ПРОЕКТ!

ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА КИБЕРСИГУРНОСТ

(обн., ДВ., бр. 94 от 2018 г., изм. и доп., бр. 69 и 85 от 2020 г. и бр. 15 и 25 от 2022 г.)

§ 1. В чл. 1, ал. 1 се правят следните изменения:

1. В т. 1 думите „включително дейности и проекти по киберотбрана и по противодействие“ се заменят с „координация и сътрудничество в областта на киберотбраната и противодействието“.

2. В т. 2 думите „мрежова и информационна сигурност“ се заменят с „киберсигурност в Република България“.

§ 2. В чл. 2 ал. 1 се изменя така:

„(1) Киберсигурност означава дейностите, необходими за защита от киберзаплахи на мрежите и информационните системи, на ползвателите на такива мрежи и системи и други лица, засегнати от киберзаплахи.“

§ 3. В чл. 3 се правят следните изменения и допълнения:

1. Заглавието се изменя така:

„Мерки за високо общо ниво на киберсигурност“

2. В ал. 1 думите „мрежова и информационна сигурност“ се заменят с „високо общо ниво на киберсигурност“ и думите „чл. 4, ал. 1“ се заменят с „чл. 4 и чл. 4а“.

3. В ал. 2 думите „мрежова и информационна сигурност, както и други препоръчителни мерки“ се заменят с „постигане на високо общо ниво на киберсигурност за субектите по чл. 4 и чл. 4а с изключение на посочените в чл. 4, ал. 1, т. 3, буква „а“.

4. Алинея 3 и ал. 4 се изменят така:

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

(4) Субектите по чл. 4 и чл. 4а поддържат система за управление на сигурността на информацията, която включва следните организационни мерки:

1. разпределение на отговорностите за киберсигурност;

2. прилагане на политика за киберсигурност;

3. правила и задължения относно обмена на информация за киберсигурността;

4. задължителна оценка на риска;

5. управление на:

а) 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 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 от 27 декември 2022 г.), наричана по-нататък „Директива (ЕС) 2022/2557“;

б) информационните активи, включително човешките ресурси;

в) инцидентите;

г) достъпите (физически и логически);

д) измененията;

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

ж) взаимодействията с трети страни.“

§ 4. Член 4 се изменя така:

„Обхват

Чл. 4. 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 таваните за средни предприятия от посочения член 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 средни предприятия;

3. субекти от видовете, посочени в приложение I или II независимо от техния размер, 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;

5. субекти, предоставящи услуги за регистрация на имена на домейни;

6. образователни институции, когато извършват научноизследователски дейности от критично значение;

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.“

§ 5. Създава се чл. 4а:

„Съществени и важни субекти

Чл. 4а. (1) За целите на закона следните субекти се считат за съществени субекти:

1. субекти от видовете, посочени в приложение I, които надхвърлят таваните 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 предприятия по смисъла на чл. 3, ал. 1 от Закона за малките и средните предприятия;

4. субектите по чл. 4, ал. 1, т. 1;

5. всички други субекти от видовете, посочени в приложение I или II, които са установени като съществени субекти съгласно чл. 4, ал. 1, т. 3, букви „г“ – „ж“;

6. субектите, посочени в чл. 4, ал. 1, 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, ал. 1, т. 3, букви „г“ – „ж“.“

§ 6. В чл. 5 се правят следните изменения:

1. В т. 2 думите „Служба „Военно разузнаване“ и запетаята след тях се заличават.

2. Точка 3 се изменя така:

„3. по отношение на информационните системи, дефинирани като критични в стратегически обекти или субектите, осъществяващи стратегически дейности, определени от ръководителите на стратегическите обекти и възлагащите стратегически дейности, които са от значение за националната сигурност, по смисъла на Наредбата за условията и реда за определяне на мерките за защита на информационните и комуникационните системи на стратегическите обекти от значение за националната сигурност и за осъществяването на контрол.“

3. Точки 4 и 5 се заличават.

§ 7. Член 6 се изменя така:

„Регистър

Чл. 6. (1) Министърът на електронното управление създава, води и поддържа регистър на субектите по чл. 4 и чл. 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 Съюза, на неговия представител, определен съгласно чл. 27а, ал. 2, до 2 месеца от възникването им.

(3) Субектите, посочени в ал. 1 и ал. 2, уведомяват съответния национален компетентен орган по чл. 16 за всяка настъпила промяна в данните, предоставени съгласно ал. 1 и ал. 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.“

§ 8. Създава се чл. 6а:

„Специални закони за сектора

Чл. 6а. (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 от ЕРИКС, компетентните 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.“

§ 9. В чл. 7, ал. 3 думите „а в случаите по чл. 8, ал. 3 – и Национална стратегия за мрежова и информационна сигурност“ и запетаята пред тях се заличават.

§ 10. Член 8 се изменя така:

„Стратегии

Чл. 8. (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 компетентните органи, единните звена за контакт и ЕРИКС съгласно закона, както и координацията и сътрудничеството между тези органи и компетентните 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 компетентните органи съгласно закона и компетентните 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. управление на уязвимостите, включващо насърчаването и улесняването на координираното оповестяване на уязвимости съгласно „Европейската база данни за уязвимости на 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. подпомагане на академичните и научноизследователските институции за разработване, подобряване и насърчаване на внедряването на инструменти за киберсигурност и сигурна мрежова инфраструктура;

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

9. 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. насърчаване на активна киберзащита.

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

§ 11. В чл. 9, ал. 3 се създават т. 8б и 8в:

„8б. министърът на регионалното развитие и благоустройството;

8в. министърът на земеделието;“.

§ 12. В чл. 10 се правят следните изменения:

1. В т. 5 след думата „предложения“ се добавя „към Министерския съвет“.

2. В т. 6 думите „Национален план за управление на киберкризи“ се заменят с „Национален план за реакция при мащабни киберинциденти и кризи, в съответствие с Препоръка (ЕС) 2017/1584 на Европейската комисия от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи“.

§ 13. В чл. 11, ал. 2 се правят следните изменения:

1. В т. 2 думите „координационно-организационна“ се заменят с „координационна“.

2. В т. 3 думите „при създаването и“ се заменят с „в“.

§ 14. В чл. 12 се правят следните изменения и допълнения:

1. В т. 2 думите „мрежова и информационна сигурност в случаите по чл. 8, ал. 3“ се заменят с „киберсигурност“.

2. Точка 6 се изменя така:

„6. 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 глава трета, и дава задължителни предписания за тяхното подобряване. В обхвата на проверките не попадат информационни системи на ведомствата по чл. 5;“.

3. В т. 7 думите „оценка за съответствие с мерките за мрежова и информационна сигурност“ се заменят с „проверки по киберсигурност“ и накрая се добавя „и ал. 2а“.

4. В т. 8 думите „мрежовата и информационната сигурност“ се заменят с „киберсигурността“.

5. Създава се т. 9:

„9. осъществява проверки на предоставените годишни одити от националните компетентни органи, с цел анализ и съответствие с изискванията по този закон.“

§ 15. В чл. 14, ал. 5 думите „по чл. 4, ал. 1“ се заменят с „по чл. 4а“.

§ 16. В чл. 15 се правят следните изменения и допълнения:

1. В ал. 2 в началото се добавя „В“, а думите „администрира и ползва“ се заменят с „се изгражда и развива“.

2. В ал. 3 се създава т. 5:

„5. при настъпване на инцидент с критични системи на стратегическите обекти и дейностите от значение за националната сигурност, ръководителите на субектите незабавно уведомяват центъра по реда на чл. 24.“

3. Алинея 5 се отменя.

4. Алинея 7 се изменя така:

„(7) 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.“

§ 17. В чл. 16 се правят следните изменения и допълнения:

1. В ал. 1 думите „мрежова и информационна сигурност“ се заменят с „киберсигурност“, а думите „приложения № 1 и 2“ се заменят с „Приложения I и II“.

2. В ал. 2 думите „по чл. 4, ал. 1, т. 3 и 4“ се заменят с „по чл. 4, ал. 1, т. 7 и 8“.

3. В ал. 3:

а) в т. 1 думите „мрежовата и информационната сигурност“ се заменят с „киберсигурността“, а думите „операторите на съществени услуги и доставчиците на цифрови услуги“ се заменят с „и на всички други субекти“;

б) в т. 2 думите „по чл. 4, ал. 1“ се заменят с „по чл. 4 и чл. 4а“;

в) в т. 3 думите „операторите на съществени услуги и доставчиците на цифрови услуги“ се заменят със „съществените и важните субекти по този закон“, а думите „мрежовата и информационната сигурност“ се заменят с „киберсигурността“;

г) в т. 4 думите „съвместно с Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA)“ се заличават, а думите „мрежовата и информационната сигурност“ се заменят с „киберсигурността“;

д) в т. 5 думите „със съдействието на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA)“ се заличават;

е) създават се т. 6 и 7:

„6. изготвят ежегодна оценка на риска и икономическия и социален ефект за прилежащия им сектор, която докладват на Националното единно звено за контакт;

7. уведомяват Комисията за идентификационните данни на СЕРИКС по чл. 18, ал. 1;

8. 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. Алинея 5 се изменя така:

„(5) Националните компетентни органи гарантират, че техните СЕРИКС си сътрудничат ефективно, ефикасно и сигурно чрез НЕРИКС.“

5. Алинеи 6, 7, 8 и 9 се отменят.

6. В ал. 10 думите „имат право да“ се заличават.

7. В ал. 12 думата „органите“ се заменя с „Комисията“.

8. Алинея 13 се изменя така:

„(13) Националните компетентни органи:

1. участват в състава на надзорния форум, по смисъла на чл. 32, параграф 4, б. „д“ от Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година 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 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.“

§ 18. В чл. 17 се правят следните изменения и допълнения:

1. В ал. 1 думите „се създава“ се заменят с „е създадено“.

2. В ал. 2 думите „мрежовата и информационната сигурност“ се заменят с „киберсигурността“.

3. Алинея 3 се изменя така:

„(3) Националното единно звено за контакт организира и координира дейността по предоставяне на информацията по чл. 6, ал. 3 на всеки две години.“

4. В ал. 4, т. 2 думите „мрежова и информационна сигурност“ се заменят с „киберсигурност“.

5. Създават се ал. 5а и 5б:

„(5а) Националното единно звено за контакт препраща информацията посочена в чл. 6, ал. 3, с изключение на информацията по чл. 6, ал. 1, т. 3, на Агенцията на Европейския съюз за киберсигурност (ENISA).

(5б) При получаване на информация за трансграничен инцидент от НЕЗК на друга държава членка НЕЗК уведомява съответните НКО/СЕРИКС и координира дейностите по разрешаване на инцидента на национално ниво, както и докладва резултатите на уведомяващия НЕЗК.“

6. В ал. 6 след думите „по ал. 5“ се добавя „и ал. 5а“, а думите „оператора на съществените услуги или на доставчика на цифрови услуги“ се заменят със „съществените и важни субекти“.

7. В ал. 7 думите „по чл. 21, ал. 3, чл. 22, ал. 2, чл. 23, ал. 2 и чл. 25, ал. 3“ се заменят с „от съществените и важните субекти за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях услуги“.

8. Създават се нови ал. 9 и ал. 10:

„(9) Националното единно звено за контакт изготвя годишен обобщен доклад за оценка на риска, базиран на получените анализи от секторните компетентни органи по смисъла на чл. 16, ал. 3, т. 5.

(10) Националното единно звено за контакт при целесъобразност обменя информация с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554.“

9. Досегашната ал. 9 става ал. 11.

§ 19. Създава се чл. 17а:

„Национални рамки за управление на кризи в областта на киберсигурността

Чл. 17а. (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. задачи и отговорности 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. национални 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 ЕС.“

§ 20. В чл. 18 се правят следните изменения и допълнения:

1. В ал. 1 думите „включително Министерството на електронното управление“ се заличават, след думите „компютърната сигурност“ се добавя „(СЕРИКС)“ и думите „мрежова и информационна сигурност“ се заменят с „киберсигурност“.

2. Създава се нова ал. 2:

„(2) 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 сътрудничество с националните екипи за реагиране при инциденти с компютърната сигурност (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. Досегашната ал. 2 става ал. 3 и в нея:

а) в т. 3 буква „б“ се изменя така:

„б) разполагат с достатъчно персонал, за да гарантират предоставянето по всяко време на техните услуги“;

б) в т. 4 думите „мрежова и информационна сигурност“ се заменят с „киберсигурност“.

4. Досегашната ал. 3 става ал. 4 и се изменя така:

„(4) 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. Досегашната ал. 4 става ал. 5.

6. Досегашната ал. 5 става ал. 6 и в нея думите „секторните екипи за реагиране при инциденти с компютърната сигурност“ се заменят със „СЕРИКС“.

7. Досегашната ал. 6 става ал. 7 и в нея думите „Националния екип“ се заменят с „НЕРИКС“.

8. Досегашната ал. 7 става ал. 8.

9. Досегашната ал. 8 става ал. 9 и в нея думите „веднъж на три месеца“ се заменят с „всеки месец“, а думите „Националния екип за реагиране при инциденти с компютърната сигурност“ се заменят с „НЕРИКС“.

10. Досегашните ал. 9 и 10 стават съответно ал. 10 и 11.

§ 21. В чл. 19 се правят следните изменения и допълнения:

1. Алинея 1 се изменя така:

„(1) Национален екип за реагиране при инциденти с компютърната сигурност отговаря на изискванията на чл. 18, ал. 1-6.“

2. В ал. 2, т. 8 думите „инциденти в мрежовата и информационната сигурност“ се заменят с „киберинциденти“.

3. Създават се ал. 4 и 5:

„(4) 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, улесняващ 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“

§ 22. В чл. 20 се правят следните изменения:

1. Алинея 2 се отменя.

2. В ал. 3 думите „споразумение за взаимодействие между заинтересованите ведомства“ се заменят със „споразумения за взаимодействие“.

3. В ал. 4 думите „може да създава междуведомствени оперативни групи“ се заменят със „създава междуведомствена оперативна група“ и след думата „частния“ се добавя „и академичния“.

4. Алинея 5 се изменя така:

„(5) 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 по конституционен ред.“

§ 23. В глава първа се създава чл. 20а:

„Партньорски проверки

Чл. 20а. (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 компетентните 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 договореностите 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.“

§ 24. Създава се нова глава втора с чл. 21-26:

„Глава втора

МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА И ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ

Управление

Чл. 21. (1) Управителните органи на съществените и важните субекти 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 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. (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, съответните европейски и международни стандарти и технически спецификации, 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, например 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. използването 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.

(3) При разглеждане 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.

Координирана оценка на риска за сигурността на критични вериги за доставка

Чл. 23. (1) Съветът по киберсигурността идентифицира и прави оценка на технологичните и нетехнологичните рискове, като изготвя съгласувано с компетентните органи мотивирано предложение до Министерски съвет да ограничи използването на конкретни технологии или на критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, за субектите на този закон, 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 на ниво Европейски съюз. Министерският съвет се произнася с административен акт, издаден по реда на Административнопроцесуалния кодекс в рамките на предоставените му с действащото законодателство правомощия.

Задължения за докладване

Чл. 24. (1) Съществените и важните субекти уведомяват СЕРИКС за всеки значителен инцидент по образец съгласно наредбите по чл. 3 по реда и условията на ал. 5. Актът на уведомяване сам по себе си не води до повишена отговорност за уведомяващия субект.

(2) Засегнатите субекти уведомяват 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 националния компетентен орган, да забавят уведомяването на получателите, докато националния 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. в рамките на 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. в рамките на 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 предходното изречение е 24 часа;

3. по искане на СЕРИКС – междинен доклад, съдържащ актуализирана информация за инцидента;

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

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, субектът представя междинен доклад, съдържащ, до колкото 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 предходното изречение 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 им предоставя цялата налична при него информация.

(8) Когато значителният инцидент засяга две или повече държави членки, НЕРИКС или 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.

(9) 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.

(10) 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.

(11) 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, 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

(12) 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 доброволно уведомление по реда на чл. 27д от субектите, установени като критични съгласно Директива (ЕС) 2022/2557.

Сертифициране на киберсигурността

Чл. 25. За да се докаже съответствие с конкретни изисквания по чл. 22, НКО може да изиска от съществените и важните субекти да използват конкретни 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 година 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 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. 26. Без да се налага употребата на определен тип технология или и с цел хармонизираното прилагане на чл. 22 се насърчава използването на европейски и международни стандарти и технически спецификации от значение за сигурността на мрежовите и информационните системи.“

§ 25. Досегашната глава втора „Мрежова и информационна сигурност“ с чл. 21-27 се отменя.

§ 26. След чл. 27 се създава глава втора „а“ с чл. 27а – 27в:

„Глава втора „а“

ЮРИСДИКЦИЯ И РЕГИСТРАЦИЯ

Юрисдикция и териториалност

Чл. 27а. (1) Субектите, попадащи в обхвата на настоящия 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 Съюза съгласно ал. 2.

(2) Ако субект по ал. 1, т. 2 не е установен в Съюза, но предлага услуги в него, той предоставя информация за своя представител в Съюза 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 Съюза, определен съгласно настоящата алинея, субект, който предлага услуги на територията на Република България, се счита под юрисдикцията на Република България.

Чл. 27б. (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) Държавите членки, които са получили искане за взаимопомощ по отношение на субект, посочен в чл. 27а, ал. 1, т. 2 могат, в рамките на искането, да предприемат подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или който притежава мрежова и информационна система на тяхна територия.

База данни с регистрационни данни на имена на домейни

Чл. 27в. (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, ал. 2 и ал. 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.“

§ 27. След чл. 27в се създава глава втора „б“ с чл. 27г – 27д:

„Глава втора „б“

ОБМЕН НА ИНФОРМАЦИЯ

Споразумения за обмен на информация в областта на киберсигурността

Чл. 27г. (1) Субектите, попадащи в обхвата на настоящия 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 заплахи, 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 компетентните 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. (1) Извън задължението за уведомяване, предвидено в чл. 23, се създава възможността за подаване на уведомления до СЕРИКС/НЕРИКС или, когато е приложимо, до компетентните органи на доброволна основа от:

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

2. 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. Компетентните органи обработват задължителните уведомления с предимство пред доброволните уведомления.

(3) При необходимост, ЕРИКС или компетентните органи предоставят на единните звена 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.

§ 28. След чл. 27д се създава глава втора „в“ с чл. 27е – 27о:

„Глава втора „в“

КОНТРОЛ

Основни аспекти на контрола

Чл. 27е. (1) Контролът за спазване на изискванията по този закон се осъществява от:

1. националните компетентни органи по чл. 16;
2. Министерство на отбраната;
3. Министерство на вътрешните работи;
4. Държавна агенция „Национална сигурност“.

(2) За осъществяване на контрол по този закон органите по ал. 1 оправомощават със заповед служители от техните администрации.

Чл. 27ж. (1) При осъществяване на своите правомощия, по отношение на съществените субекти, органите по чл. 27е имат право:

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

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

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

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

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

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

7. да 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:

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

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

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

4. да 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 компетентните органи съгласно чл. 27в;

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

6. да 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, компетентните органи заявяват целта на своето искане и поясняват исканата информация.

Чл. 27з. 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 компетентния орган 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 компетентният орган реши друго.

Чл. 27и. (1) При осъществяване на своите правомощия органите по чл. 27е могат да издават:

1. предупреждения;

2. да приемат 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, задължение за докладване, както и да определят срокове за изпълнение на такива мерки;

3. разпореждания да преустановяват поведение, което нарушава закона, и да се въздържат от повтарянето на такова поведение;

4. разпореждания да гарантират, че техните мерки за управление на риска в областта на киберсигурността са в съответствие с чл. 22, или да изпълнят задълженията за докладване по чл. 24 по конкретен начин, за което да определят срок;

5. разпореждания на 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 те могат да предприемат в отговор на тази заплаха;

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

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

(2) По отношение на съществените субекти, органите по чл. 27е могат да издават разпореждане за определяне на длъжностно лице по надзор за спазването на чл. 22 и чл. 24 от засегнатите субекти, както и на неговите конкретни задачи и срок за изпълнение.

Чл. 27к. (1) За непредприемане на действията определени по реда на чл. 27и, ал. 1, т. 1-4 и т. 6, компетентният орган по чл. 27е, може временно да спре, или да изиска от съд или съответния компетентен административен орган да спре временно лиценз, регистрация, сертификат или разрешение относно всички или част от съответните предоставени услуги или дейностите, извършвани от съществения субект.

(2) За непредприемане на действията определени по реда на чл. 32, 27и, ал. 1, т. 1-4 и т. 6, компетентният 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 в този съществен субект, да упражнява управленски функции в този субект.

(3) Органите по ал. 1 и ал. 2 се произнасят с индивидуален административен акт, който може да бъде обжалван по реда на Административнопроцесуалния кодекс.

(4) Алинея 1 и ал. 2 не се прилагат по отношение на съществени субекти, които са административните 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 както за съществените, така и за важните субекти. Тези физически лица могат да бъдат подведени под отговорност за неизпълнението на своите задължения по спазването на закона. Настоящата алинея не засяга публичната администрация, по отношение на отговорността на държавните служители и на избраните или назначените длъжностни лица.

Чл. 27л. 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 компетентните органи по чл. 16, да упражняват своите правомощия във връзка със съществен субект, който е установен като критичен съгласно Директива (ЕС) 2022/2557.

Чл. 27м. Компетентни 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 Регламент (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. (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 година 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 от 4 май 2016 г.), и Закона за защита на личните данни.

(2) Когато надзорните органи, посочени в чл. 55 или чл. 56 от Регламент (ЕС) 2016/679, наложат имуществена санкция съгласно чл. 58, параграф 2, буква „и“ от посочения регламент, компетентните органи по този закон не налагат имуществена санкция съгласно чл. 27л по отношение на предходната алинея, 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 случай, 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. (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. компетентните органи по този закон, посредством единното звено за контакт, уведомяват и се консултират с компетентните органи в другите засегнати държави членки относно предприетите надзорни и правоприлагащи мерки;

2. компетентен орган може да поиска от друг компетентен орган да предприеме надзорни или правоприлагащи мерки;

3. когато компетентен орган по този закон получи обосновано искане от друг компетентен орган, включително от друга държава членка, той оказва на искащия орган 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. 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 компетентния 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 на тази държава членка. Преди да отхвърли такова искане, компетентният орган се консултира с другите засегнати компетентни органи, както и, по искане на една от засегнатите държави членки, с Комисията и „Агенцията на Европейския съюз за киберсигурност (ENISA)“.

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

§ 29. Член 28 и чл. 29 се изменят така:

„Отговорност за неизпълнение на принудителни административни мерки

Чл. 28. (1) Административен орган, който не изпълни принудителна административна мярка по смисъла на чл. 27и, ал. 1, т. 2 – т. 7, се наказва с глоба от 10 000 до 100 000 лв.

(2) При повторно нарушение по ал. 1 наказанието е глоба от 20 000 до 200 000 лв.

Имуществени санкции

Чл. 29. (1) Наложените имуществени санкции на съществените и важните субекти съгласно настоящия член във връзка с нарушения на закона, са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата във всеки конкретен случай.

(2) Имуществените санкции се налагат в допълнение към която и да е от мерките, посочени в чл. 27и, ал. 1, т. 2 от б. б) до б. ж).

(3) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 200 000 лева до 2% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения субект, но не по –малко от 20 000 000 лева.

(4) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 100 000 лева до 1,4% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важния субект, но не по-малко от 14 000 000 лева.

(5) Освен имуществената санкция по ал. 3 и ал. 4 на съществените и важните субекти могат да бъдат налагани и една или няколко от мерките по чл. 27и и чл. 27к.

(6) При нарушение на чл. 21, управителите или членовете на управителните органи на съществените и важните субекти подлежат на имуществена санкция в размер на 1000 лв. до 100 000 лв.

(7) Принудителни административни мерки се налагат върху съществен или важен субект с цел да се преустанови нарушение на закона в съответствие с предходно решение на компетентния орган.

(8) Без да се засягат правомощията на компетентните органи по глава втора „в“, имуществени санкции могат да бъдат налагани и на административните органи.

§ 30. В чл. 30 се правят следните изменения и допълнения:

1. В ал. 1 числото „10 000“ се заменя със „100 000“.

2. В ал. 2 числото „15 000“ се заменя със „150 000“.

3. В ал. 3 думите „чл. 15, ал. 6 и чл. 19, ал. 3“ се заменят с „чл. 15, ал. 5“, числото „10 000“ се заменя със „100 000“ и числото „15 000“ се заменя със „150 000“.

§ 31. Създава се чл. 30а:

„Чл. 30а. В случай на неизпълнение на някоя от наложените мерки по чл. 27и, ал. 1, т. 2-7, органите по чл. 27е налагат периодични имуществени санкции на съществен или важен субект в размер на 5 000 лв. за всеки ден неизпълнение.

§ 32. В чл. 31 се правят следните изменения и допълнения:

1. В ал. 1 думите „както и за нарушения по чл. 28, ал. 3 и 4 и по чл. 30, ал. 3 във връзка с чл. 19, ал. 3“ се заличават..

2. В ал. 2 думите „оператори на съществени услуги или от доставчици на цифрови услуги“ се заменят със „съществени и важни субекти“,

§ 33. В допълнителните разпоредби се правят следните изменения и допълнения:

1. Параграф 1 и § 2 се изменят така:

„§ 1. Този закон въвежда изискванията на Директива (ЕС) 2022/2555 на Европейския Парламент и на Съвета от 14 декември 2022 година 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) (ОВ, L 333 от 27 декември 2022 г.).

§ 2. 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.“

2. Създава се § 2а:

„§ 2а. 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/С 324/02)“.

3. В § 3:

а) в т. 1 думите „допълнителните разпоредби на Закона за електронното управление“ се заменят с „Административнопроцесуалния кодекс“;

б) точка 2 се изменя така:

„2. 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 година 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) (ОВ, L 333 от 27 декември 2022 г.);“;

в) създава се т. 2а:

„2а. „Национална стратегия за киберсигурност“ е съгласувана рамка на държава членка, съдържаща стратегически цели и приоритети в областта на киберсигурността и управленските методи за постигането им в тази държава членка;“;

г) създава се т. 4а:

„4а. „Система за имена на домейни, която представлява йерархично“ или „DNS“ означава йерархична разпределена мрежова система за именуване, която позволява идентифициране на интернет услуги и ресурси, позволявайки на домейни, разпределяща заявки устройствата на крайните ползватели да използват интернет маршрутизация и услуги за свързване, за да достигнат до тези услуги и ресурси;“;

д) точка 5 се изменя така:

„5. „Доставчик на DNS услуги“ означава 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;“;

е) създава се т. 8а:

„8а. „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;“;

ж) създава се т. 11а:

„11а. „Значителна киберзаплаха“ е киберзаплаха, за която въз основа на техническите ѝ 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;“;

з) създава се т. 15а:

„15а. „Мащабен киберинцидент“ означава инцидент, който причинява степен на смущение, надхвърляща способността на дадена държава членка да реагира на него, или който има значително въздействие върху най-малко две държави членки;“;

и) в т. 21 думите „мрежова и информационна сигурност“ се заменят с „киберсигурност“;

к) точка 22 се изменя така:

„22. „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 година 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);“;

л) създават се т. 27а-27в:

„27а. „ИКТ продукт“ означава ИКТ продукт съгласно определението в член 2, точка 12 от Регламент (ЕС) 2019/881;

27б. „ИКТ услуга“ означава ИКТ услуга съгласно определението в член 2, точка 13 от Регламент (ЕС) 2019/881;

27в. „ИКТ процес“ означава ИКТ процес съгласно определението в член 2, точка 14 от Регламент (ЕС) 2019/881;“;

м) точка 29 се изменя така:

„29. „Регистър на имена на домейни от първо ниво“ означава 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;“;

н) създава се т. 29а:

„29а. „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;“;

о) създават се т. 31а-31г:

„31а. „Удостоверителна услуга“ означава удостоверителна услуга съгласно определението в член 3, точка 16 от Регламент (ЕС) № 910/2014;

31б. „Доставчик на удостоверителна услуга“ означава доставчик на удостоверителна услуга съгласно определението в член 3, точка 19 от Регламент (ЕС) № 910/2014;

31в. „Квалифицирана удостоверителна услуга“ означава квалифицирана удостоверителна услуга съгласно определението в член 3, точка 17 от Регламент (ЕС) № 910/2014;

31г. „Доставчик на квалифицирана удостоверителна услуга“ е доставчик на квалифицирана удостоверителна услуга съгласно определението в член 3, точка 20 от Регламент (ЕС) № 910/2014;“;

п) създава се т. 32а:

„32а. „Стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета (29);“;

р) точка 36 се изменя така:

„36. „Цифрова инфраструктура“ е инфраструктурата, която включва категориите, посочени в Приложение № 1, т. 8;“;

с) създават се т. 37-59:

„37. „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. „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. „Платформа на услуги за социална мрежа“ означава платформа, позволяваща на крайните ползватели да се свързват, споделят, откриват и общуват помежду си посредством множество устройства, по-специално чрез чатове, публикации, видеоклипове и препоръки;

40. „Обществена електронна съобщителна мрежа“ означава обществена електронна съобщителна мрежа по смисъла на § 1, т. 39 от допълнителните разпоредби на Закона за електронните съобщения;

41. „Електронна съобщителна услуга“ означава електронна съобщителна услуга по смисъла на § 1, т. 17 от допълнителните разпоредби на Закона за електронните съобщения;

42. „Субект“ означава 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. „Доставчик на управлявани услуги“ означава 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. „Доставчик на управлявани услуги за сигурност“ означава доставчик на управлявани услуги, който извършва или предоставя помощ за дейности, свързани с управлението на риска в областта на киберсигурността;

45. „Разузнавателни сведения за заплахи“ означава 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 ограничаването на последствията от инцидент с ИКТ или от киберзаплаха, включително техническите белези на дадена кибератака, отговорните за нея лица и техният начин на действие и мотивация;

46. „Уязвимо място“ означава слабост, тенденция или недостатък на актив, система, процес или контролна функция, които могат да бъдат използвани;

47. „Тестване за проникване (TLPT)“ означава 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. „Риск в областта на ИКТ, пораждан от трета страна“ означава 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. „Трета страна доставчик на услуги в областта на ИКТ“ означава предприятие, което предоставя услуги в областта на ИКТ;

50. „Вътрешногрупов доставчик на услуги в областта на ИКТ“ означава 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. „Услуги в областта на ИКТ“ означава 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. „Критична или важна функция“ означава 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. „Трета страна критичен доставчик на услуги в областта на ИКТ“ означава трета страна, която е доставчик на услуги в областта на ИКТ, определен като имащ критично значение в съответствие с чл. 27з;

54. „Трета страна доставчик на услуги в областта на ИКТ, установен в трета държава“ означава 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. „Дъщерно предприятие“ означава дъщерно предприятие по смисъла на член 2, точка 10 и член 22 от Директива 2013/34/ЕС;

56. „Основни стопански дейности“ – по смисъла на § 1, т. 44 от допълнителните разпоредби на Закон за възстановяване и преструктуриране на кредитни институции и инвестиционни посредници ;

57. „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. „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 Съюза, 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 Съюза;

59. „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.“

§ 34. Приложенията към чл. 4, ал. 1, т. 2 се изменят така:

Приложение I
към чл. 4, ал. 1, т. 2

Списък на секторите и подсекторите

Сектор	Подсектор	Вид субект	Съответствие
1. Енергетика	а) Електроенергия	—Електроенергийни предприятия съгласно определението в член 2, точка 57 от Директива (ЕС) 2019/944 на Европейския парламент и на Съвета ([1]), които осъществяват „доставките“, посочени в член 2, точка 12 от същата директива =-	– "Енергийно предприятие" по смисъла на § 1, т. 24 от допълнителните разпоредби на Закона за енергетиката – "Доставка" по смисъла на § 1, т. 16 от допълнителните разпоредби на Закона за енергетиката
		—Оператори на разпределителни системи съгласно определението в член 2, точка 29 от Директива (ЕС) 2019/944	– "Оператор на разпределителна мрежа" по смисъла на § 1, т. 34б 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
		— Оператори на преносни системи съгласно определението в член 2, точка 35 от Директива (ЕС) 2019/944	— „Оператор на преносна мрежа“ по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката
		— Производители съгласно определението в член 2, точка 38 от Директива (ЕС) 2019/944	
		— Номинирани оператори на пазара на електроенергия съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета ([2]) — Участници на пазара съгласно определението в член 2, точка 25 от Регламент (ЕС) 2019/943, 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 — 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	
	б) Районно отопление и охлаждане	— Оператори на районни отоплителни системи или районни охладителни системи съгласно определението в член 2, точка 19 от Директива (ЕС) 2018/2001 на Европейския парламент и на Съвета ([3])	
	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 2009/119/ЕО на Съвета ([4])	
	г) Природен газ	— Предприятия за доставка съгласно определението в член 2, точка 8 от Директива 2009/73/ЕО на Европейския парламент и на Съвета ([5])	— „Краен снабдител“ по смисъла на § 1, т. 28а от

			допълнителните разпоредби на Закона за енергетиката
		— Оператори на газоразпределителни системи съгласно определението в член 2, точка 6 от Директива 2009/73/ЕО	– „Оператор на разпределителна мрежа“ по смисъла на § 1, т. 34б от допълнителните разпоредби на Закона за енергетиката
		— Оператори на газопреносни системи съгласно определението в член 2, точка 4 от Директива 2009/73/ЕО	– „Оператор на преносна мрежа“ по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката
		— Оператори на системи за съхранение съгласно определението в член 2, точка 10 от Директива 2009/73/ЕО	– „Оператор на съоръжение за съхранение“ по смисъла на § 1, т. 34г от допълнителните разпоредби на Закона за енергетиката
		— Оператори на системи за ВПГ съгласно определението в член 2, точка 12 от Директива 2009/73/ЕО	– „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 1 от Директива 2009/73/ЕО	– „Производител“ по смисъла на § 1, т. 46 от допълнителните разпоредби на

			Закона за енергетиката
		—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, използвани за търговски цели	
		—Управляващи летища органи съгласно определението в член 2, точка 2 от Директива № 2009/12/ЕО на Европейския парламент и на Съвета ([6]), летища съгласно определението в член 2, точка 1 от същата директива, включително основните летища, изброени в раздел 2 от приложение II към Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета ([7]), и субекти, експлоатиращи спомагателни инсталации, намиращи се на летищата	– „Летищна администрация“ по смисъла на § 3, т. 15 от допълнителните разпоредби на Закона за гражданското въздухоплаване –„Летищен оператор“ по смисъла на § 3, т. 16 от допълнителните разпо- редби на Закона за гражданското въздухоплаване – „Летище“ по смисъла на § 3, т. 13 от допълнителните разпоредби на Закона за гражданското въздухоплаване
		—Оператори по контрола на управлението на 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 ([8])	– „Управление на въздушното движение“ по смисъла на § 3, т. 44 от допълнителните

			разпоредби на Закона за гражданското въздухоплаване
	б) Железопътен	— Управители на инфраструктура съгласно определението в член 3, точка 2 от Директива 2012/34/ЕС на Европейския парламент и на Съвета ([9])	– „Управител на железопътна инфраструктура“ по смисъла на § 1, т. 2 от допълнителните разпоредби на Закона за железопътния транспорт
		— Железопътни предприятия, съгласно определението в член 3, точка 1 от Директива 2012/34/ЕС, включително оператори на обслужващи съоръжения, посочени в член 3, точка 12 от същата директива	– „Железопътно предприятие“ по смисъла на чл. 48 от Закона за железопътния транспорт – „Оператор на обслужващо съоръжение“ по смисъла на § 1, т. 51 от допълнителните разпоредби на Закона за железопътния транспорт
	в) Воден	— 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 ([10]), с изключение на отделните кораби, експлоатирани от тези предприятия	– „Компания“ по смисъла на § 1, т. 12 от допълнителните разпоредби на Наредбата за условията и реда за постигане сигурността на корабите, пристанищата и пристанищните райони (ДВ, бр. 99 от 2014 г.)

		—Управителни органи на пристанищата съгласно определението в член 3, точка 1 от Директива 2005/65/ЕО на Европейския парламент и на Съвета ([11]), включително техните пристанищни съоръжения съгласно определението в член 2, точка 11 от Регламент (ЕО) № 725/2004, и субекти, извършващи строителни работи и експлоатиращи оборудване на територията на пристанищата	– „Пристанище“ по смисъла на чл. 92, ал. 1 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България – Чл. 117, ал. 1 и чл. 117а, ал. 1, 2, 3 и 4 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България
		—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 ([12])	– Чл. 244а, ал. 1 и 2 от Кодекса на търговското корабоплаване –Чл. 115м, ал. 1, т. 12, 13, 14 и 15 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България
	г Автомоби) лен	—Пътни органи съгласно определението в член 2, точка 12 от Делегиран регламент (ЕС) 2015/962 на Комисията ([13]), 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 съгласно определението в член 4, точка 1 от	„Интелигентни транспортни системи“ по

		Директива 2010/40/ЕС на Европейския парламент и на Съвета ([14])	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 ([15])	
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 ([16])	Закона за пазарите на финансови инструменти
		—Централни контрагенти (ЦК) съгласно определението в член 2, точка 1 от Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета ([17])	
5. Здравеопазване		—Доставчици на здравно обслужване съгласно определението в член 3, буква ж) от Директива 2011/24/ЕС на Европейския парламент и на Съвета ([18])	Закона за лечебните заведения
		—Референтни лаборатории на ЕС съгласно определението в член 15 от Регламент (ЕС) 2022/2371 на Европейския парламент и на Съвета ([19])	
		—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 ([20]) —Субекти, произвеждащи основни фармацевтични продукти и препарати, съгласно определението в раздел B, разделение 21 на NACE Rev. 2 —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 ([21])	
6. Питейна вода		Доставчици и дистрибутори на води, предназначени за консумация от човека съгласно определението в член 2, точка 1, буква а) от Директива (ЕС) 2020/2184 на Европейския парламент и на Съвета ([22]), с изключение на дистрибуторите, за които дистрибуцията на вода за	Допълнителните разпоредби на Наредба № 9 от 2001 г. за качеството на

		консумация от човека е несъществена част от общата им дейност по дистрибуция на други стоки и продукти	водата, предназначена за питейно-битови цели (ДВ, бр. 30 от 2001 г.)
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 91/271/ЕИО на Съвета ([23]), 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	
		— Доставчици на обществено достъпни електронни съобщителни услуги	
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, ал. 1, т. 2

ДРУГИ КРИТИЧНИ СЕКТОРИ

Сектор	Подсектор	Вид субект	Съответствие
1. Пощенски и куриерски услуги		Доставчици на пощенски услуги съгласно определението в член 2, точка 1а от Директива 97/67/ЕО, включително доставчици на куриерски услуги	ЗАКОН за пощенските услуги
2. Управление на отпадъците		Предприятия, извършващи управление на отпадъците съгласно определението в член 3, точка 9 от Директива 2008/98/ЕО на Европейския парламент и на Съвета ([1]), с изключение на предприятия, за които управлението на отпадъците не е основна икономическа дейност	ЗАКОН 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 ([2]), и предприятия, извършващи производство на изделия, посочени в член 3, точка 3 от същия регламент, от вещества или смеси	Закон за защита от вредното въздействие на химичните вещества и 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 ([3]), които се занимават с дистрибуция на едро и индустриално производство и преработване	„предприятие за производство на храни“ означава всяко предприятие с или без стопанска цел, обществено или частно, което извършва някоя от дейностите, свързани с който и да било етап на производство, преработка и разпространение на храни; Преходни и Заключителни разпоредби

			КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ХРАНИТЕ § 56. В едномесечен срок от влизането в сила на този закон Министерството на икономиката предоставя регистъра на предприятията за производство на храни и документацията към него на органите по чл. 12, ал. 2.
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 ([4]), 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 ([5]), с изключение на субектите, произвеждащи медицински изделия съгласно определението в приложение I, точка 5, пето тире от настоящата директива	Закон за медицинските изделия Чл. 2. (1) В зависимост от предназначеното от производителя действие медицинските изделия се разделят на: 1. ин витро диагностични медицински изделия; 2. активни имплантируеми медицински изделия; 3. медицински изделия, различни от посочените в т. 1 и 2.
	б) Производство на компютри, електронни и оптични продукти	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 26 на NACE Rev. 2	Закон за административното регулиране на производството на оптични дискове и матрици
	в) Производство на електрически съоръжения	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 27 на NACE Rev. 2	сектор Производство на електрически съоръжения (код 27 по КИД-2008) Закон за енергетиката Чл. 1. (Доп. - ДВ, бр. 74 от 2006 г., в сила от 08.09.2006 г., изм. - ДВ, бр. 49 от 2007 г., изм. - ДВ, бр. 54 от 2012 г., в сила от 17.07.2012 г., доп. - ДВ, бр. 11 от 2023 г.) Този закон урежда обществените отношения, свързани с осъществяването на

			дейностите по производство, внос и износ, пренос, разпределение, съхранение на електрическа и топлинна енергия и природен газ, пренос на нефт и нефтопродукти по тръбопроводи, търговия с електрическа и топлинна енергия и природен газ, както и правомощията на държавните органи по определянето на енергийната политика, регулирането и контрола.
	г) Производство на машини и оборудване, некласифициран и другаде	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 28 на NACE Rev. 2	
	д) Производство на моторни превозни средства, ремаркета и полуремаркета	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 29 на NACE Rev. 2	
	е) Производство на друго транспортно оборудване	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 30 на NACE Rev. 2	
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	

Преходни и заключителни разпоредби

§ 35. До 17 януари 2025 г. нзционалните компетентни органи предоставят информацията по чл. 6 на министъра на електронното управление

§ 36. До 17 април 2025 г. и на всеки две години Националното единно звено за контакт изпраща списък на съществените и важните субекти, както и субекти, предоставящи услуги за регистрация на имена на домейни на Европейската комисия.

§ 37. Министъра на електронното управление уведомява Комисията за приетата национална стратегия за киберсигурност в рамките на три месеца от приемането ѝ.

§ 38. В срок от три месеца от определянето или създаването на орган за управление на киберкризи, министъра на електронното управление уведомява Комисията.

§ 39. Най-късно до 17 януари 2025 г. министъра на електронното управление нотифицира на Комисията административнонаказателните разпоредби на този закон, както и последващите изменения в тях.

§ 40. Министерският съвет:

1. в срок до три 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 8 месеца от влизането в сила на закона привежда наредбата по чл. 3, ал. 2 в съответствие с него.

§ 41. Административните органи по чл. 16, ал. 1 в срок до 5 месеца от приемането на решението по § 41, т. 1 определят съществените и важните субекти и уведомяват министъра на електронното управление за това.

§ 42. 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., бр. 7, 21, 28 и 77, 94 от 2018 г., бр. 17, 47, 74, 94 и 100 от 2019 г., бр. 28, 51, 62 и 69 от 2020 г.; Решение № 15 на Конституционния съд от 2020 г. – бр. 101 от 2020 г.; изм., бр. 105 от 2020 г., бр. 20 от 2021 г., бр. 22 и 32 от 2022 г., бр. 58 и 84 от 2023 г. и бр. 41 от 2024 г.) се правят следните изменения и допълнения:

1. В чл. 16, се създава ал. 2а:

„(2а) Национален компетентен орган за субектите по чл. 4, ал. 1, т. 3, буква а) и б) е Комисията за регулиране на съобщенията.“

2. В чл. 30, ал. 1, т. 22 думите „като при необходимост си съдейства с компетентните органи по чл. 244а, ал. 3“ се заличават.

3. В чл. 73, ал. 4, т. 2, буква „г“ думите „глава петнадесета, раздел I“ се заменят със „Закона за киберсигурност“.

4. В глава петнадасета:

а) в наименованието думите „Сигурност на електронните съобщителни мрежи и услуги“ и запетаята след тях се заличават;

б) раздел I се отменя.

§ 43. В Закона за електронното управление (обн., ДВ, бр. 46 от 12.06.2007 г., в сила от 13.06.2008 г., изм. и доп., бр. 82 от 16.10.2009 г., в сила от 16.10.2009 г., изм., бр. 20 от 28.02.2013 г., доп., бр. 40 от 13.05.2014 г., в сила от 1.07.2014 г., изм., бр. 13 от 16.02.2016 г., в сила от 15.04.2016 г., изм. и доп., бр. 38 от 20.05.2016 г., в сила от 21.05.2017 г., бр. 50 от 1.07.2016 г., в сила от 1.07.2016 г., доп., бр. 62 от 9.08.2016 г., в сила от 1.07.2016 г., бр. 98 от 9.12.2016 г., в сила от 1.01.2017 г., изм., бр. 88 от 23.10.2018 г., изм. и доп., бр. 94 от 13.11.2018 г., бр. 94 от 29.11.2019 г., в сила от 29.11.2019 г., доп., бр. 102 от 31.12.2019 г., в сила от 29.11.2019 г., изм., бр. 69 от 4.08.2020 г., доп., бр. 85 от 2.10.2020 г., в сила от 2.10.2020 г., изм. и доп., бр. 15 от 22.02.2022 г., в сила от 22.02.2022 г., доп., бр. 66 от 1.08.2023 г., в сила от 5.08.2023 г., изм. и доп., бр. 80 от 19.09.2023 г., в сила от 19.09.2023 г.) в §1, т. 42 от Допълнителните разпоредби, думите „на чл. 17“ се заменят с „на чл. 19“.

§ 44. Законът влиза в сила след обнародване в държавен вестник.