може да бъде определена, за основно място на установяване се счита държавата членка, в която съответният субект има място на установяване с най-големия брой служители в Европейския съюз.

59. (Нова - ДВ, бр. 17 от 2026 г.) „Защита на обществения интерес" е защита на достойнството на гражданите, справедливостта и гражданските права и свободи, признати от правовия ред, както и гарантиране на сигурността, отбраната и обществения ред на страната, както и осигуряване на условия за ефективно използване на ограничените ресурси и стимулиране на ефективната конкуренция.

60. (Нова - ДВ, бр. 17 от 2026 г.) „Информационни активи" са всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на този закон (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация, поддържащите ги системи (електрозахранващи, климатизиращи и други), оперативни процеси/дейности, служители и външни организации).

61. (Нова - ДВ, бр. 17 от 2026 г.) „Сигурност на мрежовите и информационните системи" е способността на мрежовите и информационните системи да издържат - при дадено равнище на увереност - на всяко събитие, което може да засегне отрицателно наличността, автентичността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежови и информационни системи или достъпни чрез тях.

62. (Нова - ДВ, бр. 17 от 2026 г.) „Киберхигиена" е съвкупност от стандартни практики, процедури и поведенчески модели, прилагани на индивидуално и организационно ниво, с цел постигане на високо ниво на киберсигурност чрез редовна поддръжка и защита на IT системи, мрежи и крайни устройства, проактивни действия, ограничаващи риска от инциденти, нарушения и пробиви в сигурността, повишаване на информационната осведоменост, създаване на сигурна среда, управление на достъпа, план за реакция при инциденти и обучение на служителите.

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 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.

Председател на Народното събрание: Цвета Караянчева

Приложение I към чл. 4, т. 2
(Изм. - ДВ, бр. 25 от 2022 г., в сила от 29.03.2022 г.; изм., бр. 17 от 2026 г.)
Списък на секторите и подсекторите

Сектор	Подсектор	Вид субект
1. Енергетика	а) Електро-енергия	– „Енергийно предприятие" по смисъла на § 1, т. 24 от допълнителните разпоредби на Закона за енергетиката

Сектор	Подсектор	Вид субект
		– „Доставка“ по смисъла на § 1, т. 16 от допълнителните разпоредби на Закона за енергетиката – „Оператор на разпределителна мрежа“ по смисъла на § 1, т. 34б, буква „а“ от допълнителните разпоредби на 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 – „Оператор на преносна мрежа“ по смисъла на § 1, т. 34а, буква „а“ от допълнителните разпоредби на Закона за енергетиката Производители съгласно определението в член 2, точка 38 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 г. относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ, L 158/125 от 14 юни 2019 г.). – Номинирани оператори на пазара на електроенергия съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета от 5 юни 2019 г. относно вътрешния пазар на електроенергия (ОВ, L 158/54 от 14 юни 2019 г.). – Участници на пазара съгласно определението в член 2, точка 25 от Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета от 5 юни 2019 г. относно вътрешния пазар на електроенергия (ОВ, L 158/54 от 14 юни 2019 г.), предоставящи услуги за агрегиране, оптимизация на потреблението или съхраняване на енергия съгласно определението в член 2, точки 18, 20 и 59 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 г. относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ, L 158/125 от 14 юни 2019 г.). – Оператори на зарядна точка, отговарящи за управлението и експлоатацията на зарядна точка, която предоставя услуга за зареждане с електроенергия на крайни ползватели, включително от името и за сметка на доставчик на услуги за мобилност.

Сектор	Подсектор	Вид субект
	б) Районно отопление и охлаждане	Оператори на районни отоплителни системи или район- ни охладителни системи съгласно определението в член 2, точка 19 от Директива (ЕС) 2018/2001 на Европейския парламент и на Съвета от 11 декември 2018 г. за насърчаване използването на енергия от възобновяеми източници (ОВ, L 328/82 от 21 декември 2018 г.).
	в) Нефт	Оператори на нефтопроводи
		Оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт
		Централни структури за управление на запасите съгласно определението в член 2, буква е) от Директива на Съвета 2009/119/ЕО от 14 септември 2009 г. за налагане на задължение на държавите членки да поддържат минимални запаси от суров нефт и/или нефтопродукти (ОВ, L 265/9 от 9 октомври 2009 г.).
	г) Природен газ	– „Краен снабдител" по смисъла на § 1, т. 28а, буква „б" от допълнителните разпоредби на Закона за енергетиката
		– „Оператор на разпределителна мрежа" по смисъла на § 1, т. 34б, буква „б" от допълнителните разпоредби на Закона за енергетиката
		– „Оператор на преносна мрежа" по смисъла на § 1, т. 34а, буква „б" 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
		– „Оператор на съоръжение за втечнен природен газ" по смисъла на § 1, т. 34в от допълнителните разпоредби на Закона за енергетиката
		– Предприятия за природен газ съгласно определението в член 2, точка 15 от Директива (ЕС) 2024/1788 на Европейския парламент и на Съвета от 13 юни 2024 г. относно общите правила за вътрешните пазари на газ от възобновяеми източници, природен газ и водород, за изменение на Директива (ЕС) 2023/1791 и за отмяна на Директива 2009/73/ЕО (ОВ, L 2024/1788 от 15 юли 2024 г.).
		Оператори на съоръжения за рафиниране и преработка на природен газ
	д) Водород	Оператори в областта на производството, съхранението и преноса на водород
2. Транспорт	а) Въздушен	Въздушни превозвачи съгласно определението в член 3, точка 4 от Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на

Сектор	Подсектор	Вид субект
		сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ, L 97/72 от 9 април 2008 г.).
		– Управляващи летища органи съгласно определението в член 2, точка 2 от Директива 2009/12/ЕО на Европейския парламент и на Съвета относно летищните такси (ОВ, L 70/11 от 14 март 2009 г.); летища съгласно определението в член 2, точка 1 от същата директива
		Оператори по контрола на управлението на въздушното движение, осъществяващи обслужване по контрол на въздушното движение (КВД) съгласно определението в член 2, точка 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 (ОВ, L 96/1 от 31 март 2004 г.).
	б) Железопътен	Управители на инфраструктура съгласно определението в член 3, точка 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.).
		– „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	– Дружества за вътрешен, морски и крайбрежен пътнически и товарен воден транспорт съгласно определението за морски транспорт в 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.).
		– Управителни органи на пристанищата съгласно определението в член 3, точка 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 310/8 от 25 ноември 2005 г.), включително техните пристанищни съоръжения съгласно определението в член 2, точка 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.).

Сектор	Подсектор	Вид субект
		– Оператори на служби по морския трафик (СМТ) съгласно определението в член 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.).
	г) Автомобилен	Пътни органи съгласно определението в член 2, точка 10 от Делегиран регламент (ЕС) 2022/670 на Комисията от 2 февруари 2022 г. за допълнение 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 122/1 от 25 април 2022 г.), по отношение на предоставянето в целия ЕС на информационни услуги в реално време за движението по пътищата, които отговарят за контрола на управлението на движението, с изключение на публичните субекти, за които управлението на трафика или експлоатацията на интелигентни транспортни системи са несъществена част от общата им дейност.
		– Оператори на „Интелигентни транспортни системи" по смисъла на § 1, т. 40 от допълнителните разпоредби на Закона за автомобилните превози
3. Банков сектор		Кредитни институции съгласно определението в член 4, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012 (ОВ, L 176/1 от 27 юни 2013 г.).
4. Инфраструктури на финансовия пазар		Оператори на места на търговия съгласно определението в член 4, точка 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.).
		Централни контрагенти (ЦК) съгласно определението в член 2, точка 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		Доставчици на здравно обслужване съгласно определението в член 3, буква „ж" от Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на

Сектор	Подсектор	Вид субект
		пациентите при трансгранично здравно обслужване (ОВ, L 88/45 от 4 април 2011 г.). Референтни лаборатории на ЕС съгласно определението в член 15 от Регламент (ЕС) 2022/2371 на Европейския парламент и на Съвета от 23 ноември 2022 г. относно сериозните трансгранични заплахи за здравето и за отмяна на Решение № 1082/2013/ЕС (ОВ, L 314/26 от 6 декември 2022 г.).
		Субекти, извършващи научноизследователска и развойна дейност в областта на лекарствените продукти, съгласно определението в член 1, точка 2 от Директива 2001/83/ЕО на Европейския парламент и на Съвета от 6 ноември 2001 г. за утвърждаване на кодекс на Общността относно лекарствени продукти за хуманна употреба (ОВ, L 311/67 от 28 ноември 2001 г.). Субекти, произвеждащи лекарствени вещества и продукти, съгласно определението в приложение I, раздел B, разделение 21 на Статистическа класификация на икономическите дейности от Делегиран регламент (ЕС) 2023/137 на Комисията от 10 октомври 2022 г. за изменение на Регламент (ЕО) № 1893/2006 на Европейския парламент и на Съвета за установяване на статистическа класификация на икономическите дейности NACE Rev. 2 (ОВ, L 19/5 от 20 януари 2023 г.). Субекти, произвеждащи медицински изделия, които се считат за критично важни при извънредни ситуации в областта на общественото здраве („списък на критично важните медицински изделия при извънредни ситуации в областта на общественото здраве“), съгласно определението в член 22 от Регламент (ЕС) 2022/123 на Европейския парламент и на Съвета от 25 януари 2022 г. относно засилена роля на Европейската агенция по лекарствата в готовността за действия при кризи и управлението на кризи по отношение на лекарствените продукти и медицинските изделия (ОВ, L 20/1 от 31 януари 2022 г.).
6. Питейна вода		Директива (ЕС) 2020/2184 на Европейския парламент и на Съвета от 16 декември 2020 г. относно качеството на водата, предназначена за консумация от човека (ОВ, L 435/1 от 23 декември 2020 г.), с изключение на дистрибуторите, за които дистрибуцията на вода за консумация от човека е несъществена част от общата им дейност по дистрибуция на други стоки и продукти.

Сектор	Подсектор	Вид субект
7. Отпадъчни води		Предприятия, които събират, обезвреждат или пречистват градски, битови или промишлени отпадъчни води съгласно определението в член 2, точки от 1, 2 и 3 от Директива на Съвета от 21 май 1991 г. за пречистването на градските отпадъчни води, с изключение на предприятията, за които събирането, обезвреждането или пречистването на градски, битови или промишлени отпадъчни води е несъществена част от тяхната обща дейност.
8. Цифрова инфраструктура		– Доставчици на точки за обмен в интернет – Доставчици на DNS услуги с изключение на оператори на коренови сървъри за имена – Регистри на имената на домейни от първо ниво – Доставчици на услуги за изчисления в облак – Доставчици на услуги на центрове за данни – Доставчици на мрежи за доставка на съдържание – Доставчици на удостоверителни услуги – Доставчици на обществени електронни съобщителни мрежи по смисъла на § 1, т. 39 от допълнителните разпоредби на Закона за електронните съобщения – Доставчици на обществено достъпни електронни съобщителни услуги по смисъла на § 1, т. 40 от допълнителните разпоредби на Закона за електронните съобщения
9. Управление на услуги в областта на ИКТ (между предприятия)		– Доставчици на управлявани услуги – Доставчици на управлявани услуги за сигурност
10. Космическо пространство		Оператори на наземна инфраструктура, притежавани, управлявани и експлоатирани от държавите членки или от частни лица, които подпомагат предоставянето на космически услуги, с изключение на доставчиците на обществени електронни съобщителни мрежи

Приложение II към чл. 4, т. 2
(Изм. - ДВ, бр. 17 от 2026 г.)
ДРУГИ КРИТИЧНИ СЕКТОРИ

Сектор	Подсектор	Субекти
1. Пощенски и куриерски услуги		Доставчици на пощенски услуги съгласно определението в член 2, точка 1а от Директива 97/67/ЕО на Европейския парламент и на Съвета от 15 декември 1997 г. относно общите правила за развитието на вътрешния пазар на пощенските услуги в Общността и за подобряването на качеството на услугата.

Сектор	Подсектор	Субекти
2. Управление на отпадъците		Предприятия, извършващи управление на отпадъците съгласно § 1, т. 46 от допълнителните разпоредби на Закона за управление на отпадъците.
3. Производство, изготвяне и дистрибуция на химикали		Предприятия, извършващи производство на вещества и дистрибуция на вещества или смеси съгласно определението в член 3, точки 9 и 14 от Регламент (ЕО) № 1907/2006 на Европейския парламент и на Съвета от 18 декември 2006 г. относно регистрацията, оценката, разрешаването и ограничаването на химикали (REACH), за създаване на Европейска агенция по химикали, за изменение на Директива 1999/45/ЕО и за отмяна на Регламент (ЕИО) № 793/93 на Съвета и Регламент (ЕО) № 1488/94 на Комисията, както и на Директива 76/769/ЕИО на Съвета и директиви 91/155/ЕИО, 93/67/ЕИО, 93/105/ЕО и 2000/21/ЕО и предприятия, извършващи производство на изделия, посочени в член 3, точка 3 от същия регламент, от вещества или смеси.
4. Производство, преработка и разпространение на храни		Предприятия за производство на храни съгласно определението в член 3, точка 2 от Регламент (ЕО) № 178/2002 на Европейския парламент и на Съвета от 28 януари 2002 г. за установяване на общите принципи и изисквания на законодателството в областта на храните, за създаване на Европейски орган за безопасност на храните и за определяне на процедури относно безопасността на храните.
5. Производство	а) Производство на медицински изделия и медицински изделия за инвитро диагностика	Субекти, произвеждащи медицински изделия съгласно определението в член 2, точка 1 от Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ, L 117/1, 5 май 2017 г.) и субекти, произвеждащи медицински изделия за инвитро диагностика съгласно определението в член 2, точка 2 от Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ, L 117/1 от 5 май 2017 г.) съгласно определението в приложение I, точка 5, пето тире.
	б) Производство на компютри, електронни и	Предприятия, извършващи някоя от икономическите дейности съгласно определението в приложение I, раздел B, разделение 26 на

Сектор	Подсектор	Субекти
	оптични продукти	Статистическа класификация на икономическите дейности NACE Rev. 2.1 от Регламент (ЕС) 2023/137 за изменение на Регламент (ЕО) № 1893/2006 – установяване на статистическа класификация на икономическите дейности.
	в) Производство на електрически съоръжения	Предприятия, извършващи някоя от икономическите дейности съгласно определението в приложение I, раздел B, разделение 27 на Статистическа класификация на икономическите дейности NACE Rev. 2.1 от Регламент (ЕС) 2023/137 за изменение на Регламент (ЕО) № 1893/2006 – установяване на статистическа класификация на икономическите дейности.
	г) Производство на машини и оборудване, некласифицирани другаде	Предприятия, извършващи някоя от икономическите дейности съгласно определението в приложение I, раздел B, разделение 28 на Статистическа класификация на икономическите дейности NACE Rev. 2.1 от Регламент (ЕС) 2023/137 за изменение на Регламент (ЕО) № 1893/2006 – установяване на статистическа класификация на икономическите дейности.
	д) Производство на моторни превозни средства, ремаркета и полуремаркета	Предприятия, извършващи някоя от икономическите дейности съгласно определението в приложение I, раздел B, разделение 29 на Статистическа класификация на икономическите дейности NACE Rev. 2.1 от Регламент (ЕС) 2023/137 за изменение на Регламент (ЕО) № 1893/2006 – установяване на статистическа класификация на икономическите дейности.
	е) Производство на друго транспортно оборудване	Предприятия, извършващи някоя от икономическите дейности съгласно определението в приложение I, раздел B, разделение 30 на Статистическа класификация на икономическите дейности NACE Rev. 2.1 от Регламент (ЕС) 2023/137 за изменение на Регламент (ЕО) № 1893/2006 – установяване на статистическа класификация на икономическите дейности.
6. Доставчици на цифрови услуги		– Доставчици на онлайн места за търговия – Доставчици на онлайн търсачки – Доставчици на платформи на услуги за социални мрежи
7. Научни изследвания		Научноизследователски организации

Заключителни разпоредби към ЗАКОН за изменение и допълнение на Закона за военното разузнаване (ДВ, бр. 69 от 04.08.2020 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 ЗАКОН за изменение и допълнение на Закона за Министерството на вътрешните работи
(ДВ, бр. 85 от 02.10.2020 г., в сила от 01.01.2021 г.)

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

1. В чл. 15:

а) в ал. 2 думите „В Държавна агенция „Национална сигурност" се изгражда и поддържа" се заменят с „Държавна агенция „Национална сигурност" администрира и ползва";

б) създава се ал. 7:

„(7) Центърът по ал. 2 се изгражда и поддържа от Държавна агенция „Електронно управление"."

2. В параграф 14 от преходните и заключителните разпоредби думите „1 януари 2022 г." се заменят с „31 декември 2023 г.".

Преходни и заключителни разпоредби към ЗАКОН за изменение и допълнение на Закона за електронното управление
(ДВ, бр. 15 от 22.02.2022 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:

1. В чл. 9:

а) в ал. 2 думите „заместник министър-председател, определен от министър-председателя" се заменят с „министърът на електронното управление";

б) в ал. 3:

аа) точка 5 се изменя така:

„5. министърът на транспорта и съобщенията;"

бб) създава се т. 8а:

„8а. министърът на електронното управление;"

вв) точка 15 се отменя.

2. В чл. 12:

а) заглавието се изменя така: „Министър на електронното управление";

б) текстът преди т. 1 се изменя така: „Министърът на електронното управление:".

3. В чл. 13, ал. 2, т. 3 в текста преди буква „а" след думите „министъра на вътрешните работи" се поставя запетая, а думите „и председателите на Държавна агенция „Национална сигурност" и Държавна агенция „Електронно управление" се заменят с „министъра на електронното управление и председателя на Държавна агенция „Национална сигурност".

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".

Преходни и заключителни разпоредби към ЗАКОН за изменение и допълнение на Закона за пазарите на финансови инструменти
(ДВ, бр. 25 от 29.03.2022 г., в сила от 29.03.2022 г.)

§ 91. В Закона за киберсигурност (обн., ДВ, бр. 94 от 2018 г.; изм., бр. 69 и 85 от 2020 г. и бр. 15 от 2022 г.) в приложение № 1 към чл. 4, ал. 1, т. 2 в сектор „Банково дело" думите „и инвестиционните посредници" се заличават.

Преходни и заключителни разпоредби към ЗАКОН за изменение и допълнение на Закона за киберсигурност (ДВ, бр. 17 от 13.02.2026 г.)

§ 42. В двумесечен срок от изтичането на срока по § 48 националните компетентни органи предоставят информацията по чл. 6 на министъра на електронното управление.

§ 43. В тримесечен срок от изтичането на срока по § 42 и на всеки две години Националното единно звено за контакт изпраща списък на съществените и важните субекти, както и на субектите, предоставящи услуги за регистрация на имена на домейни на Европейската комисия.

§ 44. В тримесечен срок от приемането на Националната стратегия за киберсигурност министърът на електронното управление уведомява Европейската комисия.

§ 45. В срок три месеца от определянето или създаването на орган за управление на киберкризи министърът на електронното управление уведомява Европейската комисия.

§ 46. В срок три месеца от влизането в сила на този закон министърът на електронното управление нотифицира на Европейската комисия административнонаказателните разпоредби на този закон. При последващи изменения за тях се прилага същият срок за нотифициране.

§ 47. Министерският съвет:

1. в срок 6 месеца от влизането в сила на този закон определя с решение административните органи по чл. 16, ал. 1 и приема методиката по чл. 16, ал. 3, т. 8;

2. в срок 8 месеца от влизането в сила на този закон приема наредбата по чл. 3, ал. 3;

3. в срок 8 месеца от влизането в сила на този закон привежда наредбата по чл. 3, ал. 2 в съответствие с него;

4. в срок 9 месеца от влизането в сила на този закон приема Националната стратегия за киберсигурност.

§ 48. Националните компетентни органи по чл. 16, ал. 1 в срок до 5 месеца от приемането на решението по § 47, т. 1 определят съществените и важните субекти и уведомяват министъра на електронното управление за това.

§ 49. Министърът на енергетиката изгражда, поддържа и развива център за киберсигурност за нуждите на публичните предприятия в сектор „Енергетика".

§ 50. До влизането в сила на наредбата по чл. 3, ал. 3 се прилагат Правилата за минимални изисквания на сигурност на обществените електронни съобщителни мрежи и услуги и методи за управление на риска за тяхната сигурност съгласно чл. 243, ал. 3 от Закона за електронните съобщения.

§ 51. За нарушения на разпоредбите на закона, извършени до 1 юни 2026 г., се налагат глоби и имуществени санкции в размер, намален с 50 на сто от определения в глава трета.

§ 56. В срок до една година от влизането в сила на закона министърът на електронното управление представя пред Съвета за киберсигурност всички извършени преди влизането в сила на закона координирани оценки по чл. 22 от Директива (ЕС) 2022/2555.