ТАБЛИЦА ЗА СЪОТВЕТСТВИЕ С ПРАВОТО НА ЕВРОПЕЙСКИЯ СЪЮЗ		
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) с Закона за киберсигурност	**Закон за киберсигурност и Проект на Закон за изменение и допълнение на Закон за киберсигурност, Административнопроцесуален кодекс, Закон за административните нарушения и наказания, Проект на НИД на Наредбата за минималните изисквания за мрежова и информационна сигурност.**	**Степен на съответствие**
ГЛАВА I **ОБЩИ РАЗПОРЕДБИ** **Предмет** **Член 1** 1. С настоящата директива се установяват мерки, които имат за цел постигане на високо общо ниво на киберсигурност в Съюза, с оглед подобряване на функционирането на вътрешния пазар.	**Закон за киберсигурност** **Предмет** **Чл. 1.** (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност. (2) С този закон се определят и правомощията и функциите на компетентните органи в областта на киберсигурността. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Предмет** **Чл. 1. (1)** Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, координация и сътрудничество в областта на киберотбрана и противодействието на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на киберсигурност в Република България. (2) С този закон се определят и правомощията и функциите на компетентните органи в областта на киберсигурността.	Пълно съответствие
2. За тази цел с настоящата директива се установяват:	**Закон за киберсигурност** **Предмет**	Пълно съответствие

а) задължения за държавите членки да приемат национални стратегии за киберсигурност и да определят или създадат компетентни органи, органи за управление на киберкризи, единни звена за контакт по въпросите на киберсигурността (единни звена за контакт) и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС);	**Чл. 1. (1)** Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност. **Киберсигурност. Мрежова и информационна сигурност** **Чл. 2. (1)** Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им. (2) Киберсигурността включва мрежова и информационна сигурност, противодействие на киберпрестъпността и киберотбрана. (3) Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях. **Стратегии** **Чл. 8.** (1) Националната стратегия за киберсигурност е стратегическа рамка на политиката за киберсигурност, която включва: 1. цели, принципи и приоритети; 2. области на действие и мерки: а) система за киберсигурност; б) мрежова и информационна сигурност; в) противодействие на киберпрестъпността; г) киберотбрана; д) киберразузнаване; 3. взаимодействие между държава, бизнес и общество; 4. развитие и подобряване на регулаторната рамка;	

	5. повишаване на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността; 6. международно взаимодействие; 7. кибердипломация; 8. взаимодействие на техническо, оперативно и стратегическо (политическо) ниво. (2) Националната стратегия за мрежова и информационна сигурност е стратегическа рамка на политиката за мрежова и информационна сигурност, която включва: 1. цели и приоритети относно мрежовата и информационната сигурност; 2. управленска рамка за постигане на целите и приоритетите по т. 1, включително функциите и отговорностите на държавните органи и на други участници; 3. мерки във връзка с подготвеността, реагирането и възстановяването в мрежите и информационните системи, включително сътрудничеството между публичния и частния сектор; 4. съществена информация за образователните и обучителните програми и програмите за повишаване на осведомеността във връзка с мрежовата и информационната сигурност; 5. посочване на плановете за научноизследователска и развойна дейност относно мрежовата и информационната сигурност; 6. план за оценка на риска с цел набелязване на рисковете; 7. списък на различните участници в изпълнението на стратегията. (3) Национална стратегия за мрежова и информационната сигурност се изготвя, когато Националната стратегия за киберсигурност не съдържа информацията по ал. 2. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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 обществената 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.“	

б) 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;	**Закон за киберсигурност** Предмет Чл. 1. (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност. Мерки за мрежова и информационна сигурност Чл. 3. (1) Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите по чл. 4, ал. 1 и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране. (2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Минималният обхват на мерките за мрежова и информационна сигурност, както и други препоръчителни мерки, се определят с наредба на Министерския съвет по предложение на министъра на електронното управление. Мерките не може да налагат използването на определен тип технология. (3) Наредбата по ал. 2 не се прилага за ведомствата и функциите им по чл. 5, т. 2. (4) Субектите по чл. 4, ал. 1, т. 1 и 2 поддържат система за управление на сигурността на информацията, която включва следните минимални организационни мерки: 1. разпределение на отговорностите за мрежовата и информационната сигурност; 2. прилагане на политика за мрежовата и информационната сигурност; 3. управление на: а) риска; б) информационните активи, включително човешките ресурси; в) инцидентите; г) достъпите (физически и логически); д) измененията; е) непрекъснатостта на дейността и/или услугите (съществени, цифрови); ж) взаимодействията с трети страни.	Пълно съответствие

	Проект на Закон за изменение и допълнение на Закон за киберсигурност **Предмет** Чл. 1. (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, координация и сътрудничество в областта на киберотбрана и противодействието на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на киберсигурност в Република България. (2) С този закон се определят и правомощията и функциите на компетентните органи в областта на киберсигурността. Мерки за високо общо ниво на киберсигурност Чл. 3. (1) Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на субектите по чл. 4 и чл. 4а и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране. (2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност за субектите по чл. 4 и чл. 4а с изключение на посочените в чл. 4, т. 3, буква „а“, се определят с наредба на Министерския съвет по предложение на министъра на електронното управление. Мерките не може да налагат използването на определен тип технология. (3). Минималният обхват на мерките за постигане на високо общо ниво на киберсигурност и критериите за докладване на инциденти за субектите по чл. 4, т. 3, буква а), се определят с наредба на Министерския съвет по предложение на Комисията за регулиране на съобщенията и министъра на електронното управление. (4) Наредбата по ал. 2 не се прилага за ведомствата по чл. 5, т. 2.	
в) правила и задължения относно обмена на информация за киберсигурността;	**Закон за киберсигурност** **Предмет** **Чл. 1.** (1) Този закон урежда дейностите по:	Пълно съответствие

	1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността; 2. предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Предмет** **Чл. 1.** (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, координация и сътрудничество в областта на киберотбрана и противодействието на киберпрестъпността;	
г) задължения за надзор и правоприлагане за държавите членки.	**Закон за киберсигурност** **Предмет** **Чл. 1.** (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, включително дейности и проекти по киберотбрана и по противодействие на киберпрестъпността; **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Предмет** **Чл. 1.** (1) Този закон урежда дейностите по: 1. организацията, управлението и контрола на киберсигурността, координация и сътрудничество в областта на киберотбрана и противодействието на киберпрестъпността;	Пълно съответствие
Обхват **Член 2** 1. Настоящата директива се прилага за публични или частни субекти от видовете, посочени в приложение I или II, които отговарят на критериите за средни предприятия съгласно член 2 от приложението към Препоръка 2003/361/ЕО или надхвърлят таваните за средни	**Закон за киберсигурност** **Обхват** **Чл. 4. (1)** С този закон се определят изискванията към: 1. административните органи; 2. операторите на съществени услуги и доставчиците на цифрови услуги – за всеки сектор, подсектор и услуги, посочени в приложения № 1 и 2; 3. лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги, когато тези лица предоставят административни услуги по електронен път;	Пълно съответствие

предприятия, посочени в параграф 1 от същия член, и които предоставят своите услуги или извършват дейности в рамките на Съюза. Член 3, параграф 4 от приложението към посочената препоръка не се прилага за целите на настоящата директива.	4. организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път. (2) Оператор на съществени услуги е публичен или частен субект от посочените в приложение № 1 категории, който отговаря на следните критерии: 1. да предоставя съществена услуга, и 2. предоставянето на тази съществена услуга да зависи от мрежи и информационни системи, и 3. инцидентите в мрежовата и информационната сигурност да имат значително увреждащо въздействие върху предоставянето на тази услуга. (3) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1 определят операторите на съществени услуги съгласно критериите по ал. 2 и в съответствие с методика, приета от Министерския съвет, и уведомяват министъра на електронното управление за това. Методиката се приема по предложение на министъра на електронното управление. (4) Когато оператор предоставя съществена услуга в две или повече държави – членки на Европейския съюз, административният орган по чл. 16, ал. 1 провежда консултации със съответните държави преди вземането на решение относно определянето на оператора. (5) Операторите на съществени услуги спазват изискванията за мрежова и информационна сигурност, предвидени в този закон, само по отношение на предоставяните от тях съществени услуги. (6) Когато в правен акт на Европейския съюз или в закон, който е специален за конкретен сектор или услуга, посочени в приложения № 1 и 2, се предвижда операторите на съществени услуги или доставчиците на цифрови услуги да гарантират мрежовата и информационната си сигурност или да уведомяват за инциденти, се прилагат тези актове, при условие че техните изисквания са най-малкото равностойни като резултат на задълженията, предвидени в този закон.	

	Проект на Закон за изменение и допълнение на Закон за киберсигурност **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 ЕС. При установяване размера на предприятието не се прилага чл. 4 ал. 9 от Закона за малките и средни предприятия.	
2. Независимо от техния размер, настоящата директива се прилага също за субекти от видовете, посочени в приложение I или II, когато: а) услугите се предоставят от: i) доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги;	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;	Пълно съответствие
ii) доставчици на удостоверителни услуги;	б) услугите се предоставят от доставчици на удостоверителни услуги;	Пълно съответствие
iii) регистри на имена на домейни от първо ниво и доставчици на системни услуги за имена на домейни;	в) услугите се предоставят от регистри на имена на домейни от първо ниво и доставчици на системни услуги за имена на домейни;	Пълно съответствие
субектът е единствен доставчик в дадена държава членка на услуга, която е от съществено значение за поддържането на критични обществени и икономически дейности;	г) субектът е единствен доставчик на услуга, която е от съществено значение за поддържането на критични обществени и икономически дейности;	Пълно съответствие

в) смущение в предоставяната от субекта услуга би могло да окаже значително въздействие върху обществената безопасност, обществената сигурност или общественото здраве;	д) смущение (за определено време) в предоставяната от субекта услуга би могло да окаже значително въздействие върху обществената безопасност, обществената сигурност или общественото здраве;	Пълно съответствие
г) 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;	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;	Пълно съответствие
д) субектът е критичен поради своята специфична значимост на национално или регионално равнище за конкретния сектор или вид услуга или за други взаимозависими сектори в държавата членка;	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;	Пълно съответствие
е) субектът е орган на публичната администрация: i) на централното правителство, определен от държава членка в съответствие с националното право; или ii)на регионално равнище, определено от държава членка в съответствие с националното право, който след оценка, основана на риска, предоставя услуги, чието смущение би могло да има значително въздействие върху критични обществени или икономически дейности	Чл. 4. С този закон се определят изискванията към: 1. административните органи;	Пълно съответствие.
3. Независимо от размера им, настоящата директива се прилага за субекти, установени като критични субекти съгласно Директива(ЕС) 2022/2557.	4.Субекти, установени като критични субекти съгласно Директива (ЕС) 2022/2557.	Пълно съответствие

4. Независимо от размера им, настоящата директива се прилага за субекти, предоставящи услуги за регистрация на имена на домейни.	5.Субекти, предоставящи услуги за регистрация на имена на домейни.	Пълно съответствие
5. Държавите членки могат да предвидят настоящата директива да се прилага за: а) органи на публичната администрация на местно равнище; б) образователни институции, по-специално когато извършват научноизследователски дейности от критично значение.	6. Образователни институции, когато извършват научноизследователски дейности от критично значение.	Пълно съответствие
6. Настоящата директива не засяга отговорността на държавите членки да опазят националната сигурност и правомощието им да гарантират други основни функции на държавата, включително да осигуряват нейната териториална цялост и да поддържат законността и реда. 7. Настоящата директива не се прилага за органи на публичната администрация, които извършват дейности в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително предотвратяването, разследването, разкриването и наказателното преследване на престъпления. 8. Държавите членки могат да предвидят специфични субекти, които извършват дейности в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително	**Закон за киберсигурност** **Изключения** **Чл. 5.** Този закон не се прилага: 1. за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация; 2. (изм. – ДВ, бр. 69 от 2020 г.) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция "Национална сигурност", Държавна агенция "Разузнаване", Държавна агенция "Технически операции", Служба "Военно разузнаване" и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители; 3. по отношение на предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги по смисъла на Закона за електронните съобщения, с изключение на чл. 14, ал. 5, чл. 15, ал. 6 и чл. 19, ал. 3; 4. за доставчици на удостоверителни услуги по смисъла на чл. 3, т. 19 от Регламент (ЕС) № 910/2014 г. на Европейския парламент	Пълно съответствие

предотвратяването, разследването, разкриването и наказателното преследване на престъпления, или които предоставят услуги изключително на органите на публичната администрация, посочени в параграф 7 от настоящия член, да не са задължени да спазват задълженията, предвидени в член 21 или член 23 по отношение на тези дейности или услуги. В такива случаи надзорните и правоприлагащите мерки, посочени в глава VII, не се прилагат по отношение на тези конкретни дейности или услуги. Когато субектите извършват дейности или предоставят услуги изключително от вида, посочен в настоящия параграф, държавите членки могат да решат също така да освободят тези субекти от задълженията, предвидени в членове 3 и 27.	и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.); 5. за доставчици на цифрови услуги, които са микро- и малки предприятия по смисъла на чл. 3, ал. 2 и 3 от Закона за малките и средните предприятия. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 5**. Този закон не се прилага: 1. за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация; 2. (изм. – ДВ, бр. 69 от 2020 г.) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция "Национална сигурност", Държавна агенция "Разузнаване", Държавна агенция "Технически операции", и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители; 3. по отношение на 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 НАРЕДБА 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.	
9. Параграфи 7 и 8 не се прилагат, когато даден субект действа като доставчик на удостоверителни услуги.		Пълно съответствие

10. Настоящата директива не се прилага за субекти, които държавите членки са освободили от обхвата на Регламент (ЕС) 2022/2554 в съответствие с член 2, параграф 4 от посочения регламент.	**Закон за киберсигурност** **Национални компетентни органи** **Чл. 16.(13)** Националните компетентни органи: 1. участват в състава на надзорния форум, по смисъла на чл. 32, параграф 4, буква „д“ от Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ, L 333/1 от 27 декември 2022 г.)“, наричан по-нататък „Регламент (ЕС) 2022/2554“; 2. оказват съдействие на компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554 и предоставят относими технически становища по тяхно искане; 3. сключват споразумения за сътрудничество с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554, чрез които се създават механизми за координация, включително за координиране на надзорните дейности по отношение на съществените или важните субекти, по смисъла на този закон, които са определени като трети страни, критични доставчици на услуги в областта на ИКТ, съгласно чл. 31 от същия регламент; 4. провеждат, в съответствие с националното право, проверки на място на трети страни, критични доставчици на услуги в областта на ИКТ, съгласно чл. 31 от Регламент (ЕС) 2022/2554, съвместно с компетентните органи по чл. 46 от същия регламент; 5. обменят на информация с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554.	Пълно съответствие
11. Задълженията, предвидени в настоящата директива, не водят до предоставянето на информация, разкриването на която противоречи на основните интереси на националната сигурност, обществената сигурност или отбраната на държавите членки.	**Закон за киберсигурност** **Изключения** Чл. 5. Този закон не се прилага: 1. за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация; 2. (изм. – ДВ, бр. 69 от 2020 г.) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция "Национална сигурност", Държавна агенция "Разузнаване", Държавна агенция "Технически операции", Служба "Военно разузнаване" и	Пълно съответствие

	Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители; 3. по отношение на предприятия, предоставящи обществени електронни съобщителни мрежи и/или услуги по смисъла на Закона за електронните съобщения, с изключение на чл. 14, ал. 5, чл. 15, ал. 6 и чл. 19, ал. 3; 4. за доставчици на удостоверителни услуги по смисъла на чл. 3, т. 19 от Регламент (ЕС) № 910/2014 г. на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.); 5. за доставчици на цифрови услуги, които са микро- и малки предприятия по смисъла на чл. 3, ал. 2 и 3 от Закона за малките и средните предприятия. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 5.** Този закон не се прилага: 1. за комуникационните и информационните системи за обработка на класифицирана информация по смисъла на Закона за защита на класифицираната информация; 2. (изм. – ДВ, бр. 69 от 2020 г.) за мрежите и информационните системи на Министерството на отбраната, Министерството на вътрешните работи, Държавна агенция "Национална сигурност", Държавна агенция "Разузнаване", Държавна агенция "Технически операции" и Националната служба за охрана, които не са свързани с предоставянето на административни услуги по електронен път и обмен на електронни документи между административните органи; изискванията, управлението и контролът на тези мрежи и информационни системи се осъществяват при условия и по ред, определени от съответните ръководители; 3. по отношение на 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 НАРЕДБА 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.	
12. Настоящата директива се прилага, без да се засягат Регламент (ЕС) 2016/679, Директива 2002/58/ЕО, директиви 2011/93/ЕС (27) и 2013/40/ЕС (28) на Европейския парламент и на Съвета и Директива (ЕС) 2022/2557.	**Закон за киберсигурност** **Чл. 16**. (1) Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност за секторите и услугите, посочени в приложения № 1 и 2, когато такива не са създадени със специален закон. (12) Националните компетентни органи си сътрудничат с органите за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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	Пълно съответствие

	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.	
13. Без да се засяга член 346 от ДФЕС, информация, която е поверителна съгласно правилата на Съюза или националните правила, например правилата за търговската тайна, се обменя с Комисията и други съответни органи в съответствие с настоящата директива само когато този обмен е необходим за прилагането на настоящата директива. Обменяната информация се ограничава до информацията, която има значение за целите на този обмен и която е пропорционална на тези цели. Обменът на информация се извършва при зачитане на нейната поверителност и на сигурността и търговските интереси на засегнатите субекти.		Не подлежи на транспониране
14. Субектите, компетентните органи, единните звена за контакт и ЕРИКС обработват лични данни, доколкото това е необходимо за целите на настоящата директива и в съответствие с Регламент (ЕС) 2016/679, като по-специално това обработване се основава на член 6 от нея. Обработването на лични данни съгласно настоящата директива от доставчици на обществени електронни съобщителни мрежи или доставчици на обществено достъпни електронни съобщителни услуги се извършва в съответствие	**Закон за киберсигурност** **Чл. 16** (1) Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност за секторите и услугите, посочени в приложения № 1 и 2, когато такива не са създадени със специален закон. (12) Националните компетентни органи си сътрудничат с органите за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни. **Проект на Закон за изменение и допълнение на Закон за киберсигурност**	Пълно съответствие

с правото на Съюза в областта на защитата на данните и правото на Съюза в областта на неприкосновеността на личния живот, и по-специално Директива 2002/58/ЕО.	**Чл. 18. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Екипите се създават към националните компетентни органи в съответствие с методическите указания на „Агенцията на Европейския съюз за киберсигурност (ENISA)“. **(2)** Секторните екипи за реагиране при инциденти с компютърната сигурност: 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). СЕРИКС могат да обменят съответна информация с НЕРИКС на трети държави, включително лични данни в съответствие с правото на Съюза в областта на защитата на данните.	
Член 3 **Съществени и важни субекти** 1. За целите на настоящата директива следните субекти се считат за съществени субекти: а) субекти от видовете, посочени в приложение I, които надхвърлят таваните за средни предприятия, установени в член 2, параграф 1 от приложението към Препоръка 2003/361/ЕО; б) доставчици на квалифицирани удостоверителни услуги и регистри на имена на домейни от първо ниво, както и доставчици на DNS услуги, независимо от техния размер; в) доставчици на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги, които отговарят	**Закон за киберсигурност** **Обхват** **Чл. 4. (1)** С този закон се определят изискванията към: 1. административните органи; 2. операторите на съществени услуги и доставчиците на цифрови услуги – за всеки сектор, подсектор и услуги, посочени в приложения № 1 и 2; 3. лицата, осъществяващи публични функции, които не са определени като оператори на съществени услуги, когато тези лица предоставят административни услуги по електронен път; 4. организациите, предоставящи обществени услуги, които не са определени като оператори на съществени услуги или не са доставчици на цифрови услуги по смисъла на този закон, когато тези организации предоставят административни услуги по електронен път. (2) Оператор на съществени услуги е публичен или частен субект от посочените в приложение № 1 категории, който отговаря на следните критерии: 1. да предоставя съществена услуга, и	Пълно съответствие

на критериите за средни предприятия по смисъла на член 2 от приложението към Препоръка 2003/361/ЕО; г) органи на публичната администрация, посочени в член 2, параграф 2, буква е), точка i); д) всички други субекти от видовете, посочени в приложение I или II, които са установени от държава членка като съществени субекти съгласно член 2, параграф 2, букви б) — д); е) субекти, установени като критични субекти съгласно Директива (ЕС) 2022/2557, посочени в член 2, параграф 3 от настоящата директива; ж) ако държавата членка предвижда това, субекти, които тази държава членка е установила преди 16 януари 2023 г. като оператори на основни услуги в съответствие с Директива (ЕС) 2016/1148 или националното право;	2. предоставянето на тази съществена услуга да зависи от мрежи и информационни системи, и 3. инцидентите в мрежовата и информационната сигурност да имат значително увреждащо въздействие върху предоставянето **на тази услуга.** (3) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1 определят операторите на съществени услуги съгласно критериите по ал. 2 и в съответствие с методика, приета от Министерския съвет, и уведомяват министъра на електронното управление за това. Методиката се приема по предложение на министъра на електронното управление. (4) Когато оператор предоставя съществена услуга в две или повече държави – членки на Европейския съюз, административният орган по чл. 16, ал. 1 провежда консултации със съответните държави преди вземането на решение относно определянето на оператора. (5) Операторите на съществени услуги спазват изискванията за мрежова и информационна сигурност, предвидени в този закон, само по отношение на предоставяните от тях съществени услуги. (6) Когато в правен акт на Европейския съюз или в закон, който е специален за конкретен сектор или услуга, посочени в приложения № 1 и 2, се предвижда операторите на съществени услуги или доставчиците на цифрови услуги да гарантират мрежовата и информационната си сигурност или да уведомяват за инциденти, се прилагат тези актове, при условие че техните изисквания са най-малкото равностойни като резултат на задълженията, предвидени в този закон. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 4а** Съществени и важни субекти (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 , т. 1; 5. всички други субекти от видовете, посочени в приложение I или II, които са установени като съществени субекти съгласно чл. 4, т.3 букви г) - ж); 6. субектите, посочени в чл. 4, т. 4; 7. определените като **оператори на съществени услуги** към датата на влизане в сила на настоящия закон;	
2. За целите на настоящата директива субектите от видовете, посочени в приложение I или II, които не отговарят на критериите за съществени субекти съгласно параграф 1 от настоящия член, се считат за важни субекти. В това число се включват субекти, установени от държавите членки като важни субекти съгласно член 2, параграф 2, букви б)—д).	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 4а,** т.7 (2) За целите на закона субектите от видовете, посочени в приложение I или II, които не отговарят на критериите за съществени субекти съгласно ал. 1, се считат за **важни субекти**. В това число се включват субекти, установени като важни субекти съгласно чл. 4, т.3 букви г) - ж);	Пълно съответствие
3. До 17 април 2025 г. държавите членки изготвят списък на съществените и важните субекти, както и субекти, предоставящи услуги за регистрация на имена на домейни. Държавите членки извършват преглед на списъка и по целесъобразност го актуализират редовно и най-малко на всеки две години. 4. За целите на съставянето на списъка, посочен в параграф 3, държавите членки изискват от субектите, посочени в същия параграф, да	**Закон за киберсигурност** **Регистър** **Чл. 6.** (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на електронното управление създава, води и поддържа регистър на съществените услуги по смисъла на този закон, който съдържа: 1. видове съществени услуги; 2. списък на операторите на съществени услуги и предоставяните от тях услуги; 3. сфера на дейност; 4. брой потребители, разчитащи на услугата, предоставяна от оператора; 5. географски обхват на областта, която може да бъде засегната	Пълно съответствие

представят на компетентните органи най-малко следната информация: а) наименованието на субекта; б) адреса и актуални данни за контакт, включително адреси на електронната поща, IP обхвати и телефонни номера; в) когато е приложимо, съответния сектор и подсектор, посочени в приложение I или II, и г) когато е приложимо, списък на държавите членки, в които те предоставят услуги, попадащи в обхвата на настоящата директива. Субектите, посочени в параграф 3, уведомяват без забавяне за всякакви промени в данните, представени съгласно първата алинея от настоящия параграф, и при всички случаи в рамките на две седмици от датата на промяната. Комисията, със съдействието на Агенцията на Европейския съюз за киберсигурност (ENISA), предоставя без ненужно забавяне насоки и образци относно задълженията, предвидени в настоящия параграф. Държавите членки могат да установят национални механизми, чрез които субектите да се регистрират сами. 5. До 17 април 2025 г. и на всеки две години след това компетентните органи уведомяват: а) Комисията и групата за сътрудничество относно броя на всички съществени и важни субекти, изброени в параграф 3 за всеки сектор и подсектор, посочени в приложение I или II; както и	от даден инцидент. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Списъкът по ал. 1, т. 2 се преразглежда и актуализира на всеки две години от съответните административни органи по чл. 16, ал. 1, за което те уведомяват министъра на електронното управление. (3) Редът за водене, съхраняване и достъп до регистъра се определя с наредбата по чл. 3, ал. 2. (4) Регистърът по ал. 1 не е публичен. **Национално единно звено за контакт** Чл. 17. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национално единно звено за контакт. (2) Националното единно звено за контакт координира въпросите, свързани с мрежовата и информационната сигурност, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави – членки на Европейския съюз. (3) Националното единно звено за контакт предоставя на всеки две години на Европейската комисия информация относно последователността на подходите за определянето на операторите на съществени услуги, която включва: 1. националните мерки, чрез които са определени операторите на съществени услуги; 2. списък на съществените услуги; **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Регистър** **Чл. 6. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на електронното управление създава, води и поддържа регистър на субектите по чл. 4 и чл. 4а, който съдържа следната информация: а) наименованието на субекта; б) адрес и актуални данни за контакт, включително адреси на електронната поща и телефонни номера; в) IP обхвати; г) когато е приложимо, съответния сектор, подсектор и вид субект, както е посочено в приложение I или II;	

б) Комисията за съответната информация относно броя на главните и важните субекти, установени съгласно член 2, параграф 2, букви б) — д), сектора и подсектора, посочени в приложение I или II, към които те принадлежат, вида на услугата, която предоставят, и разпоредбата, измежду посочените в член 2, параграф 2, букви б) — д), съгласно която са били установени. 6. До 17 април 2025 г. и по искане на Комисията държавите членки могат да съобщят на Комисията наименованията на съществените и важните субекти, посочени в параграф 5, буква б).	д) когато е приложимо, списък на държавите членки, в които те предоставят услуги, попадащи в обхвата на този закон; е) когато е приложимо, данни за контакт на представителя, определен съгласно чл. 24, 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 член 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 определят с наредбата по чл. 3, ал. 2. (5) Регистърът по ал.1 не е публичен.	
Член 4 Специфични за сектора правни актове на Съюза 1. Когато специфични за сектора правни актове на Съюза изискват съществените или	**Закон за киберсигурност** **Чл.4 (6)** Когато в правен акт на Европейския съюз или в закон, който е специален за конкретен сектор или услуга, посочени в приложения № 1 и 2, се предвижда операторите на съществени услуги или доставчиците на цифрови услуги да гарантират мрежовата и информационната си сигурност или да уведомяват за инциденти, се прилагат тези актове, при условие че техните	Пълно съответствие

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 настоящата директива задължения, съответните разпоредби на настоящата директива, включително разпоредбите относно надзора и правоприлагането, предвидени в глава VII, не се прилагат за такива субекти. Когато специфични за сектора законодателни актове на Съюза не обхващат всички субекти в конкретен сектор, попадащ в обхвата на настоящата директива, съответните разпоредби на настоящата директива продължават да се прилагат по отношение на субектите, които не са обхванати от тези специфични за сектора правни актове на Съюза. 2. Изискванията, посочени в параграф 1 от настоящия член, се считат за равностойни по ефект на задълженията, предвидени в настоящата директива, когато: а) мерките за управление на риска в областта на киберсигурността са най-малкото равностойни по сила на мерките, определени в член 21, параграфи 1 и 2; или б) в секторния правен акт на Съюза се предвижда незабавен, по целесъобразност автоматичен и пряк, достъп до уведомленията за инциденти от ЕРИКС, компетентните органи или единните звена за контакт съгласно настоящата директива и когато изискванията за уведомяване за значителни инциденти са най-малкото равностойни на предвидените в член 23, параграфи 1 — 6 от настоящата директива.	изисквания са най-малкото равностойни като резултат на задълженията, предвидени в този закон. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Специфични за сектора правни актове** **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 член 22, или 2. в секторния правен акт на Съюза се предвижда незабавен, по целесъобразност автоматичен и пряк, достъп до уведомленията за инциденти от ЕРИКС от екипа за реагиране при инциденти с компютърната сигурност (ЕРИКС), националните компетентни органи или единните звена за контакт, съгласно настоящия закон и когато изискванията за уведомяване за значителни инциденти са най-малкото равностойни на предвидените в член 23.	

3. До 17 юли 2023 г. Комисията предоставя насоки за прилагането на параграфи 1 и 2. Комисията извършва редовен преглед на тези насоки. При изготвянето на тези насоки Комисията взема предвид всички наблюдения на групата за сътрудничество и ENISA.		
Член 5 **Минимална хармонизация** Настоящата директива не възпрепятства държавите членки да приемат или запазят разпоредби, гарантиращи по-висока степен на киберсигурност, при условие че тези разпоредби не противоречат на задълженията на държавите членки, предвидени в правото на Съюза.		Не подлежи на транспониране
Член 6 **Определения** За целите на настоящата директива се прилагат следните определения: 1) „мрежова и информационна система“ означава: а) електронно съобщителна мрежа съгласно определението в член 2, точка 1 от Директива (ЕС) 2018/1972; б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма извършват автоматична обработка на цифрови данни; или в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати	**Закон за киберсигурност** ДР § 3. По смисъла на този закон: 1. "Административен орган" е понятието по смисъла на § 1, т. 1 от допълнителните разпоредби на закона за електронното управление. 2. "Група за сътрудничество" е групата по смисъла на чл. 11 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.). 3. "Действия при инцидент" са всички процедури, подпомагащи установяването, анализа и ограничаването на инцидент, както и реагирането на такъв инцидент. 4. "Длъжностно лице" е понятието по смисъла на чл. 93, т. 1 от Наказателния кодекс. 5. "Доставчик на DNS услуги" е субект, предоставящ DNS услуги по интернет. DNS (Domain Name System) е Система за имена на домейни, която представлява йерархично разпределена мрежова система за именуване на домейни, разпределяща заявки за имена на домейни.	Пълно съответствие

от букви а) и б), с цел обработване, използване, защита и поддръжка; 2) „сигурност на мрежовите и информационните системи“ означава способността на мрежовите и информационните системи да издържат — при дадено равнище на увереност — на всяко събитие, което може да засегне отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежови и информационни системи или достъпни чрез тях; 3) „киберсигурност“ означава киберсигурност съгласно определението в член 2, точка 1 от Регламент (ЕС) 2019/881; 4) „национална стратегия за киберсигурност“ означава съгласувана рамка на държава членка, съдържаща стратегически цели и приоритети в областта на киберсигурността и управленските методи за постигането им в тази държава членка; 5) „ситуация, близка до инцидент“ означава 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, но чието случване е било успешно предотвратено или което не се е осъществило;	6. "Доставчик на цифрови услуги" е юридическо лице, предоставящо цифрова услуга. 7. "Зловреден интернет трафик" са аномалии на интернет трафика, предизвикани от хардуерни или софтуерни повреди на интернет пакети със злоумишлено модифицирани опции. 8. "Информационна защита" е комплекс от организационни, юридически, технически и технологични мерки за мониторинг, анализ, активна превенция, намаляване влиянието на уязвимости, споделяне на информация за тях, включително отстраняване на последствията от инциденти. 9. "Инцидент със "значително увреждащо въздействие" се определя, като се вземат предвид следните показатели: а) брой ползватели, разчитащи на услугите, предоставяни от субекта; б) зависимост на други сектори - от посочените в приложение № 1, от услугата, предоставяна от субекта; в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност; г) пазарният дял на субекта; д) географският обхват на областта, която би била засегната от даден инцидент; е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга. Когато е целесъобразно, се вземат предвид и характерните за сектора показатели, за да се определи дали даден инцидент би имал значително увреждащо въздействие. 10. "Кибератака" е опит за разрушаване, разкриване, променяне, забрана, кражба или получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив. 11. "Киберзаплаха" е възможността за злонамерен опит да се повреди или прекъсне компютърната мрежа, системата, услугите и данните. 12. "Киберинцидент" е събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията.	

6) „инцидент“ означава събитие, което засяга отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи; 7) „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; 8) „действия при инцидент“ означава всякакви действия и процедури, имащи за цел предотвратяването, установяването, анализа, ограничаването или реагирането на инцидент и възстановяването от него; 9) „риск“ означава потенциалната загуба или потенциалното смущение в резултат на даден инцидент и трябва да се изразява като комбинация от мащаба на загубата или смущението и вероятността от настъпване на инцидента; 10) „киберзаплаха“ означава киберзаплаха съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/881; 11) „значителна киберзаплаха“ означава киберзаплаха, за която въз основа на техническите ѝ характеристики може да се предположи, че има потенциал да окаже сериозно	13. "Киберинцидент със значителен приоритет" е киберинцидент, който оказва сериозно въздействие върху дейността на правителството, върху предоставянето на съществени услуги на голяма част от българското население или върху икономиката на Република България. 14. "Киберинцидент с висок приоритет" е киберинцидент, който има сериозно въздействие върху голяма организация или върху по-широко/местно управление или който представлява значителен риск за предоставянето на съществените услуги на голяма част от българското население или върху икономиката на Република България. 15. "Киберинцидент със среден приоритет" е киберинцидент, който има сериозно въздействие върху средна организация или който представлява значителен риск за голяма организация или за по-широко/местно управление. 16. "Киберотбрана" е комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност. 17. "Киберпространство" е глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни. 18. "Киберрезерв" е допълнителен ресурс от експерти в областта на киберсигурността, защитата на информацията и информационните технологии с компетентности, свързани с осигуряване на защита и устойчивост на комуникационните и информационните системи. 19. "Компютърна услуга "в облак" е цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно. 20. "Лица, осъществяващи публични функции" е понятието по смисъла на § 1, т. 11 от допълнителните разпоредби на Закона за електронното управление.	

въздействие върху мрежовите и информационните системи на даден субект или върху ползвателите на услугите на субекта, като причини значителни материални или нематериални вреди; 12) „ИКТ продукт“ означава ИКТ продукт съгласно определението в член 2, точка 12 от Регламент (ЕС) 2019/881; 13) „ИКТ услуга“ означава ИКТ услуга съгласно определението в член 2, точка 13 от Регламент (ЕС) 2019/881; 14) „ИКТ процес“ означава ИКТ процес съгласно определението в член 2, точка 14 от Регламент (ЕС) 2019/881; 15) „уязвимост“ означава слабост, предразположеност или недостатък на ИКТ продукти или ИКТ услуги, които могат да бъдат използвани при киберзаплаха; 16) „стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета (29); 17) „техническа спецификация“ означава техническа спецификация съгласно определението в член 2, точка 4 от Регламент (ЕС) № 1025/2012; 18) „точка за обмен в интернет“ означава мрежово средство, което дава възможност за свързване на повече от две независими мрежи	21. "Мащабен инцидент" е налице, когато са регистрирани инциденти със среден приоритет в мрежите и информационните системи на повече от 4 от субектите по чл. 4, ал. 1, с висок приоритет в мрежите и информационните системи на повече от два от субектите по чл. 4, ал. 1 и със значителен приоритет на повече от един от субектите по чл. 4, ал. 1. Класификацията на инциденти в зависимост от типа на атаката се определя по методика на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA). 22. "Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност" е мрежата по смисъла на чл. 12 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.). 23. "Мрежа и информационна система" е: а) електронна съобщителна мрежа по смисъла на § 1, т. 15 от допълнителните разпоредби на Закона за електронните съобщения; б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви "а" и "б", с цел обработване, използване, защита и поддръжка. 24. "Онлайн място за търговия" е цифрова услуга, която дава на потребители или търговци по смисъла на § 13, т. 1 и 2 от допълнителните разпоредби на Закона за защита на потребителите възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия. 25. "Онлайн търсачка" е цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с искането съдържание.	

(автономни системи), преди всичко с цел улесняване на обмена на интернет трафик, което осъществява свързване само на автономни системи и което нито изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин; 19) „система за имена на домейни“ или „DNS“ означава йерархична разпределена система за именуване, която позволява идентифициране на интернет услуги и ресурси, позволявайки на устройствата на крайните ползватели да използват интернет маршрутизация и услуги за свързване, за да достигнат до тези услуги и ресурси; 20) „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; 21) „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	26. "Организация, предоставяща обществени услуги" е понятието по смисъла на § 1, т. 14 от допълнителните разпоредби на Закона за електронното управление. 27. "Повторно" е нарушението, извършено в срок една година от влизането в сила на наказателното постановление, с което на нарушителя е наложено наказание за същото по вид нарушение. 28. "Представител" е физическо или юридическо лице, установено в държава - членка на Европейския съюз, което е изрично определено да действа от името на доставчик на цифрови услуги, който не е установен в държава - членка на Европейския съюз, и към което национален компетентен орган или екип за реагиране при инциденти с компютърната сигурност може да се обърне вместо към доставчика на цифрови услуги във връзка със задълженията на доставчика на цифрови услуги по този закон. 29. "Регистър на имена на домейни от първо ниво" е субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от първо ниво (top-level domain - TLD). 30. "Риск" е потенциалната възможност дадена заплаха да се осъществи, като се експлоатира уязвимостта на информационните активи, за да се причини вреда. 31. "Съществени услуги" са услуги, които имат съществено значение за поддържането на особено важни обществени и/или стопански дейности в един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода или цифрова инфраструктура. 32. "Спецификация" е техническа спецификация по смисъла на чл. 2, т. 4 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ, L 316/12 от 14 ноември 2012 г.).	

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; 22) „субект, предоставящ услуги за регистрация на имена на домейни“ означава регистратор или агент, действащ от името на регистратори, като например доставчик или препродавач на услуги за поверителност или прокси услуги; 23) „цифрова услуга“ означава услуга съгласно определението в член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета (30); 24) „удостоверителна услуга“ означава удостоверителна услуга съгласно определението в член 3, точка 16 от Регламент (ЕС) № 910/2014; 25) „доставчик на удостоверителна услуга“ означава доставчик на удостоверителна услуга съгласно определението в член 3, точка 19 от Регламент (ЕС) № 910/2014; 26) „квалифицирана удостоверителна услуга“ означава квалифицирана удостоверителна услуга съгласно определението в член 3, точка 17 от Регламент (ЕС) № 910/2014;	33. "Точка за обмен в интернет (ТОИ)" е мрежово средство, което дава възможност за свързване на повече от две независими автономни системи преди всичко с цел улесняване на обмена на интернет трафик. Чрез ТОИ се осъществява свързване само на автономни системи. Свързването чрез ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин. 34. "Уязвимост" е неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които може да бъдат използвани за деструктивно въздействие върху системата. 35. "Цифрова услуга" е услуга по смисъла на чл. 1, параграф 1, буква "б" от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ, L 241/1 от 17 септември 2015 г.), от категориите, посочени в приложение № 2. 36. "Цифрова инфраструктура" е инфраструктура, която включва ТОИ, доставчици на DNS услуги и регистри на имената на домейни от първо ниво. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** § 4. По смисъла на този закон: 1. Административен орган“ е орган, който принадлежи към системата на изпълнителната власт 2. "Група за сътрудничество" е групата по смисъла на чл. 11 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.). 2а. „Национална стратегия за киберсигурност“ е съгласувана рамка на държавата членка, съдържаща стратегически цели и приоритети в областта на киберсигурността и управленските методи за постигането им.	

27) „доставчик на квалифицирана удостоверителна услуга“ означава доставчик на квалифицирана удостоверителна услуга съгласно определението в член 3, точка 20 от Регламент (ЕС) № 910/2014; 28) „онлайн място за търговия“ означава онлайн място за търговия съгласно определението в член 2, буква н) от Директива 2005/29/ЕО на Европейския парламент и на Съвета (31); 29) „онлайн търсачка“ означава онлайн търсачка съгласно определението в член 2, точка 5 от Регламент (ЕС) 2019/1150 на Европейския парламент и на Съвета (32); 30) „компютърна услуга „в облак“ означава цифрова услуга, която дава възможност за администриране при поискване и широк отдалечен достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно, включително когато тези ресурси са разпределени на няколко места; 31) „услуга на център за данни“ означава 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;	3. „Действия при инцидент“ означава всякакви действия и процедури, имащи за цел предотвратяването, установяването, анализа, ограничаването или реагирането на инцидент и възстановяването от него 4. "Длъжностно лице" е понятието по смисъла на чл. 93, т. 1 от Наказателния кодекс. 4а. „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. 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. 6. "Доставчик на цифрови услуги" е юридическо лице, предоставящо цифрова услуга. 7. "Зловреден интернет трафик" са аномалии на интернет трафика, предизвикани от хардуерни или софтуерни повреди на интернет пакети със злоумишлено модифицирани опции. 8. "Информационна защита" е комплекс от организационни, юридически, технически и технологични мерки за мониторинг, анализ, активна превенция, намаляване влиянието на уязвимости, споделяне на информация за тях, включително отстраняване на последствията от инциденти. 9. „Ситуация, близка до инцидент“ е събитие, което е могло да засегне отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи, чието случване (чиято активност е била предодвратена) е било успешно предотвратено или което не се е осъществило. 10. "Кибератака" е опит за разрушаване, разкриване, променяне, забрана, кражба или	

32) „мрежа за доставяне на съдържание“ означава 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; 33) „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; 34) „представител“ означава установено в Съюза физическо или юридическо лице, изрично определено да действа от името на доставчик на DNS услуги, регистър на имена на домейни от първо ниво, субект, предоставящ услуги за регистрация на имена на домейни, доставчик на компютърни услуги „в облак“, доставчик на услуги на център за данни, доставчик на мрежи за предоставяне на съдържание, доставчик на управлявани услуги, доставчик на управлявани услуги за сигурност или доставчик на онлайн места за търговия, на онлайн търсачки или на платформи на услуги за социални мрежи, което не е установено в Съюза, и към което, по отношение на задълженията на даден субект съгласно настоящата директива, компетентен орган или ЕРИКС може да се обръща вместо към самия субект;	получаване на неупълномощен достъп до/или неупълномощено използване на информационен актив. 11. „Киберзаплаха“ означава всяко потенциално обстоятелство, събитие или действие, което може да навреди, наруши или по друг начин да окаже неблагоприятно въздействие върху мрежите и информационните системи, ползвателите на такива мрежи и системи и други лица. 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 12. "Киберинцидент" е събитие или поредица от нежелани или неочаквани събития, свързани с киберсигурността, които с голяма вероятност могат да предизвикат компрометиране на дейностите и заплашват сигурността на информацията. 12а. „Инцидент“ е събитие, което засяга отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи 13. "Киберинцидент със значителен приоритет" е киберинцидент, който оказва сериозно въздействие върху дейността на правителството, върху предоставянето на съществени услуги на голяма част от българското население или върху икономиката на Република България. 14. "Киберинцидент с висок приоритет" е киберинцидент, който има сериозно въздействие върху голяма организация или върху по-широко/местно управление или който представлява значителен риск за предоставянето на съществените услуги на голяма част от българското население или върху икономиката на Република България. 15. "Киберинцидент със среден приоритет" е киберинцидент, който има сериозно въздействие върху средна организация или който представлява значителен риск за голяма организация или за по-широко/местно управление. 15а. „Мащабен киберинцидент“ означава инцидент, който причинява степен на смущение, надхвърляща способността на	

35) „орган на публичната администрация“ означава орган, който е признат като такъв в държава членка в съответствие с националното право, с изключение на съдебната власт, парламентите и централните банки, който отговаря на следните критерии: а) създаден е с цел да задоволява нужди от общ интерес и няма промишлен или търговски характер; б) притежава правосубектност или е оправомощен по закон да действа от името на друг субект с правосубектност; в) е финансиран в по-голямата си част от държавата, регионални органи или други публичноправни организации, е обект на управленски надзор от страна на тези органи или организации, или има административен, управителен или надзорен орган, повечето от половината от членовете на който са назначени от държавата, регионалните органи или от други публичноправни организации; г) има правомощието да налага на физически или юридически лица административни или регулаторни решения, засягащи техните права в трансграничното движение на хора, стоки, услуги или капитали; 36) „обществена електронна съобщителна мрежа“ означава обществена електронна съобщителна мрежа съгласно определението в член 2, точка 8 от Директива (ЕС) 2018/1972;	дадена държавата членка да реагира на него, или който има значително въздействие върху най-малко две държави членки. 16. "Киберотбрана" е комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност. 17. "Киберпространство" е глобална мрежа от системи за компютърна обработка, електронни съобщителни мрежи, компютърни програми и данни. 18. "Киберрезерв" е допълнителен ресурс от експерти в областта на киберсигурността, защитата на информацията и информационните технологии с компетентности, свързани с осигуряване на защита и устойчивост на комуникационните и информационните системи. 19. „Компютърна услуга „в облак“ е цифрова услуга, която дава възможност за администриране при поискване и широк отдалечен достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно, включително когато тези ресурси са разпределени на няколко места. . 20. "Лица, осъществяващи публични функции" е понятието по смисъла на § 1, т. 11 от допълнителните разпоредби на Закона за електронното управление. 21. "Мащабен инцидент" е налице, когато са регистрирани инциденти със среден приоритет в мрежите и информационните системи на повече от 4 от субектите по чл. 4, ал. 1, с висок приоритет в мрежите и информационните системи на повече от два от субектите по чл. 4, ал. 1 и със значителен приоритет на повече от един от субектите по чл. 4, ал. 1. Класификацията на инциденти в зависимост от типа на атаката се определя по методика на Агенцията на Европейския съюз за киберсигурност (ENISA). 22. „Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност“ е мрежата по смисъла на	

37) „електронна съобщителна услуга“ означава електронна съобщителна услуга съгласно определението в член 2, точка 4 от Директива (ЕС) 2018/1972; 38) „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; 39) „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; 40) „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; 41) „научноизследовател-ска организация“ означава субект, чиято основна цел е да извършва приложна научноизследо- вателска или развойна дейност с цел използване на резултатите от тези научни изследвания за търговски цели, но който не включва образователни институции.	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) 23. "Мрежа и информационна система" е: а) електронна съобщителна мрежа по смисъла на § 1, т. 15 от допълнителните разпоредби на Закона за електронните съобщения; б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработва автоматично цифрови данни, или в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви "а" и "б", с цел обработване, използване, защита и поддръжка. 24. "Онлайн място за търговия" е цифрова услуга, която дава на потребители или търговци по смисъла на § 13, т. 1 и 2 от допълнителните разпоредби на Закона за защита на потребителите възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия. 25. "Онлайн търсачка" е цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с исканото съдържание. 26. "Организация, предоставяща обществени услуги" е понятието по смисъла на § 1, т. 14 от допълнителните разпоредби на Закона за електронното управление. 27. "Повторно" е нарушението, извършено в срок една година от влизането в сила на наказателното постановление, с което на нарушителя е наложено наказание за същото по вид нарушение. 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 28. „Представител“ е установено в Съюза физическо или юридическо лице, изрично определено да действа от името на доставчик на DNS услуги, регистър на имена на домейни от първо ниво, субект, предоставящ услуги за регистрация на имена на домейни, доставчик на компютърни услуги „в облак“, доставчик на услуги на център за данни, доставчик на мрежи за предоставяне на съдържание, доставчик на управлявани услуги, доставчик на управлявани услуги за сигурност или доставчик на онлайн места за търговия, на онлайн търсачки или на платформи на услуги за социални мрежи, което не е установено в Съюза, и към което, по отношение на задълженията на даден субект съгласно настоящата директива, компетентен орган или ЕРИКС може да се обръща вместо към самия субект 29. „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. 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. 30. „Риск“ е потенциалната загуба или потенциалното смущение в резултат на даден инцидент и трябва да се изразява като комбинация от мащаба на загубата или смущението и вероятността от настъпване на инцидента.	

	31. "Съществени услуги" са услуги, които имат съществено значение за поддържането на особено важни обществени и/или стопански дейности в един от следните сектори: енергетика, транспорт, банково дело, инфраструктура на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода или цифрова инфраструктура. 31а. „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. 32. "Спецификация" е техническа спецификация по смисъла на чл. 2, т. 4 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ, L 316/12 от 14 ноември 2012 г.). 32а. „Стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета (29). 33. "Точка за обмен в интернет (ТОИ)" е мрежово средство, което дава възможност за свързване на повече от две независими автономни системи преди всичко с цел улесняване на обмена на интернет трафик. Чрез ТОИ се осъществява свързване само на автономни системи. Свързването чрез ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин.	

	34. „Уязвимост“ означава слабост, предразположеност или недостатък на ИКТ продукти или ИКТ услуги, които могат да бъдат използвани при киберзаплаха 35. "Цифрова услуга" е услуга по смисъла на чл. 1, параграф 1, буква "б" от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г. установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ, L 241/1 от 17 септември 2015 г.), от категориите, посочени в приложение № 2. 36. „Цифрова инфраструктура“ е инфраструктурата, която включва категориите, посочени в Приложение № 1, т. 8 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; 60. „Информационни активи“ са всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на този закон (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация, поддържащите ги системи (електрозахранващи, климатизиращи и др.), оперативни процеси/дейности, служители и външни организации).“ 61. „Сигурност на мрежовите и информационните системи“ е способността на мрежовите и информационните системи да издържат — при дадено равнище на увереност — на всяко събитие, което може да засегне отрицателно наличността, автентичността, цялостността или поверителността на	

	съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежови и информационни системи или достъпни чрез тях.”	
ГЛАВА II **КООРДИНИРАНИ РАМКИ В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА** **Член 7** **Национална стратегия за киберсигурност** 1. Всяка държава членка приема национална стратегия 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: а) целите и приоритетите на стратегията за киберсигурност на държавата членка, като се обхващат по-специално секторите, посочени в приложения I и II; б) рамка за управление за постигане на целите и приоритетите, посочени в буква а) от настоящия параграф, включително посочените в параграф 2 политики; в) 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	**Закон за киберсигурност** **Стратегии** **Чл. 8. (1)** Националната стратегия за киберсигурност е стратегическа рамка на политиката за киберсигурност, която включва: 1. цели, принципи и приоритети; 2. области на действие и мерки: а) система за киберсигурност; б) мрежова и информационна сигурност; в) противодействие на киберпрестъпността; г) киберотбрана; д) киберразузнаване; 3. взаимодействие между държава, бизнес и общество; 4. развитие и подобряване на регулаторната рамка; 5. повишаване на осведомеността, знанията и компетентностите; стимулиране на изследванията и иновациите в областта на киберсигурността; 6. международно взаимодействие; 7. кибердипломация; 8. взаимодействие на техническо, оперативно и стратегическо (политическо) ниво. (2) Националната стратегия за мрежова и информационна сигурност е стратегическа рамка на политиката за мрежова и информационна сигурност, която включва: 1. цели и приоритети относно мрежовата и информационната сигурност; 2. управленска рамка за постигане на целите и приоритетите по т. 1, включително функциите и отговорностите на държавните органи и на други участници; 3. мерки във връзка с подготвеността, реагирането и възстановяването в мрежите и информационните системи, включително сътрудничеството между публичния и частния сектор;	Пълно съответствие

и ЕРИКС съгласно настоящата директива, както и координацията и сътрудничеството между тези органи и компетентните органи съгласно специфичните за сектора правни актове на Съюза; г) механизъм за установяване на относимите активи и оценка на рисковете в съответната държава членка; д) набелязване на мерките, гарантиращи подготвеността, реагирането и възстановяването при инциденти, включително сътрудничеството между публичния и частния сектор; е) списък с различните органи и заинтересовани страни, които участват в прилагането на националната стратегия за киберсигурност; ж) рамка на политика за засилена координация между компетентните органи съгласно настоящата директива 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; з) план, включващ необходимите мерки за укрепване на общото равнище на осведоменост на гражданите относно киберсигурността. 2. Като част от националната стратегия за киберсигурност държавите членки по-специално приемат политики:	4. съществена информация за образователните и обучителните програми и програмите за повишаване на осведомеността във връзка с мрежовата и информационната сигурност; 5. посочване на плановете за научноизследователска и развойна дейност относно мрежовата и информационната сигурност; 6. план за оценка на риска с цел набелязване на рисковете; 7. списък на различните участници в изпълнението на стратегията. (3) Национална стратегия за мрежова и информационната сигурност се изготвя, когато Националната стратегия за киберсигурност не съдържа информацията по ал. 2. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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 буква а), включително посочените в ал. 2 политики; 3. рамка за управление, в която се изясняват ролите и отговорностите на съответните заинтересовани страни на национално равнище и която е в основата на сътрудничеството и координацията на национално равнище между националните компетентни органи, единните звена за контакт и ЕРИКС съгласно закона, както и координацията и сътрудничеството между тези органи и националните компетентни органи съгласно специфичните европейски правни актове;	

а) за разрешаване на въпросите с киберсигурността по веригата за доставки на ИКТ продукти и услуги, използвана от субектите за предоставянето на техните услуги; б) относно включването и посочването на свързани с киберсигурността изисквания за ИКТ продуктите и ИКТ услугите при възлагането на обществени поръчки, включително във връзка с сертифициране в областта на киберсигурността, криптиране и използване на продукти за киберсигурност с отворен код; в) управление на уязвимостите, включващо насърчаването и улесняването на координираното оповестяване на уязвимости съгласно член 12, параграф 1; г) свързани с поддържането на общата наличност, цялостност и поверителност на общественото ядро на отворения интернет, включително, когато е целесъобразно, киберсигурността на подводните комуникационни кабели; д) насърчаване на разработването и внедряването на съответните авангардни технологии, насочени към прилагане на най- съвременни мерки за управление на риска в областта на киберсигурността; е) насърчаване и развитие на образованието и обучението в областта на киберсигурността, уменията, повишаването на осведомеността и инициативите за научноизследователска и	4. механизъм за установяване на относимите активи и оценка на риска на ниво държава; 5. мерките, гарантиращи подготвеността, реагирането и възстановяването при инциденти, включително сътрудничеството между публичния и частния сектор; 6. списък с различните органи и заинтересовани страни, които участват в прилагането на националната стратегия за киберсигурност; 7. рамка на политика за засилена координация между националните компетентни органи съгласно закона и 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 министъра на електронното управление провежда политиките: 1. за киберсигурността по веригата за доставки на ИКТ продукти и услуги, използвана от субектите за предоставянето на техните услуги; 2. относно включването и посочването на изискванията свързани с киберсигурността за ИКТ продуктите и ИКТ услугите при възлагането на обществени поръчки, включително във връзка със сертифициране в областта на киберсигурността, криптиране и използване на продукти за киберсигурност с отворен код; 3. по управление на уязвимостите, включващо насърчаването и улесняването на координираното оповестяване на уязвимости	

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; ж) подпомагане на академичните и научноизследователските институции за разработване, подобряване и насърчаване на внедряването на инструменти за киберсигурност и сигурна мрежова инфраструктура; з) включване на съответни процедури и подходящи инструменти за обмен на информация, подпомагащи доброволния обмен на информация за киберсигурността между субекти в съответствие с правото на Съюза; и) укрепване на киберустойчивостта и основните параметри за киберхигиена на малките и средните предприятия, по-специално на тези, които са изключени от обхвата на настоящата директива, чрез предоставяне на леснодостъпни насоки и помощ за техните специфични нужди; й) насърчаване на активна киберзащита. 3. Държавите членки уведомяват Комисията за своите национални стратегии за киберсигурност в рамките на три месеца от приемането им. Държавите членки могат да изключат от тези уведомления информацията, която се отнася до тяхната национална сигурност. 4. Държавите членки извършват оценка на своите национални стратегии за киберсигурност редовно и поне на всеки пет години въз основа на ключови показатели за ефективност и при	съгласно „Европейската база данни за уязвимости на Агенцията на Европейския съюз за киберсигурност (ENISA)“; 4. свързани с поддържането на общата наличност, цялостност и поверителност на обществото ядро на отворения интернет, включително, когато е целесъобразно, киберсигурността на подводните комуникационни кабели; 5. свързани с насърчаване на разработването и внедряването на съответните авангардни технологии, насочени към прилагане на най- съвременни мерки за управление на риска в областта на киберсигурността; 6. свързани с насърчаване и развитие на образованието и обучението в областта на киберсигурността, уменията, повишаването на осведомеността и инициативите за научноизследователска и развойна дейност в областта на киберсигурността, както и насоки за добри практики и механизми за контрол в областта на киберхигиената, насочени към гражданите, заинтересованите страни и субектите; 7. по подпомагане на академичните и научноизследователските институции за разработване, подобряване и насърчаване на внедряването на инструменти за киберсигурност и сигурна мрежова инфраструктура; 8. по включване на съответни процедури и подходящи инструменти за обмен на информация, подпомагащи доброволния обмен на информация за киберсигурността между субектите; 9. по укрепване на киберустойчивостта и основните параметри за киберхигиена на малките и средните предприятия, по-специално на тези, които са изключени от обхвата на настоящата директива, чрез предоставяне на леснодостъпни насоки и помощ за техните специфични нужди; 10. по насърчаване на активна киберзащита. (3) Националната стратегия за киберсигурност се актуализира на всеки пет години въз основа на ключови показатели за ефективност.	

необходимост ги актуализират. ENISA подпомага държавите членки, по тяхно искане, при разработването или актуализирането на национална стратегия за киберсигурност и на ключови показатели за ефективност за оценката на тази стратегия, за да я приведе в съответствие с изискванията и задълженията, предвидени в настоящата директива.		
Член 8 **Компетентни органи и единни звена за контакт** 1. Всяка държава членка определя или създава един или повече **компетентни органи**, отговарящи за киберсигурността и за надзорните задачи, посочени в глава VII („компетентни органи“). 2. Компетентните органи, посочени в параграф 1, наблюдават прилагането на настоящата директива на национално равнище. 3. Всяка държава членка определя или създава **единно звено за контакт**. Когато държава членка определи или създаде само един компетентен орган съгласно параграф 1, този компетентен орган изпълнява функцията и на единно звено за контакт за тази държава членка. 4. Всяко единно звено за контакт изпълнява функцията на свръзка, за да гарантира трансграничното сътрудничество на органите на своята държава членка със съответните органи на други държави членки, и, когато е целесъобразно,	**Закон за киберсигурност** **Национални компетентни органи** Чл. 16. (1) Министерският съвет определя с решение административните органи, към които се създават национални компетентни органи по мрежова и информационна сигурност за секторите и услугите, посочени в приложения № 1 и 2, когато такива не са създадени със специален закон. (2) (Изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Национален компетентен орган за всички административни органи, както и за лицата и организациите по чл. 4, ал. 1, т. 3 и 4, е Министерството на електронното управление. (3) Националните компетентни органи: 1. координират и контролират изпълнението на задачите, свързани с мрежовата и информационната сигурност на административните органи, операторите на съществени услуги и доставчиците на цифрови услуги съгласно този закон; 2. (изм. - ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) приемат, след съгласуване с Министерството на електронното управление, насоки относно обстоятелствата, при които субектите по чл. 4, ал. 1 са длъжни да уведомяват за инциденти; 3. оценяват дали административните органи, операторите на съществени услуги и доставчиците на цифрови услуги изпълняват задълженията си по глава втора, както и въздействието на това изпълнение върху мрежовата и информационната сигурност и предприемат съответните мерки при неизпълнение; 4. съвместно с Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки по отношение на техническите области, които да се вземат	Пълно съответствие

с Комисията и ENISA, както и за да осигури междусекторно сътрудничество с други компетентни органи в рамките на своята държава членка. 5. Държавите членки гарантират, че техните **компетентни органи и единни звена за контакт** разполагат с достатъчно ресурси, за да изпълняват ефективно и ефикасно възложените им задачи и по този начин да постигат целите на настоящата директива. 6. Всяка държава членка **уведомява Комисията** без излишно забавяне за самоличността на компетентния орган, посочен в параграф 1, и на единното звено за контакт, посочено в параграф 3, за задачите на тези органи и за евентуални последващи промени в тях. Всяка държава членка оповестява публично самоличността на компетентния си орган. Комисията прави обществено достъпен списъка на единните звена за контакт.	предвид във връзка с използването на европейските или международните стандарти и спецификации от значение за мрежовата и информационната сигурност; 5. със съдействието на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) изготвят препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора. (4) Националните компетентни органи гарантират, че екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 получават уведомления за инциденти по този закон. (5) Националните компетентни органи имат право да изискват от административните органи и от операторите на съществени услуги: 1. информация, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност, резултати от одити на мрежовата и информационната сигурност, когато са извършени от друг квалифициран одитор, и доказателствата, на които те се основават; 2. доказателства за ефективно изпълнение на препоръките от одити на мрежовата и информационната им сигурност. (6) В искането по ал. 5 националните компетентни органи посочват целта му и уточняват каква информация или доказателства се изискват. (7) След оценяването на информацията или на доказателствата по ал. 5 съответният национален компетентен орган дава при необходимост задължителни указания за отстраняване на установените пропуски в изпълнението на изискванията, предвидени в глава втора. (8) За целите на глава втора националните компетентни органи имат право да изискват от доставчиците на цифрови услуги да: 1. предоставят информацията, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност; 2. отстранят всеки пропуск в изпълнението на изискванията, предвидени в глава втора. (9) Когато получи доказателства, че даден доставчик на цифрови услуги не отговаря на изискванията, установени в глава втора,	

	съответният национален компетентен орган предприема действия съгласно правомощията си по ал. 8. Тези доказателства могат да се предоставят от компетентен орган на друга държава - членка на Европейския съюз, в която доставчикът на цифрови услуги предоставя услугата. (10) Националните компетентни органи имат право да изискват от екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 информация по чл. 17, ал. 4, т. 1 и ал. 7. (11) Националните компетентни органи оказват съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл. 17, ал. 2, 3, 4 и 7. (12) Националните компетентни органи си сътрудничат с органите за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни. (13) Националните компетентни органи трябва да разполагат с технически, финансови и човешки ресурси, за да гарантират, че са в състояние да изпълняват ефективно възложените им задачи в съответствие с този закон. **Национално единно звено за контакт** Чл. 17. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национално единно звено за контакт. (2) Националното единно звено за контакт координира въпросите, свързани с мрежовата и информационната сигурност, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави – членки на Европейския съюз. (3) Националното единно звено за контакт предоставя на всеки две години на Европейската комисия информация относно последователността на подходите за определянето на операторите на съществени услуги, която включва: 1. националните мерки, чрез които са определени операторите на съществени услуги; 2. списък на съществените услуги; 3. броя на операторите на съществени услуги, определени за всеки сектор в приложение № 1, и тяхното значение за този сектор;	

	4. праговете, когато има такива, за определяне на минималното ниво на доставяните услуги спрямо броя ползватели, разчитащи на тях; 5. значението на конкретния оператор на съществени услуги за поддържане на достатъчно ниво на услугата предвид наличието и на други възможности за предоставяне на тази услуга. (4) Националното единно звено за контакт уведомява Европейската комисия за: 1. обхвата на задачите на екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19, както и за съществените елементи от тяхната процедура за предприемане на действия при инциденти, след тяхното създаване или при изменение на статута или процедурите им; 2. приетата Национална стратегия за мрежова и информационна сигурност в тримесечен срок от приемането й. (5) При трансграничен инцидент Националното единно звено за контакт уведомява националното единно звено за контакт на другата засегната държава – членка на Европейския съюз, когато е постъпило искане по чл. 19, ал. 2, т. 9 от Националния екип за реагиране при инциденти с компютърната сигурност. (6) В случаите по ал. 5 Националното единно звено за контакт запазва търговските интереси на оператора на съществените услуги или на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомленията им, в съответствие с българското законодателство и с правото на Европейския съюз. (7) Националното единно звено за контакт представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления по чл. 21, ал. 3, чл. 22, ал. 2, чл. 23, ал. 2 и чл. 25, ал. 3, естеството на инцидентите и действията, предприети за разрешаването им. (8) Националното единно звено за контакт има право да изисква от националните компетентни органи информацията по ал. 3 и ал. 4, т. 1, а от Националния екип за реагиране при инциденти с компютърната сигурност – информацията по ал. 7. (9) В случай на необходимост националните компетентни органи и Националното единно звено за контакт осъществяват сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни.	

	Проект на Закон за изменение и допълнение на Закон за киберсигурност **Национални компетентни органи** **Чл. 16. (1)** Министерският съвет определя с решение административните органи, които изпълняват функциите на национални компетентни органи по киберсигурност за секторите и услугите, посочени в приложения I и II, когато такива не са създадени със специален закон. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Национален компетентен орган за всички административни органи, както и за лицата и организациите по чл. 4, т. 7 и 8, е Министерството на електронното управление. **(3)** Националните компетентни органи: 1. координират и контролират изпълнението на задачите, свързани с киберсигурността на административните органи и на всички други субекти; 2. (изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) приемат, след съгласуване с Министерството на електронното управление, насоки относно обстоятелствата, при които субектите по чл. 4 и чл. 4а са длъжни да уведомяват за инциденти; 3. оценяват дали административните органи, съществените и важните субекти по този закон изпълняват задълженията си по глава втора, както и въздействието на това изпълнение върху кибурсигурността и предприемат съответните мерки при неизпълнение; 4. изготвят препоръки и насоки по отношение на техническите области, които да се вземат предвид във връзка с използването на европейските или международните стандарти и спецификации от значение за киберсигурността; 5. изготвят препоръки и насоки, свързани с използването на вече съществуващите стандарти, включително националните, с цел еднаквото прилагане на глава втора. 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 секторния екип за реагиране при инциденти с компютърната сигурност (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) Националните компетентни органи гарантират, че екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 получават уведомления за инциденти по този закон. (5) Националните компетентни органи гарантират, че техните СЕРИКС си сътрудничат ефективно, ефикасно и сигурно чрез националните екипи за реагиране при инциденти с компютърната сигурност (НЕРИКС). : 1. информация, необходима за оценка на мрежовата и информационната им сигурност, включително съществуващи политики за сигурност, резултати от одити на мрежовата и информационната сигурност, когато са извършени от друг квалифициран одитор, и доказателствата, на които те се основават; 2. доказателства за ефективно изпълнение на препоръките от одити на мрежовата и информационната им сигурност. (10) Националните компетентни органи изискват от екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19 информация по чл. 17, ал. 4, т. 1 и ал. 7. (11) Националните компетентни органи оказват съдействие на Националното единно звено за контакт при изпълнение на функциите му по чл. 17, ал. 2, 3, 4 и 7. (12) Националните компетентни органи си сътрудничат с Комисията за защита на личните данни при работа по инцидентите, които водят до нарушаване на сигурността на лични данни. (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. **Национално единно звено за контакт** Чл. 17. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление е създадено Национално единно звено за контакт. (2) Националното единно звено за контакт координира въпросите, свързани с киберсигурността, и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави – членки на Европейския съюз. (3) Националното единно звено за контакт организира и координира дейността по предоставяне на информацията по чл. 6, ал. 3 на всеки две години (4) Националното единно звено за контакт уведомява Европейската комисия за: 1. обхвата на задачите на екипите за реагиране при инциденти с компютърната сигурност по чл. 18 и 19, както и за съществените елементи от тяхната процедура за предприемане на действия при инциденти, след тяхното създаване или при изменение на статута или процедурите им;	

	2. приетата Национална стратегия за киберсигурност в тримесечен срок от приемането ѝ. (5) 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). (6) При получаване на информация за трансграничен инцидент от Националното единно звено за контакт (НЕЗК) на друга държава членка НЕЗК уведомява съответните национални компетентни органи (НКО)/СЕРИКС и координира дейностите по разрешаване на инцидента на национално ниво, както и докладва резултатите на уведомяващия НЕЗК (7) При трансграничен инцидент Националното единно звено за контакт уведомява националното единно звено за контакт на другата засегната държава – членка на Европейския съюз, когато е постъпило искане по чл. 19, ал. 2, т. 9 от Националния екип за реагиране при инциденти с компютърната сигурност. (8) В случаите по ал. 5 и ал.7 Националното единно звено за контакт запазва търговските интереси на съществените и важни субекти, както и поверителността на информацията, съдържаща се в уведомленията им, в съответствие с българското законодателство и с правото на Европейския съюз. (9) Националното единно звено за контакт представя веднъж годишно обобщен доклад до Групата за сътрудничество относно получените уведомления от съществените и важните субекти за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях услуги, естеството на инцидентите и действията, предприети за разрешаването им. (10) Националното единно звено за контакт има право да изисква от националните компетентни органи информацията по ал. 3 и ал. 4, т. 1, а от Националния екип за реагиране при инциденти с компютърната сигурност – информацията по ал. 9. (11) Националното единно звено за контакт изготвя годишен обобщен доклад за оценка на риска, базиран на получените анализи от националните компетентни органи. (12) Националното единно звено за контакт при целесъобразност обменя информация с компетентните органи по чл. 46 от Регламент (ЕС) 2022/2554.	

	(13) В случай на необходимост националните компетентни органи и Националното единно звено за контакт осъществяват сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни.	
Член 9 **Национални рамки за управление на кризи в областта на киберсигурността** 1. Всяка държава членка определя или създава един или **повече компетентни органи, отговарящи за управлението на мащабните киберинциденти** и кризи (органи за управление на киберкризи). Държавите членки гарантират, че тези органи разполагат с адекватни ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. Държавите членки гарантират съгласуваност със съществуващите рамки за общо управление на кризи на национално равнище. 2. Когато държава членка определи или създаде повече от един орган за управление на киберкризи съгласно параграф 1, тя ясно указва кой от тези органи ще **служи като координатор** за управлението на мащабни киберинциденти и кризи. 3. Всяка държава членка набелязва способности, активи и **процедури, които** могат да бъдат разгърнати в случай на криза за целите на настоящата директива. 4. Всяка държава членка приема **национален план за реакция при мащабни киберинциденти** и кризи, в който се определят	**Закон за киберсигурност** **Съвет по киберсигурността** **Чл. 9. (1)** Съветът по киберсигурността е консултативен и координиращ орган към Министерския съвет по въпросите на киберсигурността. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Председател на Съвета по киберсигурността е министърът на електронното управление. (3) Членове на Съвета по киберсигурността са: 1. министърът на вътрешните работи; 2. министърът на отбраната; 3. министърът на външните работи; 4. министърът на финансите; 5. (изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на транспорта и съобщенията; 6. министърът на енергетиката; 7. министърът на здравеопазването; 8. министърът на околната среда и водите; 8а. (нова – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на електронното управление; 9. началникът на отбраната; 10. главният секретар на Министерството на вътрешните работи; 11. председателят на Държавна агенция "Национална сигурност"; 12. председателят на Държавна агенция "Разузнаване"; 13. (изм. – ДВ, бр. 69 от 2020 г.) директорът на Служба "Военно разузнаване"; 14. началникът на Националната служба за охрана; 15. (отм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.); 16. секретарят на Съвета по киберсигурността; 17. секретарят на Съвета по сигурността към Министерския съвет; 18. представител на президента на републиката, изрично определен от него с указ.	Пълно съответствие

целите и условията и редът за управлението на мащабни киберинциденти и кризи. По-конкретно в плана се установяват: а) целите на националните мерки и дейности за подготвеност; б) задачи и отговорности на органите за управление на киберкризи; в) процедурите за управление на киберкризи, включително тяхното интегриране в общата рамка за управление на кризи на национално равнище и канали за обмен на информация; г) националните мерки за подготвеност, включително дейности по учения и обучения; д) съответните заинтересовани страни от публичния и частния сектор и съответната инфраструктура; е) национални процедури и договорености между съответните национални органи и служби за осигуряване на ефективно участие и подкрепа от страна на държавата членка за координираното управление на мащабни киберинциденти и кризи на равнището на Съюза. 5. В срок от три месеца от определянето или създаването на органа за управление на киберкризи, посочен в параграф 1, всяка държава членка уведомява Комисията за самоличността на своя орган и за всички последващи промени в него. Държавите членки предоставят на Комисията и на Европейската мрежа за връзка на организациите при киберкризи (EU — CyCLONe)	(4) Президентът на републиката, председателят на Народното събрание и министър-председателят може да участват лично в заседанията на Съвета по киберсигурността. (5) В определени случаи и по отделни въпроси в работата на Съвета по киберсигурността по покана на неговия председател може да участват председатели на постоянни комисии на Народното събрание, народни представители и ръководители на ведомства и организации. Дейност на Съвета по киберсигурността Чл. 10. Съветът по киберсигурността: 1. анализира тенденциите на киберзаплахите, рисковете, методите за противодействие и за развитието на необходимия капацитет, приоритетите за изграждането и развитието на човешки, технологични, инфраструктурни, финансови и организационни компоненти и при необходимост предлага решения и действия по отношение на тях; 2. предлага на Министерския съвет Национална стратегия за киберсигурност и пътната карта към нея, както и изготвя периодичната им актуализация; 3. предоставя информация на Съвета по сигурността към Министерския съвет относно състоянието на сигурността в киберпространството за включване в проекта на годишен доклад за състоянието на националната сигурност по чл. 9, т. 7 от Закона за управление и функциониране на системата за защита на националната сигурност; 4. осъществява взаимодействие с компетентните органи в областта на киберсигурността, включително с националните компетентни органи по чл. 16, с Националното единно звено за контакт, с регулаторни органи и с други институции; 5. дава предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото; 6. предлага на Министерския съвет Национален план за управление на киберкризи; 7. взаимодейства със Съвета по сигурността към Министерския съвет. Национален координатор по киберсигурността	

съответната информация, свързана с изискванията на параграф 4, относно техните национални планове за реагиране при мащабни киберинциденти и кризи в срок от три месеца от приемането на тези планове. Държавите членки може да изключат информация, когато и доколкото такова изключване е необходимо за тяхната национална сигурност.	Чл. 11. (1) Министър-председателят определя национален координатор по киберсигурността, който е и секретар на Съвета по киберсигурността. (2) Националният координатор по киберсигурността: 1. ръководи изготвянето и актуализирането на Националната стратегия за киберсигурност и пътната карта към нея; 2. участва при изграждането и развитието на Националната координационно-организационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост; 3. участва при създаването и развитието на Националния киберситуационен център, координира действията и комплексната реакция при заплаха от киберкриза и заплахи от хибриден характер; 4. предлага на Съвета по киберсигурността: а) нива за оценка на заплахата от кибератаки и киберинциденти и критерии за определянето им; б) степени за определяне нивото на готовност за противодействие на кибератаки и киберинциденти – в зависимост от нивото на заплаха; в) мерките, които да се предприемат при съответните степени на готовност; 5. при необходимост, в състояние на повишена заплаха от кибер- или от хибриден характер, подпомага сформирането на екипи за анализ, реакция и възстановяване с участието на експерти от различни ведомства и организации; 6. съдейства при планирането, подготовката и провеждането на учения в областта на киберсигурността; 7. осигурява взаимодействие и подпомага дейността на секретаря на Съвета по сигурността към Министерския съвет. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** Съвет по киберсигурността Чл. 9. (1) Съветът по киберсигурността е консултативен и координиращ орган към Министерския съвет по въпросите на киберсигурността. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Председател на Съвета по киберсигурността е министърът на електронното управление.	

	(3) Членове на Съвета по киберсигурността са: 1. министърът на вътрешните работи; 2. министърът на отбраната; 3. министърът на външните работи; 4. министърът на финансите; 5. (изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на транспорта и съобщенията; 6. министърът на енергетиката; 7. министърът на здравеопазването; 8. министърът на околната среда и водите; 8а. (нова – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министърът на електронното управление; 8б. министърът на регионалното развитие и благоустройството; 8в. министърът на земеделието и храните; 9. началникът на отбраната; 10. главният секретар на Министерството на вътрешните работи; 11. председателят на Държавна агенция "Национална сигурност"; 12. председателят на Държавна агенция "Разузнаване"; 13. (изм. – ДВ, бр. 69 от 2020 г.) директорът на Служба "Военно разузнаване"; 14. началникът на Националната служба за охрана; 15. председателят на Комисия за регулиране на съобщенията; 16. секретарят на Съвета по киберсигурността; 17. секретарят на Съвета по сигурността към Министерския съвет; 18. представител на президента на републиката, изрично определен от него с указ. (4) Президентът на републиката, председателят на Народното събрание и министър-председателят може да участват лично в заседанията на Съвета по киберсигурността. (5) В определени случаи и по отделни въпроси в работата на Съвета по киберсигурността по покана на неговия председател може да участват председатели на постоянни комисии на Народното събрание, народни представители и ръководители на ведомства и организации. Дейност на Съвета по киберсигурността Чл. 10. Съветът по киберсигурността:	

	1. анализира тенденциите на киберзаплахите, рисковете, методите за противодействие и за развитието на необходимия капацитет, приоритетите за изграждането и развитието на човешки, технологични, инфраструктурни, финансови и организационни компоненти и при необходимост предлага решения и действия по отношение на тях; 2. предлага на Министерския съвет Национална стратегия за киберсигурност и пътната карта към нея, както и изготвя периодичната им актуализация; 3. предоставя информация на Съвета по сигурността към Министерския съвет относно състоянието на сигурността в киберпространството за включване в проекта на годишен доклад за състоянието на националната сигурност по чл. 9, т. 7 от Закона за управление и функциониране на системата за защита на националната сигурност; 4. осъществява взаимодействие с компетентните органи в областта на киберсигурността, включително с националните компетентни органи по чл. 16, с Националното единно звено за контакт, с регулаторни органи и с други институции; 5. дава предложения към Министерския Съвет за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото; 6. предлага на Министерския съвет Национален план за реакция при мащабни киберинциденти и кризи; 7. взаимодейства със Съвета по сигурността към Министерския съвет. **Национален координатор по киберсигурността** Чл. 11. (1) Министър-председателят определя национален координатор по киберсигурността, който е и секретар на Съвета по киберсигурността. (2) Националният координатор по киберсигурността: 1. ръководи изготвянето и актуализирането на Националната стратегия за киберсигурност и пътната карта към нея; 2. участва при изграждането и развитието на Националната координационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост;	

	3. участва в развитието на Националния киберситуационен център, координира действията и комплексната реакция при заплаха от киберкриза и заплахи от хибриден характер; 4. предлага на Съвета по киберсигурността: а) нива за оценка на заплахата от кибератаки и киберинциденти и критерии за определянето им; б) степени за определяне нивото на готовност за противодействие на кибератаки и киберинциденти – в зависимост от нивото на заплаха; в) мерките, които да се предприемат при съответните степени на готовност; 5. при необходимост, в състояние на повишена заплаха от кибер- или от хибриден характер, подпомага сформирането на екипи за анализ, реакция и възстановяване с участието на експерти от различни ведомства и организации; 6. съдейства при планирането, подготовката и провеждането на учения в областта на киберсигурността; 7. осигурява взаимодействие и подпомага дейността на секретаря на Съвета по сигурността към Министерския съвет. **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.	
Член 10 ***Екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС)*** 1. Всяка държава членка определя или създава един или повече ЕРИКС. ЕРИКС могат да бъдат определени или създадени в рамките на компетентен орган. ЕРИКС отговарят на изискванията, посочени в член 11, параграф 1, обхващат най-малко секторите, подсекторите и видовете субекти, посочени в приложения I и II, и отговарят за предприемането на действия при инциденти в съответствие с подробно определена процедура. 2. Държавите членки гарантират, че всеки ЕРИКС разполага с достатъчни ресурси, за да изпълнява ефективно задачите си, установени в член 11, параграф 3. 3. Държавите членки гарантират, че всеки ЕРИКС разполага с подходяща, сигурна и устойчива комуникационна и информационна инфраструктура за обмен на информация със съществените и важните субекти, както и с други относими заинтересовани страни. За тази цел държавите членки гарантират, че всеки ЕРИКС допринася за внедряването на сигурни инструменти за обмен на информация. 4. ЕРИКС си сътрудничат и, когато е подходящо, обменят относима информация в съответствие с член	**Закон за киберсигурност** **Секторни екипи за реагиране при инциденти с компютърната сигурност** **Чл. 18. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, включително Министерството на електронното управление, създават секторни екипи за реагиране при инциденти с компютърната сигурност. Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA). (2) Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания: 1. да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки момент и да бъдат ясно посочени и добре известни на субектите по чл. 4, ал. 1 и на партньорите; 2. секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони; 3. да осигуряват непрекъснатост на дейността си чрез: а) подходяща система за управление и разпределяне на заявките; б) достатъчен персонал, който да е постоянно на разположение; в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение; 4. изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и с българското законодателство.	Пълно съответствие

29 със секторни и междусекторни общности на съществените и важните субекти. 5. ЕРИКС участват в партньорски проверки, организирани в съответствие с член 19. 6. Държавите членки гарантират, че чрез мрежата на ЕРИКС техните ЕРИКС си сътрудничат ефективно, ефикасно и сигурно. 7. ЕРИКС могат да установяват отношения на сътрудничество с националните екипи за реагиране при инциденти с компютърната сигурност на трети държави. Като част от тези отношения на сътрудничество държавите членки улесняват ефективния, ефикасен и сигурен обмен на информация с тези национални екипи за реагиране при инциденти с компютърната сигурност 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). ЕРИКС могат да обменят съответна информация с националните екипи за реагиране при инциденти с компютърната сигурност на трети държави, включително лични данни в съответствие с правото на Съюза в областта на защитата на данните. 8. ЕРИКС могат да си сътрудничат с националните екипи за реагиране при инциденти с компютърната сигурност на трети държави или с равностойни органи на трети държави, по-специално с цел да им се предостави помощ в областта на киберсигурността. 9. Всяка държава членка уведомява Комисията без ненужно забавяне за идентификационните данни на ЕРИКС по параграф 1 от настоящия член, а ЕРИКС, определен за координатор съгласно член 12, параграф	(3) Секторните екипи за реагиране при инциденти с компютърната сигурност разполагат с ресурси за ефективно изпълнение на задачите си, които включват най-малко следното: 1. наблюдение на инциденти на национално равнище; 2. подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните субекти; 3. реакция при инциденти и оказване на методологическа помощ при разрешаване на инциденти – при поискване; 4. осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация. (4) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди. (5) С цел улесняване на сътрудничеството секторните екипи за реагиране при инциденти с компютърната сигурност насърчават възприемането и използването на общи практики за стандартизация за: 1. процедури за предприемане на действия при инциденти и рискове; 2. схеми за класификация на инциденти, рискове и информация. (6) Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност, която се изгражда от секторните екипи и от Националния екип по чл. 19. (7) Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон. (8) Секторните екипи за реагиране при инциденти с компютърната сигурност изпращат веднъж на три месеца обобщена статистическа информация до Националния екип за реагиране при инциденти с компютърната сигурност относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност.	

1, за съответните му задачи във връзка със съществените и важните субекти и за всички последващи промени в тях. 10. Държавите членки може да поискат помощ от ENISA при създаването на техните ЕРИКС.	(9) Секторните екипи за реагиране при инциденти с компютърната сигурност, обхващащи стратегически обекти и дейности, които са от значение за националната сигурност: 1. изграждат комуникационна свързаност с центъра по чл. 15, ал. 2, която се използва за подпомагане изпълнението на дейностите по чл. 15; 2. (в сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) уведомяват незабавно центъра по чл. 15, ал. 2 за настъпилите инциденти. (10) (В сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) В случаите по ал. 9, т. 2 последващите действия на субектите по чл. 4, ал. 1 се координират с центъра по чл. 15, ал. 2 и със съответния секторен екип за реагиране при инциденти с компютърната сигурност. **Национален екип за реагиране при инциденти с компютърнат сигурност** **Чл. 19. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национален екип за реагиране при инциденти с компютърната сигурност, който отговаря на изискванията на чл. 18, ал. 2. (2) Националният екип за реагиране при инциденти с компютърната сигурност: 1. действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво; 2. подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност; 3. участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност; 4. обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост; 5. предоставя съвети и препоръки на органите на държавната власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност; 6. оказва експертна подкрепа на административните органи и на други юридически лица при изграждане, внедряване и	

	поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област; 7. участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури; 8. при възникване на инциденти в мрежовата и информационната сигурност дава препоръчителни указания на административните органи, на националните компетентни органи и на секторните екипи за реагиране при инциденти с компютърната сигурност; 9. информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този закон, и в случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване; 10. участва в международни мрежи за сътрудничество. (3) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, оказват съдействие на Националния екип за реагиране при инциденти с компютърната сигурност за отстраняване на установени от него киберинциденти в техните мрежи и/или услуги. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Секторни екипи за реагиране при инциденти с компютърната сигурност** **Чл. 18. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Екипите се създават към националните компетентни органи в съответствие с методическите указания на „Агенцията на Европейския съюз за киберсигурност (ENISA)“. (2) 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 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). СЕРИКС могат да обменят съответна информация с НЕРИКС на трети държави, включително лични данни в съответствие с правото на Съюза в областта на защитата на данните. 4. при целесъобразност, предоставят на компетентните органи определени или създадени в съответствие с Регламент (ЕС) 2022/2554, относимо техническо становище и съдействие. (3) Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания: 1. да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки момент и да бъдат ясно посочени и добре известни на субектите по чл. 4, ал. 1 и на партньорите; 2. секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони; 3. да осигуряват непрекъснатост на дейността си чрез: а) подходяща система за управление и разпределяне на заявките; б) разполагат с достатъчно персонал, за да гарантират предоставянето по всяко време на техните услуги; в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение; 4. изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на „Агенцията на Европейския съюз за киберсигурност (ENISA)“ и с българското законодателство.	

	(4) 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, учзвимости 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) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди. (6) С цел улесняване на сътрудничеството СЕРИКС насърчават възприемането и използването на общи практики за стандартизация за: 1. процедури за предприемане на действия при инциденти и рискове; 2. схеми за класификация на инциденти, рискове и информация. (7) Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност, която се изгражда от секторните екипи и от НЕРИКС по чл. 19. (8) Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон.	

	(9) Секторните екипи за реагиране при инциденти с компютърната сигурност изпращат всеки месец обобщена статистическа информация до НЕРИКС относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност. (10) Секторните екипи за реагиране при инциденти с компютърната сигурност, обхващащи стратегически обекти и дейности, които са от значение за националната сигурност: 1. изграждат комуникационна свързаност с центъра по чл. 15, ал. 2, която се използва за подпомагане изпълнението на дейностите по чл. 15; 2. (в сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) уведомяват незабавно центъра по чл. 15, ал. 2 за настъпилите инциденти. (11) (В сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) В случаите по ал. 9, т. 2 последващите действия на субектите по чл. 4, ал. 1 се координират с центъра по чл. 15, ал. 2 и със съответния секторен екип за реагиране при инциденти с компютърната сигурност. Национален екип за реагиране при инциденти с компютърната сигурност (НЕРИКС) Чл. 19. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Национален екип за реагиране при инциденти с компютърната сигурност, отговаря на изискванията на чл. 18, ал. 1 - 6. (2) Националният екип за реагиране при инциденти с компютърната сигурност: 1. действа като звено за контакт по въпроси, свързани с мрежовата и информационната сигурност на национално ниво и по оперативни въпроси на международно ниво; 2. подпомага дейностите по създаването на секторните екипи за реагиране при инциденти с компютърната сигурност; 3. участва в изграждането и дейностите на Националната мрежа на екипите за реагиране при инциденти с компютърната сигурност; 4. обобщава и анализира предоставената информация от секторните екипи за реагиране при инциденти с компютърната сигурност и изготвя доклади в случай на необходимост;	

	5. предоставя съвети и препоръки на органите на държавната власт, органите на местното самоуправление и юридическите лица, създадени със специален закон, по важни въпроси, свързани с мрежовата и информационната сигурност; 6. оказва експертна подкрепа на административните органи и на други юридически лица при изграждане, внедряване и поддържане в актуално състояние на системи за управление на информационната сигурност съгласно националните и международните стандарти в тази област; 7. участва в разработването и тестването на национални и по линия на Европейския съюз и НАТО стандартни оперативни процедури; 8. при възникване на киберинциденти дава препоръчителни указания на административните органи, на националните компетентни органи и на секторните екипи за реагиране при инциденти с компютърната сигурност; 9. информира незабавно Националното единно звено за контакт за уведомленията за трансгранични инциденти със значително увреждащо въздействие и за трансгранични инциденти със съществено въздействие, подадени съгласно този закон, и в случай на необходимост иска съдействие от Националното единно звено за контакт за тяхното разрешаване; 10. участва в международни мрежи за сътрудничество. 11. НЕРИКС, определен за координатор съгласно чл. 19, ал. 4, уведомява Комисията за съответните му задачи във връзка със съществените и важните субекти и за всички последващи промени в тях. (3) Предприятията, предоставящи обществени електронни съобщителни мрежи и/или услуги, оказват съдействие на Националния екип за реагиране при инциденти с компютърната сигурност за отстраняване на установени от него киберинциденти в техните мрежи и/или услуги. (4) Националният екип за реагиране при инциденти с компютърната сигурност осъществява функциите на координатор за целлите 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.	
Член 11 ***Изисквания към ЕРИКС, технически възможности и задачи на ЕРИКС*** 1. ЕРИКС отговарят на следните изисквания: а) ЕРИКС гарантират високо ниво на достъпност на своите комуникационни канали, като не допускат съществуването на точки, повредата в които може да доведе до общ срив, и разполагат с различни средства, чрез които могат да установяват връзка и да бъдат търсени във всеки един момент. Те посочват ясно комуникационните канали и ги оповестяват на заинтересованите страни и на партньорите от сътрудничеството; б) помещенията и поддържащите дейността на ЕРИКС информационни системи се разполагат в зони за сигурност;	**Закон за киберсигурност** ***Секторни екипи за реагиране при инциденти с компютърната сигурност*** **Чл. 18. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, включително Министерството на електронното управление, създават секторни екипи за реагиране при инциденти с компютърната сигурност. Екипите се създават към националните компетентни органи в съответствие с методическите указания на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA). (2) Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания: 1. да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки	Пълно съответствие

в) ЕРИКС разполагат с подходяща система за управление и разпределяне на заявките, по-специално за да се улесни ефективното и ефикасно предаване на задачите от един на друг изпълнител; г) ЕРИКС гарантират поверителността и надеждността на своите операции; д) ЕРИКС разполагат с достатъчно персонал, за да гарантират предоставянето по всяко време на техните услуги, както и гарантират, че техният персонал е обучен подобаващо; е) ЕРИКС разполагат с резервни системи и резервно работно пространство, за да гарантират непрекъснатост своите услуги; ЕРИКС могат да участват в мрежи за международно сътрудничество. 2. Държавите членки гарантират, че техните ЕРИКС разполагат съвместно с техническите възможности, за да изпълняват задачите, установени в параграф 3. Държавите членки гарантират, че на техните ЕРИКС са разпределени достатъчно ресурси, за да се осигури адекватно кадрово обезпечаване с оглед на даването на възможност на ЕРИКС да развият техническите си способности. 3. ЕРИКС имат следните задачи: а) наблюдение и анализ на киберзаплахи, уязвимости и инциденти на национално равнище, както и, при поискване, предоставяне на помощ за засегнати съществени и важни субекти във връзка с наблюдението на техните мрежови и информационни системи в реално време или почти в реално време; б) подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за киберзаплахи, уязвимости и инциденти до засегнатите съществени и важни субекти, както и до компетентните органи и други относими заинтересовани страни, по възможност в почти реално време;	момент и да бъдат ясно посочени и добре известни на субектите по чл. 4, ал. 1 и на партньорите; 2. секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони; 3. да осигуряват непрекъснатост на дейността си чрез: а) подходяща система за управление и разпределяне на заявките; б) достатъчен персонал, който да е постоянно на разположение; в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение; 4. изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на Европейския съюз, с указанията на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и с българското законодателство. (3) Секторните екипи за реагиране при инциденти с компютърната сигурност разполагат с ресурси за ефективно изпълнение на задачите си, които включват най-малко следното: 1. наблюдение на инциденти на национално равнище; 2. подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните субекти; 3. реакция при инциденти и оказване на методологическа помощ при разрешаване на инциденти – при поискване; 4. осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация. (4) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди. (5) С цел улесняване на сътрудничеството секторните екипи за реагиране при инциденти с компютърната сигурност насърчават възприемането и използването на общи практики за стандартизация за: 1. процедури за предприемане на действия при инциденти и рискове; 2. схеми за класификация на инциденти, рискове и информация. (6) Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност,	

в) реагиране на инциденти и оказване на помощ на засегнатите съществени и важни субекти, когато е приложимо; г) събиране и анализиране на криминалистични данни и осигуряване на динамичен анализ на рисковете и инцидентите и ситуационна осведоменост за киберсигурността; д) предоставяне, по искане на съществен или важен субект, на проактивно сканиране на мрежовите и информационните системи на съответния субект с цел откриване на уязвимости с потенциално значително въздействие; е) участие в мрежата на ЕРИКС и предоставяне според техните способности и компетенции на взаимопомощ на останалите членове на мрежата на ЕРИКС при заявка от тяхна страна; ж) когато е приложимо, действие като координатор за целите на координираното оповестяване на уязвимости съгласно член 12, параграф 1; з) допринасяне за внедряването на сигурни инструменти за обмен на информация съгласно член 10, параграф 3. ЕРИКС могат да извършват проактивно неинвазивно сканиране на публично достъпни мрежови и информационни системи на съществени и важни субекти. Такова сканиране се извършва с цел откриване на уязвими или конфигурирани по необезопасен начин мрежови и информационни системи и за информиране на засегнатите субекти. Такова сканиране не трябва да има отрицателно въздействие върху функционирането на услугите на субектите.	която се изгражда от секторните екипи и от Националния екип по чл. 19. (7) Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон. (8) Секторните екипи за реагиране при инциденти с компютърната сигурност изпращат веднъж на три месеца обобщена статистическа информация до Националния екип за реагиране при инциденти с компютърната сигурност относно всички регистрирани от тях инциденти в мрежовата и информационната сигурност. (9) Секторните екипи за реагиране при инциденти с компютърната сигурност, обхващащи стратегически обекти и дейности, които са от значение за националната сигурност: 1. изграждат комуникационна свързаност с центъра по чл. 15, ал. 2, която се използва за подпомагане изпълнението на дейностите по чл. 15; 2. (в сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) уведомяват незабавно центъра по чл. 15, ал. 2 за настъпилите инциденти. (10) (В сила от 31.12.2023 г. - изм., ДВ, бр. 85 от 2020 г.) В случаите по ал. 9, т. 2 последващите действия на субектите по чл. 4, ал. 1 се координират с центъра по чл. 15, ал. 2 и със съответния секторен екип за реагиране при инциденти с компютърната сигурност. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Секторни екипи за реагиране при инциденти с компютърната сигурност** Чл. 18. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Административните органи по чл. 16, ал. 1, създават секторни екипи за реагиране при инциденти с компютърната сигурност (СЕРИКС). Екипите се създават към националните компетентни органи в съответствие с методическите указания на „Агенцията на Европейския съюз за киберсигурност (ENISA)“.	

При изпълнението на задачите, посочени в първа алинея, ЕРИКС могат да дадат приоритет на конкретни задачи въз основа на основан на риска подход. 4. ЕРИКС изграждат отношения на сътрудничество с относими заинтересовани страни в частния сектор, с цел постигане на целите на настоящата директива. 5. За да улеснят сътрудничеството, посочено в параграф 4, ЕРИКС насърчават приемането и използването на общи или стандартизирани практики, схеми за класификация и таксономии във връзка с: а) процедури за предприемане на действия при инциденти; б) управление на кризи; както и в) координирано оповестяване на уязвимости съгласно член 12, параграф 1.	(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 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). СЕРИКС могат да обменят съответна информация с НЕРИКС на трети държави, включително лични данни в съответствие с правото на Съюза в областта на защитата на данните. 4. при целесъобразност, предоставят на компетентните органи определени или създадени в съответствие с Регламент (ЕС) 2022/2554, относимо техническо становище и съдействие. (3) Секторните екипи осъществяват дейността си в съответствие с процедури, утвърдени от ръководителя на ведомството, към което са създадени, и отговарят на следните изисквания: 1. да разполагат с комуникационни канали с висока надеждност, които да осигуряват възможност да бъдат търсени във всеки момент и да бъдат ясно посочени и добре известни на субектите по чл. 4, ал. 1 и на партньорите; 2. секторните екипи и информационните системи, поддържащи тяхната дейност, да са разположени в защитени зони; 3. да осигуряват непрекъснатост на дейността си чрез: а) подходяща система за управление и разпределяне на заявките; б) разполагат с достатъчно персонал, за да гарантират предоставянето по всяко време на техните услуги; в) инфраструктура с гарантирана непрекъснатост на дейността, осигурена от резервни системи и резервно работно помещение; 4. изпълнението на реактивни, проактивни дейности и дейности по управление на качеството на сигурността да е в съответствие с регламентиращите и препоръчителните документи на	

	Европейския съюз, с указанията на „Агенцията на Европейския съюз за киберсигурност (ENISA)“ и с българското законодателство. (4) 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, учзвимости 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) Секторните екипи за реагиране при инциденти с компютърната сигурност осъществяват сътрудничество с частния сектор и с академичните среди. (6) С цел улесняване на сътрудничеството СЕРИКС насърчават възприемането и използването на общи практики за стандартизация за: 1. процедури за предприемане на действия при инциденти и рискове; 2. схеми за класификация на инциденти, рискове и информация. (7) Секторните екипи за реагиране при инциденти с компютърната сигурност си сътрудничат в Национална мрежа на екипите за реагиране при инциденти с компютърната сигурност, която се изгражда от секторните екипи и от НЕРИКС по чл. 19. (8) Секторните екипи за реагиране при инциденти с компютърната сигурност информират незабавно Националния	

	екип за реагиране при инциденти с компютърната сигурност за уведомленията за инциденти със значително увреждащо въздействие, за инциденти със съществено въздействие и за трансгранични инциденти, подадени съгласно този закон.	
Член 12 ***Координирано оповестяване на уязвимости и Европейска база данни за уязвимостите*** 1. Всяка държава членка определя един от своите екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) като координатор за целите на координираното оповестяване на уязвимости. Определеният за координатор ЕРИКС 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. Задачите на определения за координатор ЕРИКС 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. Държавите членки гарантират, че физическите или юридическите лица могат да докладват анонимно на определения за координатор ЕРИКС за уязвимост, при поискване от тяхна страна в тази връзка. Определеният за координатор ЕРИКС гарантира, че се извършват надлежни последващи действия по	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Национален екип за реагиране при инциденти с компютърната сигурност (НЕРИКС)** **Чл. 19. (1)** (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Национален екип за реагиране при инциденти с компютърната сигурност, отговаря на изискванията на чл. 18, ал. 1 - 6. (4) Националният екип за реагиране при инциденти с компютърната сигурност осъществява функциите на координатор за целлите 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.	Пълно съответствие

отношение на докладваната уязвимост, и гарантира анонимността на физическото или юридическото лице, докладващо за уязвимостта. Когато докладвана уязвимост би могла да окаже значително въздействие върху субекти в повече от една държава членка, определеният за координатор ЕРИКС на всяка засегната държава членка, по целесъобразност, си сътрудничи с други определени за координатори ЕРИКС в рамките на мрежата на ЕРИКС. 2. ENISA разработва и поддържа, след консултация с групата за сътрудничество, Европейска база данни за уязвимостите. За тази цел ENISA създава и поддържа подходящите информационни системи, политики и процедури и приема необходимите технически и организационни мерки, за да гарантира сигурността и целостта на Европейската база данни за уязвимостите, по-специално за да даде възможност на субектите, независимо дали попадат в обхвата на настоящата директива, и техните доставчици на мрежови и информационни системи да оповестяват и регистрират, на доброволна основа, публично известни уязвимости, налични в ИКТ продукти или ИКТ услуги. На всички заинтересовани страни се предоставя достъп до информацията за уязвимостите, съдържаща се в Европейската база данни за уязвимостите. Тази база данни включва: а) информация, описваща уязвимостта; б) засегнатите ИКТ продукти или ИКТ услуги и тежестта на уязвимостта с оглед на обстоятелствата, при които тя може да бъде използвана злонамерено; в) наличността на съответните корекции и, при липса на налични корекции, насоки, предоставени от компетентните органи или ЕРИКС, насочени към потребителите на уязвими ИКТ продукти и ИКТ		

услуги за това как да бъде ограничен рискът, произтичащ от оповестените уязвимости.		
Член 13 **Сътрудничество на национално равнище** 1. Ако са отделени, компетентните органи, единното звено за контакт и ЕРИКС на една и съща държава членка си сътрудничат по отношение на изпълнението на задълженията, предвидени в настоящата директива. 2. Държавите членки гарантират, че техните ЕРИКС или, когато е приложимо, техните компетентни органи, получават уведомления за значителни инциденти съгласно член 23, и за инциденти, киберзаплахи и ситуации, близки до инциденти, съгласно член 30. 3. Държавите членки гарантират, че техните ЕРИКС или, когато е приложимо, техните компетентни органи информират техните единни звена за контакт за уведомления за инциденти, киберзаплахи и ситуации, близки до инциденти, подадени съгласно настоящата директива. 4. За да се гарантира ефективното изпълнение на задачите и задълженията на компетентните органи, единните звена за контакт и ЕРИКС, държавите членки осигуряват, доколкото е възможно, подходящо сътрудничество между тези образувания и правоприлагащите органи, органите за защита на данните, националните органи съгласно регламенти (ЕО) № 300/2008 и (ЕС) 2018/1139, надзорните органи съгласно Регламент (ЕС) № 910/2014, компетентните органи съгласно Регламент(ЕС) 2022/2554,	Закон за киберсигурност Сътрудничество и координация Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министерството на електронното управление координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция "Национална сигурност", Министерството на вътрешните работи и Министерството на отбраната. (3) За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят със споразумение за взаимодействие между заинтересованите ведомства. (4) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление може да създава междуведомствени оперативни групи с участието на ведомства, организации и институции, включително от частния сектор, имащи отношение към тези дейности. (5) Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност – в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност.	Пълно съответствие

националните регулаторни органи съгласно Директива (ЕС) 2018/1972, компетентните органи съгласно Директива (ЕС) 2022/2557, както и компетентните органи съгласно други специфични за сектора правни актове на Съюза, в рамките на тази държава членка. 5. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива и техните компетентни органи съгласно Директива (ЕС) 2022/2557 редовно си сътрудничат и обменят информация във връзка с установяване на критичните субекти по отношение на рискове, киберзаплахи и инциденти, както и за несвързани с киберпространството рискове, заплахи и инциденти, засягащи субекти, установени като критични субекти съгласно Директива (ЕС) 2022/2557, и за мерки, взети в отговор на такива рискове, опасности и инциденти. Държавите членки гарантират също, че техните компетентни органи съгласно настоящата директива и техните компетентни органи съгласно Регламент (ЕС) № 910/2014, Регламент (ЕС) 2022/2554 и Директива (ЕС) 2018/1972 редовно обменят съответната информация, включително по отношение на съответните инциденти и киберзаплахи. 6. Държавите членки опростяват чрез технически средства докладването за уведомленията, посочени в членове 23 и 30.	Проект на Закон за изменение и допълнение на Закон за киберсигурност Сътрудничество и координация Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (2) За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят между заинтересованите ведомства. (3) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление създава междуведомствена оперативна група с участието на ведомства, организации и институции, включително от частния и академичния сектор, имащи отношение към тези дейности. (4) 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.	

ГЛАВА III **СЪТРУДНИЧЕСТВО НА РАВНИЩЕТО НА СЪЮЗА И НА МЕЖДУНАРОДНО РАВНИЩЕ** **Член 14** Група за сътрудничество 1. С цел подкрепа и улесняване на стратегическото сътрудничество и обмена на информация между държавите членки, както и с цел укрепване на доверието, се създава група за сътрудничество. 2. Групата за сътрудничество изпълнява задачите си въз основа на двугодишните работни програми, посочени в параграф 7. 3. Групата за сътрудничество се състои от представители на държавите членки, Комисията и ENISA. Европейската служба за външна дейност участва в дейностите на групата за сътрудничество като наблюдател. Европейските надзорни органи (ЕНО) и компетентните органи съгласно Регламент (ЕС) 2022/2554 могат да участват в дейностите на групата за сътрудничество в съответствие с член 47, параграф 1 от посочения регламент. Групата за сътрудничество може да кани Европейския парламент и представители на съответните заинтересовани страни да участват в нейната работа, когато това е целесъобразно. Комисията осигурява административното обслужване.	**Закон за киберсигурност** **Сътрудничество и координация** **Чл. 20. (1)** Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (5) Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност – в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Сътрудничество и координация** Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (4) 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. Партньорски проверки	Пълно съответствие

4. Групата за сътрудничество изпълнява следните задачи: а) предоставяне на насоки на компетентните органи във връзка с транспонирането и прилагането на настоящата директива; б) предоставяне на насоки на компетентните органи във връзка с разработването и прилагането на политики за координирано оповестяване на уязвимости, както е посочено в член 7, параграф 2, буква в); в) обмен на най-добри практики и информация във връзка с прилагането на настоящата директива, включително във връзка с киберзаплахи, инциденти, уязвимости, ситуации, близки до инциденти, инициативи за повишаване на осведомеността, обучение, учения и умения, изграждане на капацитет, стандарти и технически спецификации, както и установяването на съществени и важни субекти съгласно член 2, параграф 2, букви б) — д); г) обмен на консултации и сътрудничество с Комисията по възникващи инициативи за политики в областта на киберсигурността и цялостната съгласуваност на специфичните за сектора изисквания в областта на киберсигурността; д) взаимни консултации и сътрудничество с Комисията по проекти за делегирани актове или актове за изпълнение, приети съгласно настоящата директива; е) обмен на най-добри практики и информация с относимите институции, органи, служби и агенции на Съюза; ж) размяна на мнения относно прилагането на специфичните за сектора правни актове на Съюза, които съдържат разпоредби относно киберсигурността; з) по целесъобразност, обсъждане на доклади от партньорски проверки съгласно посоченото в член 19, параграф 9 и изготвяне на заключения и препоръки;	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 националните 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.	

и) извършване на координирани оценки на риска за сигурността на критичните вериги на доставки в съответствие с член 22, параграф 1; й) обсъждане на случаи на взаимопомощ, включително опит и резултати от трансгранични съвместни надзорни действия, както е посочено в член 37; к) по искане на една или повече засегнати държави членки — обсъждане на конкретните искания за взаимопомощ, както е посочено в член 37; л) предоставяне на стратегически насоки на мрежата на ЕРИКС и EU-CyCLONe по конкретни възникващи въпроси; м) обмен на мнения относно политиката за последващи действия след мащабни киберинциденти и кризи въз основа на извлечените поуки от мрежата на ЕРИКС и EU-CyCLONe; н) допринасяне за способностите в областта на киберсигурността в Съюза посредством улесняване на обмена на национални длъжностни лица чрез програма за изграждане на капацитет, включваща персонал от компетентните органи или ЕРИКС; о) организиране на редовни съвместни заседания с относимите частни заинтересованите страни от Съюза с цел обсъждане на дейностите, извършвани от групата за сътрудничество, и събиране на информация относно възникващите предизвикателства пред политиките; п) обсъждане на работата, предприета във връзка с ученията в областта на киберсигурността, включително извършената от ENISA работа; р) установяване на методологията и организационните аспекти на партньорските проверки, посочени в член 19, параграф 1, както и определяне на методологията за самооценка за държавите членки в съответствие с член 19, параграф 5 със съдействието на Комисията и ENISA, и в сътрудничество с Комисията и ENISA – разработване на кодекси за поведение, които да		

залегнат в основата на работните методи на определените експерти по киберсигурността в съответствие с член 19, параграф 6; с) изготвяне на доклади за целите на прегледа, посочен в член 40, относно опита, натрупан на стратегическо и оперативно равнище и от партньорските проверки; т) обсъждане и редовно извършване на оценка на актуалното състояние на киберзаплахите или инцидентите, като например софтуер за изнудване. Групата за сътрудничество представя на Комисията, на Европейския парламент и на Съвета докладите, посочени в първа алинея, буква с). 5. Държавите членки гарантират ефективно, ефикасно и сигурно сътрудничество на своите представители в групата за сътрудничество. 6. Групата за сътрудничество може да изисква от мрежата на ЕРИКС технически доклади по избрани теми. 7. До 1 февруари 2024 г. и на всеки две години след това, групата за сътрудничество изготвя работна програма за действията, които трябва да бъдат предприети за изпълнение на нейните цели и задачи. 8. Комисията може да установи чрез актове за изпълнение процедурните правила, необходими за работата на групата за сътрудничество. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 39, параграф 2. Комисията обменя становища и си сътрудничи с групата за сътрудничество във връзка с проектите на актове за изпълнение, посочени в първа алинея от		

настоящия параграф в съответствие с параграф 4, буква д). 9. Групата за сътрудничество провежда заседания редовно и във всеки случай поне веднъж годишно с групата за устойчивост на критичните субекти, създадена съгласно Директива (ЕС) 2022/2557 за да се насърчават и улесняват стратегическото сътрудничество и обменът на информация.		
Член 15 **Мрежа на ЕРИКС** 1. Създава се мрежа на националните ЕРИКС, с цел да се допринесе за изграждането на доверие между държавите членки и да се насърчи бързото и ефективно оперативно сътрудничество между държавите членки. 2. Мрежата на ЕРИКС се състои от представители на ЕРИКС, определени или създадени съгласно член 10, и екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на Съюза (CERT-EU). Комисията участва в мрежата на ЕРИКС като наблюдател. ENISA осигурява административното обслужване и активно оказват помощ за сътрудничеството между ЕРИКС. 3. Мрежата на ЕРИКС изпълнява следните задачи: а) обмен на информация относно способностите на ЕРИКС; б) улесняване на споделянето, трансфера и обмена на технологии и съответните мерки, политики,	**Закон за киберсигурност** **Сътрудничество и координация** Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (5) Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност – в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност. **§ 3.ДР** **22. "Мрежата на националните екипи** за реагиране при инциденти с компютърната сигурност" е мрежата по смисъла на чл. 12 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ, L 194/1 от 19 юли 2016 г.). **Проект на Закон за изменение и допълнение на Закон за киберсигурност** Сътрудничество и координация	Пълно съответствие

инструменти, процеси, най-добри практики и рамки между ЕРИКС; в) обмен на относима информация за инциденти, ситуации, близки до инциденти, киберзаплахи, рискове и уязвимости; г) обмен на информация във връзка с публикации и препоръки в областта на киберсигурността; д) осигуряване на оперативна съвместимост по отношение на спецификациите и протоколите за обмен на информация; е) по искане на потенциално засегнат от инцидент член на мрежата на ЕРИКС — обмен и обсъждане на информация във връзка с този инцидент и свързаните киберзаплахи, рискове и уязвимости; ж) по искане на член на мрежата на ЕРИКС — обсъждане и, при възможност, осъществяване на координирана реакция на инцидент, констатиран в рамките на юрисдикцията на тази държава членка; з) предоставяне на държавите членки на помощ за справянето с трансгранични инциденти съгласно настоящата директива; и) сътрудничество, обмен на най-добри практики или предоставяне на помощ на ЕРИКС, определени за координатори съгласно член 12, параграф 1 с оглед на управлението на координирано оповестяване на уязвимости, които могат да имат значително въздействие върху субекти в повече от една държава членка; й) обсъждане и набелязване на допълнителни форми на оперативно сътрудничество, включително по отношение на: i) категории киберзаплахи и инциденти;	Чл. 20. (1) Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (4) 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.	

ii) ранни предупреждения; iii) взаимопомощ; iv) принципи и договорености за координация при реакция на трансгранични рискове и инциденти; v) допринасяне за националния план за реакция при мащабни киберинциденти и кризи в областта на киберсигурността, посочен в член 9, параграф 4, по искане на държава членка; к) информиране на групата за сътрудничество относно дейностите на мрежата на ЕРИКС и допълнителните форми на оперативно сътрудничество, обсъдени в съответствие с буква й), и при необходимост искане на насоки във връзка с това; л) извършване на равносметка от ученията в областта на киберсигурността, включително организираните от ENISA; м) по искане на отделен ЕРИКС — обсъждане на способностите и подготвеността на същия този ЕРИКС; н) сътрудничество и обмен на информация с регионални и центрове за операции по сигурността (ЦОС) и такива на равнището на Съюза с цел подобряване на общата ситуационна осведоменост за инциденти и киберзаплахи в ЕС; о) по целесъобразност обсъждане на доклади от партньорски проверки съгласно посоченото в член 19, параграф 9; п) предоставяне на насоки, с цел да се улесни сближаването на оперативните практики по отношение на прилагането на разпоредбите на настоящия член във връзка с оперативното сътрудничество.		

4. До 17 януари 2025 г., както и на всеки две години след това, за целите на посочения в член 40 преглед, мрежата на ЕРИКС извършва оценка на напредъка, постигнат по отношение на оперативното сътрудничество, и приема доклад. В доклада по-специално се правят заключения и препоръки въз основа на резултатите от партньорските проверки, посочени в член 19, извършени във връзка с националните ЕРИКС. Този доклад се представя на групата за сътрудничество. 5. Мрежата на ЕРИКС приема свой процедурен правилник. 6. Мрежата на ЕРИКС и EU-CyCLONe се споразумяват за процедурни правила и си сътрудничат въз основа на тях.		
Член 16 **Европейска мрежа за връзка на организациите при киберкризи (EU — CyCLONe)** 1. Европейската мрежа за връзка на организациите при киберкризи (EU — CyCLONe) е създадена с цел подпомагане на координираното управление на мащабни киберинциденти и кризи, свързани с киберсигурността, на оперативно равнище и осигуряване на редовния обмен на съответната информация сред държавите членки и институциите, органите, службите и агенциите на Съюза, се създава Европейската мрежа за връзка на организациите при киберкризи (EU — CyCLONe). 2. EU-CyCLONe се състои от представители на органите на държавите членки за управление на киберкризи, както и от Комисията в случаите, когато		Не подлежи на транспониране

потенциален или текущ мащабен киберинцидент има или е вероятно да окаже значително въздействие върху услугите и дейностите, попадащи в обхвата на настоящата директива. В други случаи Комисията участва в дейностите на EU-CyCLONe като наблюдател. ENISA осигурява административното обслужване на EU-CyCLONe и оказва подкрепа за сигурния обмен на информация, а също и предоставя необходимите инструменти в подкрепа на сътрудничеството между държавите членки, като гарантира сигурен обмен на информация. Когато това е целесъобразно, EU-CyCLONe може да кани представители на съответните заинтересовани страни да участват в нейната работа като наблюдатели. 3. EU-CyCLONe има следните задачи: а) повишаване на степента на подготвеност при управлението на мащабни киберинциденти и кризи; б) развитие на споделена ситуационна осведоменост за мащабни киберинциденти и кризи; в) оценка на последиците и въздействието на съответните мащабни киберинциденти и кризи и предлагане на възможни мерки за смекчаването им; г) координиране на управлението на мащабни киберинциденти и кризи и подпомагане на процеса на вземане на решения на политическо равнище във връзка с такива инциденти и кризи; д) обсъждане, по искане на засегната държава членка, на националните планове за реакция при мащабни киберинциденти и кризи, посочени в член 9, параграф 4. 4. EU-CyCLONe приема свой процедурен правилник.		

5. EU-CyCLONe докладва редовно на групата за сътрудничество относно управлението на мащабни киберинциденти и кризи, както и тенденции, като се фокусира по-специално върху тяхното въздействие върху съществените и важните субекти. 6. EU-CyCLONe си сътрудничи с мрежата на ЕРИКС въз основа на договорените процедурни правила, предвидени в член 15, параграф 6. 7. До 17 юли 2024 г. и на всеки 18 месеца след това, EU-CyCLONe представя доклад за оценка на своята работа на Европейския парламент и на Съвета.		
Член 17 **Международно сътрудничество** Когато това е целесъобразно, Съюзът може да сключва международни споразумения в съответствие с член 218 от ДФЕС с трети държави или международни организации, които допускат и уреждат участието им в определени дейности на групата за сътрудничество, мрежата на ЕРИКС и EU-CyCLONe. Тези споразумения са в съответствие с правото на Съюза в областта на защитата на данните.		Не подлежи на транспониране
Член 18 **Доклад за състоянието на киберсигурността в Съюза** 1. В сътрудничество с Комисията и групата за сътрудничество ENISA приема двугодишен доклад за състоянието на киберсигурността в Съюза и внася и представя този доклад пред Европейския парламент. Докладът, наред с другото, се предоставя в машинночетим формат и включва следното: а) оценка на риска в областта на киберсигурността на равнището на Съюза, като се отчита картината на киберзаплахите; б) оценка на развитието на		Не подлежи на транспониране

способностите в областта на киберсигурността в публичния и частния сектор в Съюза; в) оценка на общото равнище на осведоменост относно киберсигурността и киберхигиената сред гражданите и субектите, включително малките и средните предприятия; г) обобщена оценка на резултата от партньорските проверки по член 19; д) обобщена оценка на степента на зрялост на способностите и ресурсите в областта на киберсигурността в целия Съюз, включително тези на секторно равнище, както и на степента, в която националните стратегии за киберсигурност на държавите членки са приведени в съответствие. 2. В доклада се включват конкретни препоръки за политиките с оглед на справянето с недостатъците и повишаването на степента на киберсигурността в Съюза, както и резюме на констатациите за конкретния период от докладите за техническото състояние на киберсигурността на ЕС във връзка с инциденти и киберзаплахи, изготвяни от ENISA в съответствие с член 7, параграф 6 от Регламент (ЕС) 2019/881. 3. ENISA, в сътрудничество с Комисията, групата за сътрудничество и мрежата на ЕРИКС, изготвя методологията, включително съответните променливи, като качествени и количествени показатели, на обобщената оценка, посочена в параграф 1, буква д).		
Член 19 **Партньорски проверки** 1. До 17 януари 2025 г. групата за сътрудничество съставя, със съдействието на Комисията и ENISA и, когато е приложимо, мрежата	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Партньорски проверки** **Чл.20а (1)** Министъра на електронното управление може да изпрати искане до Групата за сътрудничество и „Агенцията на	Пълно съответствие

на ЕРИКС, методологията и организационните аспекти на партньорските проверки с цел извличане на поуки от споделения опит, укрепване на взаимното доверие, постигане на високо общо ниво на киберсигурност, както и подобряване на способностите и политиките на държавите членки в областта на киберсигурността, необходими за прилагането на настоящата директива. Участието в партньорски проверки е доброволно. Партньорските проверки се извършват от експерти по киберсигурност. Експертите по киберсигурността се определят от най-малко две държави членки, различни от държавата членка, която е обект на проверка. Партньорските проверки обхващат най-малко един от следните параметри: а) степента на прилагане на мерките за управлението на риска в областта на киберсигурността и задълженията за докладване, предвидени в членове 21 и 23; б) равнището на способностите, включително наличните финансови, технически и човешки ресурси, както и ефективността от изпълнението на задачите на компетентните органи; в) оперативните способности на ЕРИКС; г) степента на прилагане на взаимопомощта по член 37; д) степента на прилагане на договореностите за обмен на информация в областта на киберсигурността, посочени в член 29; е) специфични въпроси от трансгранично или междусекторно естество. 2. Методологията, посочена в параграф 1, включва обективни, недискриминационни, справедливи и прозрачни критерии, въз основа на които държавите членки определят експерти в областта на киберсигурността, отговарящи на условията за провеждане на партньорските проверки. Комисията и ENISA участват като наблюдатели в партньорските проверки.	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. 37о, 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.	

3. Държавите членки могат да определят специфични въпроси, както е посочено в параграф 1, буква е), за целите на дадена партньорска проверка. 4. Преди да започне дадена партньорска проверка, както е посочено в параграф 1, държавите членки съобщават на участващите държави обхвата, включително определените специфични въпроси съгласно параграф 3. 5. Преди започването на партньорската проверка държавата членка може да извърши самооценка на проверяваните аспекти и да предостави тази самооценка на определените експерти в областта на киберсигурността. Групата за сътрудничество, със съдействието на Комисията и ENISA, определя методологията за самооценка на държавите членки. 6. Партньорските проверки включват физически или виртуални посещения на място, както и дистанционен обмен на информация. С оглед на принципа на доброто сътрудничество държавата членка, която е обект на партньорска проверка, предоставя на определените експерти по киберсигурността информацията, необходима за оценката, без да се засяга правото на Съюза или националното право относно защитата на поверителна или класифицирана информация или защитата на основните функции на държавата, като например националната сигурност. Групата за сътрудничество, в сътрудничество с Комисията и ENISA, разработва подходящи кодекси за поведение, които са в основата на работните методи на определените експерти в областта на киберсигурността. Всяка информация, получена в процеса на партньорска проверка, се използва единствено за тази цел. Участващите в партньорската проверка експерти в областта на киберсигурността не оповестяват никаква		

чувствителна или поверителна информация, получена в хода на тази проверка, на които и да е трети страни. 7. След като са били обект на партньорска проверка в държава членка, същите аспекти не подлежат на последваща партньорска проверка в тази държава членка в рамките на две години след приключването на партньорската проверка, освен ако държавата членка не поиска друго или не се постигне съгласие за това след предложение на групата за сътрудничество. 8. Държавите членки гарантират, че всеки риск от конфликт на интереси, засягащ определените експерти по киберсигурността, се разкрива на останалите държави членки, групата за сътрудничество, Комисията и ENISA преди започването на партньорската проверка. Държавата членка, която е обект на партньорската проверка, може да възрази срещу определянето на конкретни експерти по киберсигурността по надлежно обосновани причини, съобщени на държавата членка, която ги е определила. 9. Участващите в партньорските проверки експерти в областта на киберсигурността изготвят доклади за констатациите и заключения от партньорската проверка. Държавите членки, които са обект на партньорска проверка, могат да представят коментари по проектите на доклади, които ги засягат, като тези коментари се прилагат към докладите. Докладите включват препоръки за подобряване на аспектите, обхванати от партньорската проверка. Докладите се представят на групата за сътрудничество и мрежата на ЕРИКС, ако това е целесъобразно. Държава членка, която е обект на партньорска проверка, може да реши да направи публично достъпен своя доклад или негова редактирана версия.		

ГЛАВА IV ***МЕРКИ ЗА УПРАВЛЕНИЕ НА РИСКА В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА И ЗАДЪЛЖЕНИЯ ЗА ДОКЛАДВАНЕ*** ***Член 20*** ***Управление*** 1. Държавите членки гарантират, че 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 член 21, следят за прилагането им и могат да бъдат подведени под отговорност за нарушение на посочения член от страна на субектите. Прилагането на настоящия параграф не засяга националното право по отношение на правилата за отговорност, прилагани към публичните институции, както и отговорността на държавните служители и на избраните или назначените длъжностни лица. 2. Държавите членки гарантират, че от членовете на управителните органи на съществените и важните субекти се изисква редовно да преминават през обучение, и насърчават съществените и важните субекти да предлагат подобно обучение на своите служители, с цел 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.	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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 посочени в ал.2 и за своите служители.	Пълно съответствие

Член 21 Мерки за управление на риска в областта на киберсигурността 1. Държавите членки гарантират, че съществените и важните субекти предприемат подходящи и пропорционални технически, оперативни и организационни мерки за управление на рисковете за сигурността на мрежовите и информационните системи, които тези субекти използват при своите операции или при предоставяне на своите услуги, както и за предотвратяване или свеждане до минимум на въздействието на инцидентите върху получателите на услугите им и върху други услуги. Като се вземат предвид последните постижения в тази област и, когато е приложимо, съответните европейски и международни стандарти, както и разходите за прилагането им, мерките, посочени в първа алинея, гарантират ниво на сигурност на мрежовите и информационните системи, съответстващо на породените рискове. При оценката на пропорцио- налността 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 сериозност, включително тяхното обществено и икономическо въздействие. 2. Мерките, посочени в параграф 1, се основават на подход, обхващащ всички опасности, който има за цел да защити мрежовите и информационните системи и физическата среда на тези системи от инциденти, и включват поне следното: а) политики за анализ на риска и сигурност на информационните системи; б) действия при инцидент;	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** *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, посочени в 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;	Пълно съответствие

в) непрекъснатост на стопанската дейност, например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи; г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите преки снабдители или доставчици на услуги; д) сигурност при придобиването на мрежови и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им; е) политики и процедури за оценяване на ефективността на мерките за управление на риска в областта на киберсигурността; ж) основни киберхигиенни практики и обучение в областта на киберсигурността; з) политики и процедури относно използването на криптография и, когато е целесъобразно, криптиране; и) сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи; й) 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. Държавите членки гарантират, че когато разглеждат въпроса кои мерки по параграф 2, буква г) от настоящия член 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. Държавите членки гарантират също така, че когато се разглежда въпросът кои мерки от посочените в същата	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 от настоящия член 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 по 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.	

буква 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 член 22, параграф 1. 4. Държавите членки гарантират, че когато един субект установи, че не спазва мерките, предвидени в параграф 2, той предприема без излишно забавяне всички необходими, подходящи и пропорционални коригиращи мерки.		
5. До 17 октомври 2024 г. Комисията приема актове за изпълнение за определяне на техническите и методологичните изисквания за мерките, посочени в параграф 2, по отношение на доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни, доставчиците на мрежи за доставка на съдържание, доставчиците на управлявани услуги, доставчиците на управлявани услуги за сигурност, доставчиците на онлайн места за търговия, на онлайн търсачките и на платформите на услуги за социални мрежи и доставчиците на удостоверителни услуги. Комисията може да приема актове за изпълнение за определяне на техническите и методологичните изисквания, както и на секторни изисквания, ако е необходимо, по отношение на мерките по параграф 2, по отношение на съществените и важните субекти, различни от посочените в първа алинея от настоящия параграф. При изготвянето на актовете за изпълнение, посочени в първа и втора алинея от настоящия параграф, Комисията доколкото е възможно следва		Не подлежи на транспониране

европейските и международните стандарти, както и съответните технически спецификации. Комисията обменя становища и си сътрудничи с групата за сътрудничество и ENISA по проектите на актове за изпълнение в съответствие с член 14, параграф 4, буква д). Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 39, параграф 2.		
Член 22 **Координирана на равнището на Съюза оценка на риска за сигурността на критични вериги за доставка** 1. Групата за сътрудничество, в сътрудничество с Комисията и ENISA, може да извършва координирани оценки на риска за сигурността на конкретни критични вериги за доставка на ИКТ услуги, ИКТ системи или ИКТ продуктови вериги за доставка, при които се вземат предвид техническите и, когато е уместно, нетехническите рискови фактори. 2. След консултиране с групата за сътрудничество и ENISA, и когато е целесъобразно, със съответните заинтересовани страни, Комисията установява конкретните критични ИКТ услуги, ИКТ системи или ИКТ продукти, които може да бъдат предмет на координирана оценка на риска за сигурността по параграф 1.		Не подлежи на транспониране
Член 23 **Задължения за докладване** 1. Всяка държава членка гарантира, че съществените и важните субекти уведомяват без ненужно забавяне нейния ЕРИКС, или, ако е приложимо, нейния компетентен орган в съответствие	**Закон за киберсигурност** **Глава втора** **МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ** ***Задължения на административните органи по отношение на изискванията за сигурност и уведомяване за инциденти***	Пълно съответствие

с параграф 4 за всеки инцидент, който има значително въздействие върху предоставянето на техните услуги, съгласно посоченото в параграф 3 (значителен инцидент). Когато е подходящо, засегнатите субекти уведомяват без ненужно забавяне получателите на техните услуги за значителни инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги. Всяка държава членка гарантира, че тези субекти докладват, наред с другото, всяка информация, позволяваща на ЕРИКС или, когато е приложимо, на компетентния орган да определи всякакво трансгранично въздействие на инцидентите. Актът на уведомяване сам по себе си не води до повишена отговорност за уведомяващия субект. Когато засегнатите субекти уведомят компетентния орган за значителен инцидент съгласно първа алинея, държавата членка гарантира, че този компетентен орган препраща уведомлението на ЕРИКС след получаването му. В случай на трансграничен или междусекторен значителен инцидент държавите членки гарантират, че техните единни звена за контакт получават своевременно съответната информация, нотифицирана в съответствие с параграф 4. 2. Когато е приложимо, държавите членки гарантират, че съществените и важните субекти съобщават без излишно забавяне на получателите на техните услуги, които са потенциално засегнати от значителна киберзаплаха, всички мерки или средства за защита, които тези получатели могат да предприемат като реакция на тази заплаха. Когато е целесъобразно, субектите уведомяват тези получатели и за самата значителна киберзаплаха. 3. Даден инцидент се **счита за значителен,** ако:	**Чл. 21. (1) Административните органи** осигуряват и отговарят за сигурността на използваните от тях мрежи и информационни системи. (2) Административните органи предприемат: 1. подходящи и пропорционални мерки, които трябва да осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск; 2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на дейността им; 3. мерките, определени с наредбата по чл. 3, ал. 2. (3) Административните органи уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на тяхната дейност. (4) Първоначално уведомяване се прави до два часа след констатирането на инцидента. Уведомленията се подават по образец съгласно наредбата по чл. 3, ал. 2 и съдържат информация, която дава възможност на секторния екип да определи евентуалното трансгранично въздействие на инцидента. (5) В срок до 5 работни дни административният орган предоставя на секторния екип пълната информация за инцидента, определена с наредбата по чл. 3, ал. 2. (6) При наличие на обосновано предположение, че докладваният инцидент може да се класифицира като компютърно престъпление, секторният екип уведомява Главна дирекция "Борба с организираната престъпност" на Министерството на вътрешните работи. (7) Секторният екип запазва поверителността на информацията, съдържаща се в уведомленията. Задължения на лицата, осъществяващи публични функции, и на организациите, предоставящи обществени услуги, по отношение на изискванията за сигурност и уведомяване за инциденти **Чл. 22. (1) Лицата и организациите по чл. 4, ал. 1, т. 3 и** 4 осигуряват и отговарят за мрежовата и информационната си сигурност при предоставянето на административни услуги по електронен път.	

а) е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект; б) е засегнал или е в състояние да засегне други физически или юридически лица, причинявайки значителни материални или нематериални вреди. 4. Държавите членки гарантират, че за целите на уведомяването по параграф 1 засегнатите субекти подават до ЕРИКС или, когато е приложимо, до компетентния орган: а) без ненужно забавяне и при всички случаи в рамките на 24 часа след узнаването за 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; б) без ненужно забавяне и при всички случаи в рамките на 72 часа след узнаването за значителния инцидент — уведомление за инцидент, в което, когато е приложимо, се актуализира информацията, посочена в буква а), и се посочва първоначална оценка на значителния инцидент, включително неговата тежест и въздействие, както и, когато има такива, показателите за нарушена сигурност; в) по искане на ЕРИКС или, когато е приложимо, на компетентния орган — междинен доклад за съответните новости на състоянието; г) окончателен доклад не по-късно от един месец след подаването на уведомлението за инцидента по буква б), включващ следното:	(2) Лицата и организациите по ал. 1 уведомяват секторния екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път. В тези случаи се прилага съответно чл. 21, ал. 4, 5 и 6. (3) Секторният екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на лицата и организациите по ал. 1, както и поверителността на информацията, съдържаща се в уведомленията им. Задължения на операторите на съществени услуги по отношение на изискванията за сигурност и уведомяване за инциденти **Чл. 23. (1)** Операторите на съществени услуги предприемат: 1. подходящи и пропорционални мерки, които трябва да осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск; 2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, с цел осигуряване на непрекъснатост на предоставяните от тях съществени услуги; 3. мерките, определени с наредбата по чл. 3, ал. 2. (2) Операторите на съществени услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат въздействие върху непрекъснатостта на предоставяните от тях съществени услуги. В тези случаи се прилагат съответно чл. 21, ал. 4, 5 и 6. (3) Когато оператор на съществени услуги разчита на доставчик на цифрови услуги, за да предоставя съществена услуга, операторът уведомява доставчика на цифрови услуги за всяко значително увреждащо въздействие върху непрекъснатостта на съществената услуга, дължащо се на инцидент, засягащ доставчика на цифрови услуги. (4) Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на оператора на съществени услуги, както и поверителността на информацията, съдържаща се в уведомлението му. Задължения на доставчиците на цифрови услуги по отношение на изискванията за сигурност и уведомяване за инциденти **Чл. 25. (1)** Доставчиците на цифрови услуги предприемат:	

i) подробно описание на инцидента, включително неговата тежест и въздействие; ii) вида на заплахата или причината, която вероятно е породила инцидента; iii) приложените и текущите мерки за ограничаване; iv) когато е приложимо, трансграничното въздействие на инцидента; д) в случай на текущ инцидент към момента на представяне на окончателния доклад, посочен в буква г), държавите членки гарантират, че засегнатите субекти представят доклад за напредъка по това време и окончателен доклад в срок от един месец от справянето с инцидента. Чрез дерогация от първа алинея, буква б) доставчикът на удостоверителни услуги уведомява ЕРИКС или, когато е приложимо, компетентния орган за значителните инциденти, които оказват въздействие върху предоставянето на неговите удостоверителни услуги, без излишно забавяне и при всички случаи в рамките на 24 часа, след като е узнал за значителния инцидент. 5. ЕРИКС или компетентният орган предоставят, без излишно забавяне и когато е възможно в рамките на 24 часа след получаването на ранното предупреждение по параграф 4, буква а), отговор на уведомяващия субект, включително първоначална обратна информация за значителния инцидент и, при искане от субекта, насоки или оперативни съвети за прилагането на възможни мерки за ограничение.	1. подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тях при предоставянето на територията на Република България на услугите, посочени в приложение № 2; 2. подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи мрежовата и информационната им сигурност, върху предоставяните от тях на територията на Република България услуги, посочени в приложение № 2, с цел осигуряване на непрекъснатост на тези услуги; 3. мерките, определени с наредбата по чл. 3, ал. 2. (2) Мерките по ал. 1, т. 1 осигуряват ниво на мрежова и информационна сигурност, съответстващо на съществуващия риск, като са съобразени със: 1. сигурността на системите и съоръженията; 2. действията при инциденти; 3. управление на непрекъснатостта на дейностите; 4. наблюдение, одит и изпитване; 5. спазване на международни стандарти. (3) Доставчиците на цифрови услуги уведомяват съответния секторен екип за реагиране при инциденти с компютърната сигурност за инцидентите, които имат съществено въздействие върху непрекъснатостта на предоставяните от тях цифрови услуги. В тези случаи се прилагат съответно чл. 21, ал. 4, 5 и 6. (4) За определяне на въздействието на даден инцидент като съществено се вземат предвид: 1. броят ползватели, засегнати от инцидента, и по-специално ползвателите, които разчитат на услугата за предоставяне на собствените си услуги; 2. продължителността на инцидента; 3. географският обхват по отношение на областта, засегната от инцидента; 4. степента на нарушаване на функционирането на услугата; 5. степента на въздействие върху стопанските и обществените дейности. (5) Доставчиците на цифрови услуги подават уведомление по ал. 3 само когато имат достъп до информацията, която е необходима,	

Когато ЕРИКС не е първоначалният получател на уведомлението, посочено в параграф 1, насоките се предоставят от компетентния орган в сътрудничество с ЕРИКС. ЕРИКС предоставя допълнителна техническа подкрепа, ако засегнатия субект изиска това. Когато има подозрения, че значителният инцидент е с престъпно естество, ЕРИКС или компетентният орган предоставят насоки относно докладването на значителния инцидент на правоприлагащите органи. 6. Когато е целесъобразно и особено когато значителният инцидент засяга две или повече държави членки, ЕРИКС, компетентният орган или единното звено за контакт информира без излишно забавяне другите засегнати държави членки и ENISA за значителния инцидент. Тази информация включва вида информация, получена в съответствие с параграф 4. При това ЕРИКС, компетентният орган или единното звено за контакт запазват сигурността и търговските интереси на субекта, както и поверителността на предоставената информация в съответствие с правото на Съюза или с националното законодателство. 7. При необходимост от обществено уведомяване с цел предотвратяване на значителен инцидент или справяне с текущ значителен инцидент или когато оповестяването на значителния инцидент е в обществен интерес по друга причина, ЕРИКС на държавата членка, или когато е приложимо нейният компетентен орган, и когато е уместно, ЕРИКС или компетентните органи на други засегнати държави членки могат, след като се консултират със засегнатия субект, да уведомят обществеността за значителния инцидент или да изискат от него на направи това.	за да се оцени въздействието на инцидента като съществено съгласно ал. 4. (6) След консултация със засегнатия доставчик на цифрови услуги съответният секторен екип за реагиране при инциденти с компютърната сигурност и когато е приложимо, органите или екип за реагиране при инциденти с компютърната сигурност на други засегнати държави – членки на Европейския съюз, може да информират обществеността за отделни инциденти или да изискат от доставчика на цифрови услуги да информира за това, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент или когато разкриването на инцидента е в интерес на обществеността поради други причини. (7) Съответният секторен екип за реагиране при инциденти с компютърната сигурност запазва търговските интереси на доставчика на цифрови услуги, както и поверителността на информацията, съдържаща се в уведомлението му. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 23(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 забави 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.	

8. По искане на ЕРИКС или на компетентния орган единното звено за контакт предава уведомленията, получени съгласно параграф 1, на единните звена за контакт на други засегнати държави членки. 9. На всеки три месеца единното звено за контакт представя на ENISA обобщителен доклад, включващ анонимизирани и обобщени данни за значителните инциденти, инцидентите, киберзаплахите и ситуациите, близки до инциденти, за които е изпратено уведомление в съответствие с параграф 1 от настоящия член и с член 30. За да допринесе за предоставянето на сравнима информация, ENISA може да приема технически насоки за параметрите на включената в обобщителния доклад информация. ENISA информира групата за сътрудничество и мрежата на ЕРИКС за своите констатации относно получените уведомления на всеки шест месеца. 10. ЕРИКС или, когато е приложимо, компетентните органи предоставят на компетентните 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 параграф 1 от настоящия член и с член 30 от субектите, установени като критични субекти съгласно Директива (ЕС) 2022/2557. 11. Комисията може да приема актове за изпълнение, в които допълнително се уточняват видът на информацията, форматът и процедурата на изпратено по параграф 1 от настоящия член и по член 30 уведомление, и на съобщение, изпратено по параграф 2 от настоящия член. До 17 октомври 2024 г. Комисията приема – по отношение на доставчици на DNS услуги, регистрите	(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, посочена в точка 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:	

на имена на домейни от първо ниво, доставчици на компютърни услуги „в облак“, доставчици на услуги на центрове за данни, доставчици на мрежи за доставка на съдържание, доставчици на управлявани услуги, доставчици на управлявани услуги за сигурност, както и доставчици на онлайн места за търговия, на онлайн търсачките и на платформите на услуги за социални мрежи – актове за изпълнение, в които допълнително се уточняват случаите, в които даден инцидент се счита за значителен, както е посочено в параграф 3. Комисията може да приема такива актове за изпълнение по отношение на други съществени и важни субекти. Комисията обменя становища и си сътрудничи с групата за сътрудничество във връзка с проектите на актове за изпълнение, посочени в първа и втора алинея от настоящия параграф в съответствие с член 14, параграф 4, буква д). Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 39, параграф 2.	а) подробно описание на инцидента, включително неговата 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 инцдента, субктът представя междинен доклад, сдържащ, 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, 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) НЕРИКС предоставя на определните за компетентните 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.	
Член 24 ***Използване на европейски схеми за сертифициране на киберсигурността*** 1. За да се докаже съответствие с конкретни изисквания по член 21, държавите членки могат да изискат от съществените и важните субекти да използват конкретни ИКТ продукти, ИКТ услуги и	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** Сертифициране на киберсигурността Чл.24. За да се докаже съответствие с кокончретни изисквания по чл. 22, НКО може да изиска от съществените и важните субекти да използват конкретни, доказано подходящи в оперативно и икономическо отношение ИКТ продукти ИКТ продукти, ИКТ услуги и ИКТ процедури, които са разработени	Пълно съответствие

ИКТ процедури, които са разработени от съществените или важните субекти или са придобити от трети страни, сертифицирани в рамките на европейските схеми за киберсигурност, приети съгласно член 49 от Регламент (ЕС) 2019/881. Освен това държавите членки насърчават съществените и важните субекти да използват квалифицирани удостоверителни услуги. 2. В съответствие с член 38 Комисията е оправомощена да приема делегирани актове за допълване на настоящата директива, като определя за кои категории съществени и важни субекти се изисква да ползват определени сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси или да получат сертификат съгласно конкретна европейска схема за сертифициране на киберсигурността, приета в съответствие с член 49 от Регламент (ЕС) 2019/881. Тези делегирани актове се приемат, когато са установени недостатъчни нива на киберсигурност, и те предвиждат срок за изпълнение. Преди да приеме такива делегирани актове, Комисията извършва оценка на въздействието и провежда консултации в съответствие с член 56 от Регламент (ЕС) 2019/881. 3. В случаите, при които не е налична подходяща европейска схема за сертифициране на киберсигурността за целите на параграф 2 от настоящия член, след консултация с групата за сътрудничество и Европейската група за сертифициране на киберсигурността Комисията може да изиска от ENISA да изготви схема за сертифициране съгласно член 48, параграф 2 от Регламент (ЕС) 2019/881.	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) 2010/881“). Националният компетентен орган насърчава съществените и важните субекти да използват квалифицирани удостоверителни услуги.	

Член 25 ***Стандартизация*** 1. С цел насърчаване на еднообразното прилагане на член 21, параграфи 1 и 2 държавите членки, без да налагат употребата на определен тип технология или да упражняват дискриминация в нейна полза, насърчават използването на европейски и международни стандарти и технически спецификации от значение за сигурността на мрежовите и информационните системи. 2. В сътрудничество с държавите членки и след като се консултира със съответните заинтересовани страни, когато това е целесъобразно, ENISA изготвя препоръки и насоки по отношение на техническите области, които да се вземат под внимание във връзка с параграф 1, както и по отношение на вече съществуващите стандарти, включително националните стандарти, което да позволи обхващането на тези области.	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Стандартизация** **Чл.25** 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	Пълно съответствие
ГЛАВА V **ЮРИСДИКЦИЯ И РЕГИСТРАЦИЯ** Член 26 *Юрисдикция и териториалност* 1. Субектите, попадащи в обхвата на настоящата директива, се считат за попадащи под юрисдикцията на държавата членка, в която са установени, освен в случай на: а) доставчици на обществени електронни съобщителни мрежи или доставчици на обществено достъпни електронни съобщителни услуги, за които се	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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	Пълно съответствие

счита, че попадат под юрисдикцията на държавата членка, в която предоставят своите услуги; б) 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 параграф 2; в) органи на публичната администрация, за които се счита, че попадат под юрисдикцията на държавата членка, която ги е създала. 2. За целите на настоящата директива се счита, че основното място на установяване в Съюза на субектите, посочени в параграф 1, буква б), 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. 3. Ако субект по параграф 1, буква б) не е установен в Съюза, но предлага услуги в него, той посочва представител в Съюза. Представителят	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) При получаване на искане за взаимопомощ по отношение на субект, посочен в чл.27а, ал.1, т. 2, националните компетентни органи могат, да предприемат подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или който притежава мрежова и информационна система на тяхна територия.	

трябва да е установен в една от държавите членки, в които се предлагат услугите. Счита се, че този субект е под юрисдикцията на държавата членка, в която е установен представителят. При липсата на представител в Съюза, определен съгласно настоящия член, всяка държава членка, в която субектът предоставя услуги, може да предприеме правни действия срещу него за нарушение на настоящата директива. 4. Определянето на представител от страна на субект по параграф 1, буква б) не засяга правните действия, които биха могли да се предприемат срещу самия субект. 5. Държавите членки, които са получили искане за взаимопомощ по отношение на субект, посочен в параграф 1, буква б), 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.		
Член 27 **Регистър на субектите** 1. ENISA създава и поддържа регистър на 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, въз основа на информацията,	**Закон за киберсигурност** **Регистър** **Чл. 6.** (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на електронното управление създава, води и поддържа регистър на съществените услуги по смисъла на този закон, който съдържа: 1. видове съществени услуги; 2. списък на операторите на съществени услуги и предоставяните от тях услуги; 3. сфера на дейност; 4. брой потребители, разчитащи на услугата, предоставяна от оператора; 5. географски обхват на областта, която може да бъде засегната от даден инцидент. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Списъкът по ал. 1, т. 2 се преразглежда и актуализира на всеки две години	Пълно съответствие

получена от единните звена за контакт в съответствие с параграф 4. При поискване ENISA дава възможност за достъп на компетентните органи до регистъра, като същевременно осигурява защитата на поверителността на информацията, когато е приложимо. 2. До 17 януари 2025 г. държавите членки изискват от субектите, посочени в параграф 1, да представят на компетентните органи следната информация: а) наименованието на субекта; б) съответния сектор, подсектор и вид субект, както е посочено в приложение I или II, когато е приложимо; в) адреса на основното място на установяване и на останалите законови места на установяване на субекта в Съюза или, при липсата на място на установяване в Съюза, на неговия представител, определен съгласно член 26, параграф 3; г) актуални данни за контакт, включително адреси на електронна поща и телефонни номера на субекта и, когато е приложимо, на неговия представител, определен съгласно член 26, параграф 3; д) държавите членки, в които субектът предоставя услуги; както и е) IP обхватите на субекта. 3. Държавите членки гарантират, че субектите по параграф 1 уведомяват компетентния орган без забавяне за всякакви промени в изпратената от тях информация съгласно параграф 2, и при всички положения в рамките на три месеца от датата на промяната. 4. След получаването на информацията, посочена в параграфи 2 и 3, с изключение на информацията, посочена в параграф 2, буква е), единното звено за контакт на съответната държава членка препраща тази информация на ENISA без ненужно забавяне след получаването и.	от съответните административни органи по чл. 16, ал. 1, за което те уведомяват министъра на електронното управление. (3) Редът за водене, съхраняване и достъп до регистъра се определя с наредбата по чл. 3, ал. 2. (4) Регистърът по ал. 1 не е публичен. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** Регистър Чл. 6. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министърът на електронното управление създава, води и поддържа регистър на субектите по чл. 4 и чл. 4а, който съдържа следната информация: а) наименованието на субекта; б) адрес и актуални данни за контакт, включително адреси на електронната поща и телефонни номера; в) IP обхвати; г) когато е приложимо, съответния сектор, подсектор и вид субект, както е посочено в приложение I или II; д) когато е приложимо, списък на държавите членки, в които те предоставят услуги, попадащи в обхвата на този закон; е) когато е приложимо, данни за контакт на представителя, определен съгласно чл. 24, 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	

5. Когато е приложимо, информацията, посочена в параграфи 2 и 3 от настоящия член, се представя чрез националния механизъм, посочен в член 3, параграф 4, алинея четвърта.	представител, определен съгласно член 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 определят с наредбата по чл. 3, ал. 2. (5) Регистърът по ал.1 не е публичен.	
Член 28 **База данни с регистрационни данни на имена на домейни** 1. С цел допринасяне за сигурността, стабилността и устойчивостта на системата за имена на домейни държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на такива имена на домейни, надлежно да събират и поддържат точни и пълни данни за регистрацията на имената на домейни в специално предназначена база данни в съответствие с правото на Съюза в областта на защитата на данните по отношение на личните данни. 2. За целите на параграф 1 държавите членки изискват базата данни за съхранение на данните за регистрация на имена на домейни да съдържа необходимата информация 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. Тази информация включва: а) името на домейна; б) датата на регистрация;	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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.	Пълно съответствие

в) името, адреса на електронната поща и телефонния номер за контакт на регистранта; г) 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. Държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да имат установени политики и процедури, включително процедури за проверка, за да осигурят, че базите данни по параграф 1 включват точна и пълна информация. Държавите членки изискват тези политики и процедури да бъдат публично достъпни. 4. Държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да правят публично достояние, без излишно забавяне след регистрацията на име на домейн, данните за нея, които не са лични. 5. Държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да предоставят достъп до конкретни данни за регистрация на имена на домейни при законосъобразни и надлежно обосновани искания от законно търсещите достъп, в съответствие с правото на Съюза в областта на защитата на данните. Държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да отговарят без излишно забавяне и при всички случаи в срок от 72 часа след получаването на всякакви искания за достъп. Държавите членки изискват	(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.	

политиките и процедурите относно оповестяването на такива данни да бъдат публично достъпни. 6. Спазването на задълженията, предвидени в параграфи 1 — 5, не води до дублиране на събирането на данни за регистрация на имена на домейни. За тази цел държавите членки изискват регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да си сътрудничат помежду си.		
ГЛАВА VI **ОБМЕН НА ИНФОРМАЦИЯ** **Член 29** Споразумения за обмен на информация в областта на киберсигурността 1. Държавите членки гарантират, че субектите, попадащи в обхвата на настоящата директива, и когато е относимо, други субекти, които не попадат в обхвата на настоящата директива, могат да обменят на доброволна основа помежду си 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:	**Закон за киберсигурност** ***Сътрудничество и координация*** **Чл. 20. (1)** Координацията и ръководството на стратегическо ниво се осъществява от Съвета по киберсигурността във взаимодействие със Съвета по сигурността към Министерския съвет. Националният координатор по киберсигурността осигурява връзката между стратегическото ръководство и системата за координация на оперативно ниво. (2) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Министерството на електронното управление координира дейностите по изграждане на Националната координационно-организационна мрежа за киберсигурност и на Националния киберситуационен център в сътрудничество с Държавна агенция "Национална сигурност", Министерството на вътрешните работи и Министерството на отбраната. (3) За координация и обмен на информация при възникване на инцидент или при извършване на компютърно престъпление на междуведомствено ниво се създават звена за контакт с цел осведоменост на компетентните по случая институции и изготвянето на общ отговор. Процедурите и правилата за това сътрудничество се определят със споразумение за взаимодействие между заинтересованите ведомства. (4) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) За координиране на дейностите за реакция при кибератаки и мащабни инциденти министърът на електронното управление може да създава междуведомствени оперативни групи с	Пълно съответствие

а) има за цел предотвратяване, откриване, реагиране или възстановяване от инциденти или смекчаване на тяхното въздействие; б) 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. Държавите членки гарантират, че 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. Държавите членки улесняват създаването на споразумения за обмен на информация в областта на киберсигурността, посочени в параграф 2 от настоящия член. 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 публичните органи в такива споразумения, държавите членки могат да налагат условия по отношение на информацията, предоставяна от компетентните органи или ЕРИКС.	участието на ведомства, организации и институции, включително от частния сектор, имащи отношение към тези дейности. (5) Сътрудничеството на международно ниво се осъществява чрез Групата за сътрудничество, а координацията и сътрудничеството между екипите за реагиране при инциденти с компютърната сигурност – в Мрежата на националните екипи за реагиране при инциденти с компютърната сигурност. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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	

Държавите членки предлагат помощ за прилагането на такива споразумения в съответствие със своите политики, посочени в член 7, параграф 2, буква з). 4. Държавите членки гарантират, че съществените и важните субекти уведомяват компетентните органи за своето участие в споразуменията за обмен на информация в областта на киберсигурността по параграф 2 при присъединяването им към такива споразумения или, когато е приложимо, за оттеглянето им от тях, след като то влезе в сила. 5. ENISA предоставя помощ за установяването на споразуменията за обмен на информация в областта на киберсигурността по параграф 2, като обменя най-добри практики и предоставя насоки.	на набор от отбранителни способности, отстраняване и оповестяване на уязвимости, техники за откриване, ограничаване и предотвратяване на заплахи, стратегии за ограничаване или етапи за реакция или възстановяване или насърчаване на съвместни научни изследвания относно киберзаплахите между публични и частни субекти. (2) Обменът на информация се осъществява в рамките на общности на съществените и важните субекти, и когато е относимо, на техните снабдители или доставчици на услуги. Този обмен се осъществява чрез споразумения за обмен на информация в областта на киберсигурността с оглед на потенциално чувствителния характер на споделяната информация. (3) Националните компетентни органи улесняват създаването на споразумения за обмен на информация в областта на киберсигурността, посочени в ал.2. Тези споразумения може да уточняват оперативните елементи, включително използването на специално предназначени ИКТ платформи и инструменти за автоматизиране, съдържанието и условията по споразуменията за обмен на информация. Когато определят подробностите за участието на административните органи в такива споразумения, Националните компетентни органи могат да налагат условия по отношение на информацията, предоставяна от компетентните органи или ЕРИКС. Националните компетентни органи оказват помощ при прилагането на такива споразумения в съответствие с политиките, посочени в чл. 8, ал. 2, т. 8. (4) Съществените и важните субекти уведомяват националните компетентни органи за своето участие в споразуменията за обмен на информация в областта на киберсигурността по ал. 2 при присъединяването в такива споразумения или при прекратяването им.	
Член 30 ***Доброволно уведомяване за относима информация*** 1. Държавите членки гарантират, че в допълнение към задължението за уведомяване,	**Закон за киберсигурност** **Уведомяване за инциденти от субекти извън посочените по чл. 4, ал. 1**	Пълно съответствие

предвидено в член 23, уведомления могат да се подават до ЕРИКС или, когато е приложимо, до компетентните органи на доброволна основа от: а) съществени и важни субекти по отношение на инциденти, киберзаплахи и ситуации, близки до инциденти; б) субекти, различни от посочените в буква а), независимо дали попадат в обхвата на настоящата директива, по отношение на значителни инциденти, киберзаплахи и ситуации, близки до инциденти. 2. Държавите членки обработват уведомленията по параграф 1 от настоящия член в съответствие с процедурата, предвидена в член 23. Държавите членки могат да обработват задължителните уведомления с предимство пред доброволните уведомления. Когато е необходимо, ЕРИКС и, когато е приложимо, 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, на които той не би бил предмет, ако не подаде уведомлението.	**Чл. 27. (1)** Субекти извън посочените по чл. 4, ал. 1 може да уведомяват секторните екипи за реагиране при инциденти с компютърната сигурност за инциденти, които имат въздействие върху непрекъснатостта на предоставяните от тях услуги. (2) При обработването на уведомленията секторните екипи за реагиране при инциденти с компютърната сигурност действат съгласно съответните разпоредби на тази глава, като уведомленията на субектите по чл. 4, ал. 1 се обработват с предимство пред уведомленията по ал. 1. (3) Уведомленията по ал. 1 се обработват само когато това не представлява несъразмерна или неоправдана тежест. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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 националните компетентни 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 буква а), независимо дали попадат в обхвата на настоящия закон, по отношение на значителни инциденти, киберзаплахи и ситуации, близки до инциденти. (2) Уведомленията по ал. 1, се обработват в съответствие с процедурата, предвидена в чл. 23. Националните компетентни органи обработват задължителните уведомления с предимство пред доброволните уведомления. (3) При необходимост, ЕРИКС или националналните компетентни 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.	
ГЛАВА VII ***НАДЗОР И ПРАВОПРИЛАГАНЕ*** ***Член 31*** ***Основни аспекти относно надзора и правоприлагането*** 1. Държавите членки гарантират, че техните компетентни органи ефективно осъществяват надзор и предприемат мерки, необходими за осигуряване на спазването на настоящата директива. 2. Държавите членки могат да разрешат на своите компетентни органи да приоритизират надзорните задачи. Това приоритизиране се основава на основан на риска подход. За тази цел при изпълнението на надзорните си задачи, предвидени в членове 32 и 33, компетентните органи могат да установят надзорни методологии, които дават възможност за приоритизиране на тези задачи, следвайки основан на риска подход. 3. Компетентните органи работят в тясно сътрудничество с надзорните органи съгласно Регламент (ЕС) 2016/679 при работа по инцидентите, които водят до нарушаване на сигурността на лични данни, без да се засягат компетенциите и задачите на надзорните органи съгласно посочения регламент.	**Проект на Закон за изменение и допълнение на Закона за киберсигурност** ***ГЛАВА ВТОРА „В“*** ***КОНТРОЛ*** ***Основни аспекти на контрола*** ***Чл.27е. (1***) Контролът за спазване на изискванията по този закон се осъществява от: 1. националните компететнтни 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.	Пълно съответствие

4. Без да се засягат националните законодателни и институционални рамки, държавите членки гарантират, че при надзора на спазването на настоящата директива от органите на публичната администрация и налагането на правоприлагащи мерки при нарушаване на настоящата директива, компетентните органи разполагат с подходящите правомощия да осъществяват подобни задачи с оперативна независимост по отношение на органите на публичната администрация, над които се упражнява надзор. Държавите членки могат да вземат решение за налагането на подходящи, пропорционални и ефективни надзорни и правоприлагащи мерки по отношение на тези субекти в съответствие с националните законодателни и институционални рамки.		
Член 32 **Надзорни и правоприлагащи мерки по отношение на съществените субекти** 1. Държавите членки гарантират, че надзорните и правоприлагащи мерки, наложени на съществените субекти по отношение на определените в настоящата директива задължения, са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата по всеки отделен случай. 2. Държавите членки гарантират, че при упражняването на своите надзорни задачи във връзка със съществените субекти компетентните органи имат правомощия да подлагат тези субекти най-малко на: а) проверки на място или дистанционни проверки, включително случайни, извършвани от обучени специалисти;	**Проект на Закон за изменение и допълнение на Закона за киберсигурност** **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	Пълно съответствие

б) редовни и целеви одити на сигурността, извършвани от независим орган или компетентен орган; в) извънпланови одити, включително когато са обосновани поради значителен инцидент или нарушение на настоящата директива от страна на съществения субект; г) проверки за сигурност, основани на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска, при необходимост със съдействието на съответния субект; д) искания за информация, необходима за оценка на мерките за управление на риска в областта на киберсигурността, приети от съответния субект, включително документирани политики в областта на киберсигурност, както и съответствие със задълженията за изпращане на информация на компетентните органи съгласно член 27; е) искания за достъп до данни, документи и всякаква информация, необходими за осъществяването на техните надзорни задачи; ж) искания за доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.	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 киберсигурността, приети от съответния субект, включително документирани политики в областта на киберсигурност, както и изпълнение на задълженията за изпращане на информация на националните компетентни органи съгласно чл. 27в (Регистъра на ENISA); 6. да им бъде предоставен достъп до данни, документи и всякаква информация, необходими за осъществяването на техните надзорни задачи; 7. изискват и да им бъдат предоставени доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.	
Надзорни и правоприлагащи мерки по отношение на съществените субекти	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 27з. (1**) Целевите одити на сигурността, посочени в чл. 27ж се основават на оценки на риска, извършени от компетентния	Пълно съответствие

Целевите одити на сигурността, посочени в първа алинея, буква б), се основават на оценки на риска, извършени от компетентния орган или одитирания субект, или на друга налична информация, свързана с риска. Резултатите от всеки целеви одит на сигурността се предоставят на компетентния орган. 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.	орган или одитирания субект, или на друга налична информация, свързана с риска. (2) Резултатите от всеки целеви одит на сигурността се предоставят на националните компетентни органи по чл. 16, ал. 1. (3) Разходите за такъв целеви одит на сигурността, извършен от независим орган, се заплащат от одитирания субект, освен в надлежно обосновани случаи, когато националният компетентен орган реши друго.	
3. При упражняване на своите правомощия по параграф 2, буква д), е) или ж) компетентните органи заявяват целта на своето искане и уточняват исканата информация.	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл.27ж. ал 3.** (3) При упражняване на своите правомощия по ал. 1, т.5, 6 и 7, съответно ал. 2, т. 4, 5 и 6, националните компетентни органи заявяват целта на своето искане и поясняват исканата информация.	Пълно съответствие
4. Държавите членки гарантират, че в рамките на своите правомощия по правоприлагане във връзка със съществените субекти техните компетентни органи са упълномощени най-малкото: а) да издават предупреждения при нарушаване на настоящата директива от засегнатите субекти; б) да приемат обвързващи указания, включително относно мерките, необходими за предотвратяване на възникването на инцидент или за справяне с него, както и срокове за изпълнение на такива мерки и задължения за докладване на изпълнението, или разпореждане от засегнатите субекти да поправят установените пропуски или нарушения на настоящата директива;	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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, за изпълнение на 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	Пълно съответствие

в) да разпореждат на засегнатите субекти да преустановяват поведение, което нарушава настоящата директива, и да се въздържат от повтарянето на такова поведение; г) да разпореждат на засегнатите субекти да гарантират, че техните мерки за управление на риска в областта на киберсигурността са в съответствие с член 21(Мерки за управление на риска), или да изпълнят задълженията за докладване по член 23 по конкретизиран начин и в рамките на посочен срок; д) да разпореждат на засегнатите субекти да уведомяват физическите или юридическите лица, на които предоставят услуги или с оглед на които извършват дейности, потенциално засегнати от значителна киберзаплаха, за естеството на заплахата, както и за възможните защитни или коригиращи мерки, които могат да бъдат предприети от тези физически или юридически лица в отговор на тази заплаха; е) да разпореждат на засегнатите субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността, в рамките на разумен срок; ж) да определят длъжностно лице по надзор с ясно определени задачи за определен срок, което да следи за спазването на членове 21 и 23 от засегнатите субекти; з) да разпореждат на засегнатите субекти да обявяват публично аспектите на нарушенията на настоящата директива, по конкретен начин;	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 определят длъжностно лице по надзор за спазването на чл. 22 и чл. 23 от засегнатите субекти, както и на неговите конкретни задачи и срок за изпълнение .	

и) да налагат или изискват налагането от съответните органи, съдилища или трибунали съгласно националното право на административна глоба по член 34 в допълнение към която и да е от мерките по букви а) — з) от настоящия параграф. 5. Когато правоприлагащите мерки, приети съгласно параграф 4, букви а) — г) и е), са неефективни, държавите членки гарантират, че компетентните им органи разполагат с правомощие да определят срок, до който от съществения субект се изисква да предприеме необходимото действие за отстраняване на недостатъците или за привеждане в съответствие с изискванията на тези органи. Ако изисканото действие не се предприеме в определения срок, държавите членки гарантират, че компетентните им органи разполагат с правомощия: а) да спрат временно или да изискат от сертифициращ или разрешаващ орган, от съдилище или от трибунал, в съответствие с националното право, да спре временно сертификат или разрешение относно всички или част от съответните предоставени услуги или дейностите, извършвани от съществения субект; б) да изискат от съответните органи, съдилища или трибунали налагането съгласно националното право на временна забрана спрямо всяко физическо лице, изпълняващо управленски функции на равнището на главно изпълнително длъжностно лице или законен представител в този съществен субект, да упражнява управленски функции в този субект. Временни спирания или забрани, наложени съгласно настоящия параграф, се прилагат само докато съответният субект предприеме необходимото действие за отстраняване на недостатъците или за изпълнение на изискванията на компетентния орган, за които са приложени такива правоприлагащи мерки. Налагането на такива временни спирания или забрани подлежи на подходящи процедурни гаранции в	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 27к (1)** За непредприемане на действията определени по реда на чл. 27и, ал. 1, т. 1-4 и т. 6, националният компетентен 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. 27и, ал. 1, т. 1-4 и т. 6 , националният компетентен орган по чл. 27е, може да изиска от съд или от друг държавен орган налагането на временна забрана спрямо всяко физическо лице, изпълняващо управленски функции или законен представител в този съществен субект, да упражнява управленски функции в този субект. (3) Компетентният административен орган за временно спиране на лиценз, регистрация, сертификат или разрешение по ал. 1 се произнася с индивидуален административен акт, който може да бъде обжалван по реда на Административнопроцесуалния кодекс. (4) 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 в този закон. Тези физически лица могат да бъдат подведени под отговорност за неизпълнението на своите задължения по спазването на закона.	Пълно съответствие

съответствие с общите принципи на правото на Съюза и Хартата, включително правото на ефективни правни средства за защита и на справедлив съдебен процес, презумпцията за невиновност и правото на защита. Правоприлагащите мерки, предвидени в настоящия параграф, не се прилагат за органи на публичната администрация, които са предмет на настоящата директива.		
6. Държавите членки гарантират, че всяко физическо лице, отговорно за съществен 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 настоящата директива, от страна на този субект. Държавите членки гарантират, че е възможно тези физически лица да бъдат подвеждани под отговорност за неизпълнението на своите задължения да осигурят спазването на настоящата директива. Що се отнася до органите на публичната администрация, настоящият параграф не засяга националното право по отношение на отговорността на държавните служители и на избраните или назначените длъжностни лица.	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 27к** (5) Всяко физическо лице, отговорно за съществен или важен субект или действащо като негов законен представител въз основа на правомощие да го представлява, да взема решения от негово име или да упражнява контрол върху него, има необходимите правомощия, за да осигури спазването на закона. За тези лица се прилагат всички мерки, предвидени в този закон. Тези физически лица могат да бъдат подведени под отговорност за неизпълнението на своите задължения по спазването на закона.	Пълно съответствие
7. Когато предприемат правоприлагащите мерки, посочени в параграф 4 или 5, компетентните органи се съобразяват с правата на защита и отчитат обстоятелствата по всеки отделен случай и, като минимум, вземат предвид: а) сериозността на нарушението и значимостта на нарушените разпоредби, като се има предвид, че за тежко нарушение се считат във всички случаи наред с другото: i) повторни нарушения; ii) неуведомяване или несправяне със значителни инциденти; iii) неотстраняване на недостатъци съгласно обвързващи указания от компетентните органи;	**От Административнопроцесуален кодекс** В сила от 12.07.2006 г.,изм. ДВ. бр.102 от 8 Декември 2023г. **Съразмерност** **Чл. 6.** (1) Административните органи упражняват правомощията си по разумен начин, добросъвестно и справедливо. (2) Административният акт и неговото изпълнение не могат да засягат права и законни интереси в по-голяма степен от най-необходимото за целта, за която актът се издава. (3) Когато с административния акт се засягат права или се създават задължения за граждани или за организации, прилагат се онези мерки, които са по-благоприятни за тях, ако и по този начин се постига целта на закона.	Пълно съответствие

iv) възпрепятстване на одити или дейности по мониторинг от компетентния орган след констатация на нарушение; v) предоставяне на невярна или грубо неточна информация във връзка с мерките за управление на риска в областта на киберсигурността или задълженията за докладване по членове 21 и 23; б) продължителността на нарушението; в) всички относими предишни нарушения от страна на съответния субект; г) всички причинени материални или нематериални вреда, включително финансови или икономически загуби, въздействия върху други услуги и броят на засегнатите потребители; д) умисъл или небрежност от страна на извършителя на нарушението; е) всички предприети от субекта мерки за предотвратяване или ограничаване на материалните или нематериалните вреди; ж) всяко придържане към одобрени кодекси на поведение или одобрени механизми за сертифициране; з) равнището на съдействие, което отговорните физически или юридически лица оказват на компетентния орган;	(4) От две или повече законосъобразни възможности органът е длъжен при спазване на ал. 1, 2 и 3 да избере тази възможност, която е осъществима най-икономично и е най-благоприятна за държавата и обществото. (5) Административните органи трябва да се въздържат от актове и действия, които могат да причинят вреди, явно несъизмерими с преследваната цел. Истинност **Чл. 7. (1)** Административните актове се основават на действителните факти от значение за случая. (2) На преценка подлежат всички факти и доводи от значение за случая. (3) Истината за фактите се установява по реда и със средствата, предвидени в този кодекс. Определяне на административните наказания **От Закон за административните нарушения и наказания** Отразена деноминацията от 05.07.1999 г. **Чл. 27. (1)** Административното наказание се определя съобразно с разпоредбите на този закон в границите на наказанието, предвидено за извършеното нарушение. (2) При определяне на наказанието се вземат предвид тежестта на нарушението, подбудите за неговото извършване и другите смекчаващи и отегчаващи вината обстоятелства, както и имотното състояние на нарушителя. (3) Смекчаващите обстоятелства обуславят налагането на по-леко наказание, а отегчаващите - на по-тежко наказание. (4) Заменяването на предвидените за нарушенията наказания с по-леки по вид не се допуска освен в случаите, предвидени в чл. 15, алинея 2. (5) (Доп. - ДВ, бр. 109 от 2020 г., в сила от 23.12.2021 г.) Не се допуска също така определяне на наказание под предвидения най-нисък размер на наказанията глоба и временно лишаване от право да се упражнява определена професия или дейност, освен в предвидените в закон случаи.	
8. Компетентните органи излагат подробни мотиви за своите правоприлагащи мерки. Преди да	От Административнопроцесуален кодекс В сила от 12.07.2006 г.,изм. ДВ. бр.102 от 8 Декември 2023г.	Пълно съответствие

приемат такива мерки, компетентните органи уведомяват засегнатите субекти за предварителните си констатации. Те също така предоставят разумен срок на тези субекти да представят забележки, освен в надлежно обосновани случаи, когато това би възпрепятствало незабавните действия за предотвратяване или реагиране на инциденти.	Форма на индивидуалния административен акт Чл. 59. (1) Административният орган издава или отказва издаване на акта с мотивирано решение. Произнасяне на компетентния орган Чл. 97. (1) (Доп. - ДВ, бр. 77 от 2018 г., в сила от 01.01.2019 г.) В двуседмичен срок от получаване на преписката, когато е едноличен, и в едномесечен срок, когато е колективен, компетентният да разгледа жалбата или протеста орган се произнася с мотивирано решение, с което обявява оспорения акт за нищожен, отменя го изцяло или отчасти като незаконосъобразен или нецелесъобразен или отхвърля жалбата или протеста. Когато органът отхвърли жалбата или протеста, мотивите за това решение се смятат за част от мотивите на административния акт. Компетентният орган е длъжен незабавно да уведоми жалбоподателя за датата на получаване на преписката.	
9. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива информират съответните компетентни органи в същата държава членка съгласно Директива (ЕС) 2022/2557, когато упражняват своите надзорни и правоприлагащи правомощия, имащи за цел да гарантират спазването на настоящата директива от 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 съгласно настоящата директива да упражняват своите надзорни и правоприлагащи правомощия във връзка със субект, който е установен като критичен субект съгласно Директива (ЕС) 2022/2557. 10. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива си сътрудничат със съответните компетентни органи на засегнатата държава членка съгласно Регламент(ЕС) 2022/2554. По-специално, държавите	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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, националните компетентни 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,	Пълно съответствие

членки гарантират, че техните компетентни органи съгласно настоящата директива 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 настоящата директива от страна на съществен 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.	който е определен като трета страна критичен доставчик на услуги в областта на ИКТ, в съответствие с член 31 от Регламент (ЕС) 2022/2554.	
Член 33 **Надзорни и правоприлагащи мерки по отношение на важните субекти** 1. Когато разполагат с доказателства, индикации или информация, че важен субект вероятно не изпълнява настоящата директива, и по-специално членове 21 и 23 от нея, държавите членки гарантират, че компетентните органи предприемат действия, при необходимост, посредством последващи надзорни мерки. Държавите членки гарантират, че тези мерки са ефективни, пропорционални и възпиращи, като вземат предвид обстоятелствата във всеки отделен случай. 2. Държавите членки гарантират, че при упражняването на своите надзорни задачи във връзка със важните субекти компетентните органи имат правомощия да подлагат тези субекти най-малко на: а) проверки на място и последващ дистанционен надзор, извършвани от обучени специалисти; б) целеви одити на сигурността, извършвани от независим орган или компетентен орган; в) проверки за сигурност, основани на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска, при необходимост със съдействието на съответния субект;	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл.27ж.** (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 за 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 член 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, националните компетентни органи заявяват целта на своето искане и поясняват исканата информация.	Пълно съответствие

г) искания за 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 член 27; д) искания за достъп до данни, документи и информация, необходими за изпълнението на надзорните им задачи; е) искания за доказателства за изпълнението на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства. Целевите одити на сигурността, посочени в първа алинея, буква б), се основават на оценки на риска, извършени от компетентния орган или одитирания субект, или на друга налична информация, свързана с риска. Резултатите от всеки целеви одит на сигурността се предоставят на компетентния орган. 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.		
3. При упражняване на своите правомощия по параграф 2, буква г), д) или е) компетентните органи заявяват целта на своето искане и поясняват исканата информация. 5. Член 32, параграфи 6, 7 и 8 се прилагат mutatis mutandis за надзорните и правоприлагащи мерки, предвидени в настоящия член за важните субекти.	От От Административнопроцесуален кодекс В сила от 12.07.2006 г.,изм. ДВ. бр.102 от 8 Декември 2023г. Съразмерност Чл. 6. (1) Административните органи упражняват правомощията си по разумен начин, добросъвестно и справедливо.	Пълно съответствие

	(2) Административният акт и неговото изпълнение не могат да засягат права и законни интереси в по-голяма степен от най-необходимото за целта, за която актът се издава. (3) Когато с административния акт се засягат права или се създават задължения за граждани или за организации, прилагат се онези мерки, които са по-благоприятни за тях, ако и по този начин се постига целта на закона.	
4. Държавите членки гарантират, че при упражняване на своите правомощия по правоприлагане във връзка със важните субекти компетентните органи са оправомощени най-малкото: а) да издават предупреждения при нарушение на настоящата директива от засегнатите субекти; б) да приемат обвързващи указания или разпореждане, с които се изисква от засегнатите субекти да поправят установените пропуски или нарушението на настоящата директива; в) да разпореждат на засегнатите субекти да преустановяват поведение, което нарушава настоящата директива, и да се въздържат от повтарянето на такова поведение; г) да разпореждат на засегнатите субекти да гарантират, че техните мерки за управление на риска в областта на киберсигурността са в съответствие с член 21, или да изпълнят задълженията за докладване по член 23 по конкретизиран начин и в рамките на определен срок; д) да разпореждат на засегнатите субекти да уведомяват физическите или юридическите лица, на които предоставят услуги или с оглед на които извършват дейности, потенциално засегнати от значителна киберзаплаха, за естеството на заплахата, както и за възможните защитни или коригиращи мерки, които могат да бъдат предприети от тези	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **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, за изпълнение на 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;	Пълно съответствие

физически или юридически лица в отговор на тази заплаха; е) да разпореждат на засегнатите субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността, в рамките на разумен срок; ж) да разпореждат на засегнатите субекти да обявяват публично аспектите на нарушението на настоящата директива, по конкретен начин; з) да налагат или изискват налагането от засегнатите органи, съдилища или трибунали в съответствие с националното право на административна глоба по член 34 в допълнение към която и да е от мерките по букви а) — ж) от настоящия параграф.	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 определят длъжностно лице по надзор за спазването на чл. 22 и чл. 23 от засегнатите субекти, както и на неговите конкретни задачи и срок за изпълнение .	
6. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива си сътрудничат със съответните компетентни органи на засегнатата държава членка съгласно Регламент (ЕС) 2022/2554. По-специално, държавите членки гарантират, че техните компетентни органи съгласно настоящата директива 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 настоящата директива от страна на 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.	**Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Чл. 27м. (1)** 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.	Пълно съответствие
Член 34 **Общи условия за налагане на административни глоби на съществените и важните субекти**	Закон за киберсигурност Глава трета АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ Отговорност за нарушения, свързани с уведомяване за инциденти	Пълно съответствие

1. Държавите членки гарантират, че наложените административни глоби на съществените и важните субекти съгласно настоящия член във връзка с нарушения на настоящата директива, са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата във всеки конкретен случай.	Чл. 28. (1) Административен орган, който не уведоми или уведоми след срока по чл. 21, ал. 4 секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на неговата дейност, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление, се наказва с глоба от 1000 до 10 000 лв. (2) При повторно нарушение по ал. 1 наказанието е глоба от 2000 до 20 000 лв. (3) На лице или организация по чл. 4, ал. 1, т. 3 и 4, която не уведоми или уведоми след срока по чл. 21, ал. 4 секторния екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от тях административни услуги по електронен път, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв. (4) При повторно нарушение по ал. 3 глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв. (5) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на оператор на съществени услуги, който не уведоми или уведоми след срока по чл. 21, ал. 4 съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има въздействие върху непрекъснатостта на предоставяните от него съществени услуги, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление. (6) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на доставчик на цифрови услуги, който не уведоми или уведоми след срока по чл. 21, ал. 4 съответния секторен екип за реагиране при инциденти с компютърната сигурност за всеки инцидент, който има съществено въздействие върху непрекъснатостта на предоставяните от него цифрови услуги, както и когато уведомлението не съдържа достатъчно информация по чл. 21, ал. 4, изречение второ, в случай че деянието не съставлява престъпление.	

	Отговорност за непредоставяне на информация или неизпълнение на указания Чл. 29. (1) Административен орган, който не предостави информацията и доказателствата по чл. 16, ал. 5 или не изпълни задължителни указания по чл. 16, ал. 7, се наказва с глоба от 1000 до 10 000 лв. (2) При повторно нарушение по ал. 1 наказанието е глоба от 2000 до 20 000 лв. (3) Когато деянието по ал. 1 е извършено от оператор на съществени услуги, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв. (4) При повторно нарушение по ал. 3 глобата е от 2000 до 20 000 лв., а имуществената санкция е от 5000 до 25 000 лв. (5) Глобите и имуществените санкции по ал. 3 и 4 се налагат и на доставчик на цифрови услуги, който не предостави информацията по чл. 16, ал. 8, т. 1 или не отстрани пропуск по чл. 16, ал. 8, т. 2. Отговорност за други нарушения Чл. 30. (1) Длъжностно лице, което извърши или допусне извършването на друго нарушение по глава втора, се наказва с глоба от 1000 до 10 000 лв., освен ако деянието не съставлява престъпление. (2) При повторно нарушение по ал. 1 наказанието е глоба от 1500 до 15 000 лв. (3) На лице, което не изпълни задължение по чл. 14, ал. 5, чл. 15, ал. 6 и чл. 19, ал. 3, се налага глоба от 1000 до 10 000 лв. или имуществена санкция от 1500 до 15 000 лв. Установяване на нарушенията, издаване, обжалване и изпълнение на наказателните постановления Чл. 31. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Актовете за установяване на нарушения по този закон, извършени от административни органи, както и за нарушения по чл. 28, ал. 3 и 4 и по чл. 30, ал. 3 във връзка с чл. 19, ал. 3, се съставят от длъжностни лица, определени от министъра на електронното управление. (2) Актовете за установяване на нарушения по този закон, извършени от оператори на съществени услуги или от доставчици на цифрови услуги, се съставят от длъжностни лица,	

	определени от ръководителите на административните органи по чл. 16, ал. 1. (3) Актовете за установяване на нарушения по чл. 30, ал. 3 във връзка с чл. 14, ал. 5 се съставят от длъжностни лица, определени от министъра на вътрешните работи. (4) Актовете за установяване на нарушения по чл. 30, ал. 3 във връзка с чл. 15, ал. 6 се съставят от длъжностни лица, определени от председателя на Държавна агенция "Национална сигурност". (5) Наказателните постановления се издават от: 1. (изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) министъра на електронното управление или от изрично оправомощени от него длъжностни лица – в случаите по ал. 1; 2. ръководителите на административните органи по чл. 16, ал. 1 или от изрично оправомощени от тях длъжностни лица – в случаите по ал. 2; 3. министъра на вътрешните работи или от изрично оправомощени от него длъжностни лица – в случаите по ал. 3; 4. председателя на Държавна агенция "Национална сигурност" или от изрично оправомощени от него длъжностни лица – в случаите по ал. 4. (6) Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на закона за административните нарушения и наказания. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Отговорност за неизпълнение на принудителни административни мерки** Чл. 28. (1) Съществен или важен субект, който не изпълни принудителна административна мярка по смисъла на чл. 27и, ал. 1, т. 2 – т. 7, се наказва с глоба или имуществена санкция в размер от 5 000 до 25 000 лв. (2) При повторно нарушение по ал. 1 наказанието е глоба или имуществена санкция в размер от 10 000 до 50 000 лв. **Глоби и имуществени санкции**	

	Чл. 29. (1) Глобите и имуществените санкции се налагат независимо от която и да е от мерките, посочени в чл. 27и, ал. 1, т. 2-7и чл. 27к. (2) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 50 000 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. (3) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 25 000 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. (4) При нарушение на чл. 21, ръководителите на административните органи, управителите или членовете на управителните органи на съществените и важните субекти подлежат на глоба в размер на 1000 лв. до 10 000 лв.“ (5) Алинея 2 не се прилага по отношение на съществени субекти, които са административни органи.“	
Член **Общи условия за налагане на административни глоби на съществените и важните субекти** 1. Държавите членки гарантират, че наложените административни глоби на съществените и важните субекти съгласно настоящия член във връзка с нарушения на настоящата директива, са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата във всеки конкретен случай.		Пълно съответствие
2. Административни глоби се налагат в допълнение към която и да е от мерките, посочени в член 32, параграф 4, букви а) — з), член 32, параграф 5 и член 33, параграф 4, букви а) — ж).	**Проект на Закон за изменение и допълнение на Закона за киберсигурност** Глоби и имуществени санкции Чл. 29. (1) Глобите и имуществените санкции се налагат независимо от която и да е от мерките, посочени в чл. 27и, ал. 1, т. 2-7и чл. 27к.	Пълно съответствие

3. Когато се взема решение дали да бъде наложена административна глоба и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат най-малко елементите, предвидени в член 32, параграф 7.	От ЗАКОН ЗА АДМИНИСТРАТИВНИТЕ НАРУШЕНИЯ И НАКАЗАНИЯ доп. ДВ. бр.106 от 22 Декември 2023г., доп. ДВ. бр.39 от 1 Май 2024г.	Пълно съответствие
4. Държавите членки гарантират, че когато нарушават член 21 или член 23, съществените субекти, в съответствие с параграфи 2 и 3 от настоящия член, подлежат на административни глоби в максимален размер от най-малко 10 000 000 EUR или най-малко 2 % — която от сумите е по-голяма — от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения субект. 5. Държавите членки гарантират, че когато нарушават член 21 или член 23, важните субекти, в съответствие с параграфи 2 и 3 от настоящия член, подлежат на административни глоби в максимален размер от най-малко 7 000 000 EUR или най-малко 1,4 % — която от сумите е по-голяма — от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи важният субект.	**Проект на Закон за изменение и допълнение на Закона за киберсигурност** **Имуществени санкции** **Чл. 29.** ((2) Съществен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 50 000 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. (3) Важен субект, който не изпълни задълженията по чл. 22 и чл. 24 се наказва с имуществена санкция от 25 000 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. (4) При нарушение на чл. 21, ръководителите на административните органи, управителите или членовете на управителните органи на съществените и важните субекти подлежат на глоба в размер на 1000 лв. до 10 000 лв.“	Пълно съответствие
6. Държавите членки може да предвидят правомощие за налагане на периодични наказателни плащания с цел принуждаване на съществен или важен субект да преустанови нарушение на настоящата директива в съответствие с предходно решение на компетентния орган.		

7. Без да се засягат правомощията на компетентните органи по членове 32 и 33, всяка държава членка може да установи правилата за това дали и в каква степен административните глоби могат да бъдат налагани на органи на публичната администрация.		
8. Когато в правната система на държава членка не са предвидени административни наказания „глоба“, въпросната държава членка гарантира, че настоящият член се прилага по такъв начин, че глобата се инициира от компетентния орган и се налага от компетентните национални съдилища или трибунали, като в същото време се гарантира, че тези правни средства за защита са ефективни и имат ефект, равностоен на административните наказания „глоба“, налагани от компетентните органи. Във всички случаи наложените глоби са ефективни, пропорционални и възпиращи. Държавата членка уведомява Комисията за разпоредбите в правото си, които тя приема съгласно настоящия параграф, до 17 октомври 2024 г., и я уведомява незабавно за всеки последващ закон за изменение или за всяко изменение, които ги засягат.		Не подлежи на транспониране
Член 35 **Нарушения, водещи до нарушаване на сигурността на лични данни** 1. Когато в хода на надзора или правоприлагането компетентните органи разберат, че нарушението на задълженията по членове 21 и 23 от настоящата директива от страна на съществен или важен субект може да доведе до нарушаване на сигурността на лични данни съгласно определеното в член 4, параграф 12 от Регламент (ЕС) 2016/679, за което трябва да се изпрати уведомление съгласно член 33 от посочения регламент, те без ненужно забавяне уведомяват надзорните органи, посочени в член 55 или 56 от същия регламент.	**Закон за киберсигурност** **Чл. 17. (1) (Изм. – ДВ, бр. 15 от 2022 г., в сила от 22.02.2022 г.) Към Министерството на електронното управление се създава Национално единно звено за контакт** (9) В случай на необходимост националните компетентни органи и Националното единно звено за контакт осъществяват сътрудничество със съответните правоприлагащи органи и с Комисията за защита на личните данни. **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **Нарушения в сигурността на личните данни** **Чл. 27н (1)** Националните компетентни органи 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	Пълно съответствие

2. Когато надзорните органи, посочени в член 55 или 56 от Регламент (ЕС) 2016/679, наложат административна глоба съгласно член 58, параграф 2, буква и) от посочения регламент, компетентните органи не налагат административна глоба съгласно член 34 от настоящата директива за нарушение, посочено в параграф 1 от настоящия член, произтичащо от същото деяние, което е било предмет на административната глоба съгласно член 58, параграф 2, буква и) от Регламент (ЕС) 2016/679. Компетентните органи могат обаче да налагат правоприлагащи мерки, предвидени в член 32, параграф 4, букви а) — з), член 32, параграф 5 и член 33, параграф 4, букви а) — ж) от настоящата директива. 3. Когато надзорният орган, компетентен съгласно Регламент (ЕС) 2016/679, е установен в държава членка, различна от тази на компетентния орган, компетентният орган уведомява надзорния орган, установен в собствената му държава членка относно възможното нарушаване на сигурността на данните, посочено в параграф 1.	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.	
Член 36 **Санкции** Държавите членки установяват система от санкции, приложими при нарушение на националните разпоредби, приети в съответствие с настоящата директива, и вземат всички необходими мерки за осигуряване на прилагане им. Предвидените санкции трябва да бъдат ефективни, пропорционални и възпиращи. Най-късно до 17 януари 2025 г. държавите членки нотифицират на Комисията тези разпоредби и мерки и я нотифицират незабавно за всяко последващо изменение, което ги засяга.	**Закон за киберсигурност** **Глава трета** **АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ** **Проект на Закон за изменение и допълнение на Закон за киберсигурност** **ГЛАВА ВТОРА „в“** **КОНТРОЛ** **Основни аспекти на контрола** **ГЛАВА ТРЕТА.** *АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ*	Пълно съответствие

Член 37 **Взаимопомощ** 1. Когато субект предоставя услуги в повече от една държава членка или предоставя услуги в една или повече държави членки и неговите мрежови и информационни системи са разположени в една или повече други държави членки, компетентните органи на засегнатите държави членки си сътрудничат и се подпомагат взаимно, ако е необходимо. Това сътрудничество включва най-малко следното: а) компетентните органи, прилагащи надзорни или правоприлагащи мерки в държава членка, посредством единното звено за контакт, уведомяват и се консултират с компетентните органи в другите засегнати държави членки относно предприетите надзорни и правоприлагащи мерки; б) компетентен орган може да поиска от друг компетентен орган да предприеме надзорни или правоприлагащи мерки; в) когато компетентен орган получи обосновано искане от друг компетентен орган, 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. Взаимопомощта, посочена в алинея първа, буква в), 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	**Проект на Закон за изменение и допълнение на Закона за киберсигурност** **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. националните компетентни 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. национален компетентен орган може да поиска от друг компетентен орган в друга държава членка да предприеме надзорни или правоприлагащи мерки; 3. Когато национален компетентен орган 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. Национален компетентен орган, към когото е отправено искане за помощ, не отхвърля това искане, освен ако не бъде установено, че не е компетентен да предостави исканата помощ, поисканата помощ не е пропорционална на надзорните задачи на националния компетентен орган или искането се отнася до информация или включва дейности, които, ако бъдат оповестени или извършени, биха противоречили на националната сигурност, обществената сигурност или отбраната. Преди да отхвърли такова искане, националният компетентен орган се консултира с другите	Пълно съответствие

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 ENISA. 2. Когато е подходящо и при общо съгласие компетентните органи от различни държави членки може да извършват общи надзорни действия.	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.	
ГЛАВА VIII ***ДЕЛЕГИРАНИ АКТОВЕ И АКТОВЕ ЗА ИЗПЪЛНЕНИЕ*** ***Член 38*** ***Упражняване на делегирането*** 1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия. 2. Правомощието да приема делегирани актове, посочено в член 24, параграф 2, се предоставя на Комисията за срок от пет години, считано от 16 януари 2023 г. 3. Делегирането на правомощия, посочено в член 24, параграф 2, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С		Не се налага транспониране . Нормата се отнася до ЕК

решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в Официален вестник на Европейския съюз или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила. 4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество. 5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета. 6. Делегиран акт, приет съгласно член 24, параграф 2, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на същия акт на Европейския парламент и на Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.		
Член 39 **Процедура на комитет** 1. Комисията се подпомага от комитет. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011. 2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.		Не се налага транспониране . Нормата се отнася до ЕК.

3. Когато становището на комитета трябва да бъде получено по писмена процедура, тази процедура се прекратява без резултат, ако в рамките на срока за даване на становище председателят на комитета вземе такова решение или член на комитета отправи такова искане.		
ГЛАВА IX **ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ** **Член 40** **Преглед** До 17 октомври 2027 г. и на всеки 36 месеца след това, Комисията прави преглед на действието на настоящата директива и докладва на Европейския парламент и на Съвета. В доклада по-специално се прави оценка на относимостта на размера на засегнатите субекти и на секторите, подсекторите и вида на субекта, посочен в приложения I и II, за функционирането на икономиката и обществото във връзка с киберсигурността. За тази цел и с оглед на допълнителното засилване на стратегическото и оперативното сътрудничество Комисията взема предвид докладите на групата за сътрудничество и мрежата на ЕРИКС за натрупания опит на стратегическо и оперативно равнище. Докладът се придружава, ако това е необходимо, от законодателно предложение.		Не се налага транспониране . Нормата се отнася до ЕК.
Член 41 **Транспониране** 1. До 17 октомври 2024 г. държавите членки приемат и публикуват разпоредбите, необходими, за	„§ 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	Частично транспониране

да се съобразят с настоящата директива. Те незабавно информират Комисията за това. Те прилагат тези разпоредби, считано от 18 октомври 2024 г. 2. Когато държавите членки приемат разпоредбите, посочени в параграф 1, в тях се съдържа позоваване на настоящата директива или то се извършва при официалното им публикуване. Условията и редът на позоваване се определят от държавите членки.	(ЕС) 2016/1148 (Директива МИС 2) (ОВ, L 333 от 27 декември 2022 г.).	
Член 42 Изменение на Регламент (ЕС) № 910/2014 В Регламент (ЕС) № 910/2014 член 19 се заличава, считано от 18 октомври 2024 г. ***Член 43*** Изменение на Директива (ЕС) 2018/1972 В Директива (ЕС) 2018/1972 членове 40 и 41 се заличават, считано от 18 октомври 2024 г. ***Член 44*** ***Отмяна*** Директива (ЕС) 2016/1148 се отменя, считано от 18 октомври 2024 г. Позоваванията на отменената директива се считат за позовавания на настоящата директива и се четат съгласно с таблицата на съответствието в приложение ***III.*** ***Член 45*** Влизане в сила Настоящата директива влиза в сила на двадесетия ден след публикуването ѝ в Официален вестник на Европейския съюз.		Не се налага транспониране . Нормата се отнася до ЕК.

Адресати на настоящата директива са държавите членки. Съставено в Страсбург на 14 декември 2022 година За Европейския парламент Председател R. METSOLA Член 46 Адресати За Съвета Председател M. BEK		

ПРИЛОЖЕНИЕ I

СЕКТОРИ С ВИСОКА СТЕПЕН НА КРИТИЧНОСТ

Сектор	Подсектор	Вид субект
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
		— Оператори на разпределителни системи съгласно определението в член 2, точка 29 от Директива (ЕС) 2019/944
		— Оператори на преносни системи съгласно определението в член 2, точка 35 от Директива (ЕС) 2019/944
		— 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 Европей- ския парламент и на Съвета (2) Участници на пазара съгласно определението в член 2, точка 25 от Регламент (ЕС) 2019/943, предоставящи услуги за агрегиране, опти- мизация 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 Дирек- тива (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)
		— Оператори на газоразпределителни системи съгласно определението в член 2, точка 6 от Директива 2009/73/ЕО
		— Оператори на газопреносни системи съгласно определението в член 2, точка 4 от Директива 2009/73/ЕО

Закон за киберсигурност

Приложение № 1

към чл. 4, ал. 1, т. 2

(Изм. – ДВ, бр. 25 от 2022 г.,

в сила от 29.03.2022 г.)

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

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

Пълно съответствие

		— Оператори на системи за съхранение съгласно определението в член 2, точка 10 от Директива 2009/73/ЕО				
		— Оператори на системи за ВПГ съгласно определението в член 2, точка 12 от Директива 2009/73/ЕО				
		— Предприятия за природен газ съгласно определението в член 2, точка 1 от Директива 2009/73/ЕО				
		— 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				
		— 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)				
	б) Железопътен	— Управители на инфраструктура съгласно определението в член 3, точка 2 от Директива 2012/34/ЕС на Европейския парламент и на Съвета (9)				
		— Железопътни предприятия, съгласно определението в член 3, точка 1 от Директива 2012/34/ЕС, включително оператори на обслуж- ващи съоръжения, посочени в член 3, точка 12 от същата директива				
	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, експлоа- тирани от тези предприятия				
		— 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				
		— 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)				
	г) Автомобилен	— 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 Директива 2010/40/ЕС на Европейския парламент и на Съвета (14)				
				Директива 2009/72/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ, L 211/55 от 14 август 2009 г.)	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 преносна система по смисъла на чл. 2, т. 4 от Директива 2009/72/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ, L 211/55 от 14 август 2009 г.)	– "Оператор на преносна мрежа" по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката	
			б) нефт	– Оператори на нефтопроводи		
				– Оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт		
			в) природен газ	– Предприятия за доставка по смисъла на чл. 2, т. 8 от Директива 2009/73/ЕО на Европейския парламент и	– "Краен снабдител" по смисъла на § 1, т. 28а от допълнителните	

3. Банков сектор		Кредитни институции съгласно определението в член 4, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета (15)			на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	разпоредби на Закона за енергетиката
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)				
		— 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)			– Оператори на газоразпределителна система по смисъла на чл. 2, т. 6 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	– "Оператор на разпределителна мрежа" по смисъла на § 1, т. 34б от допълнителните разпоредби на Закона за енергетиката
		— 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 консумация от човека е несъществена част от общата им дейност по дистрибуция на други стоки и продукти			– Оператори на газопреносна система по смисъла на чл. 2, т. 4 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	– "Оператор на преносна мрежа" по смисъла на § 1, т. 34а от допълнителните разпоредби на Закона за енергетиката
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			– Оператори на система за съхранение по смисъла на чл. 2, т. 10 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	– "Оператор на съоръжение за съхранение" по смисъла на § 1, т. 34г от допълнителните разпоредби на Закона за енергетиката
8. Цифрова инфра- структура		— 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			– Оператори на система за втечнен природен газ по смисъла на чл. 2, т. 12	– "Оператор на съоръжение за втечнен природен

9. Управление на услуги в областта на ИКТ (между предприятия)		Доставчици на управлявани услуги Доставчици на управлявани услуги за сигурност
10.Публична ад-министрация	— Органи на публичната администрация на централното държавно управление, определени от държава членка в съответствие с национал- ното право	
— Органи на публичната администрация на регионално равнище, определени от държава членка в съответствие с националното право		
11. 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	
(1) Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 г. относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ L 158, 14.6.2019 г., стр. 125).		
(2) Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета от 5 юни 2019 г. относно вътрешния пазар на електроенергия (ОВ L 158, 14.6.2019 г., стр. 54).		
(3) Директива (ЕС) 2018/2001 на Европейския парламент и на Съвета от 11 декември 2018 година за насърчаване използването на енергия от възобновяеми източници (ОВ L 328, 21.12.2018 г., стр. 82).		
(4) Директива 2009/119/ЕО на Съвета от 14 септември 2009 г. за налагане на задължение на държавите членки да поддържат минимални запаси от суров нефт и/или нефтопродукти (ОВ L 265, 9.10.2009 г., стр. 9).		
(5) Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ L 211, 14.8.2009 г., стр. 94).		
Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 г. относно летищните такси (ОВ L 70, 14.3.2009 г., стр. 11). Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. относно насоките на Съюза за развитието на трансевропейската транспортна мрежа и за отмяна на Решение № 661/2010/ЕС (ОВ L 348, 20.12.2013 г., стр. 1).		
(8) Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за определяне на рамката за създаването на Единно европейско небе (рамков регламент) (ОВ L 96, 31.3.2004 г., стр. 1).		
(9) Директива 2012/34/ЕС на Европейския парламент и на Съвета от 21 ноември 2012 г. за създаване на единно европейско железопътно пространство (ОВ L 343, 14.12.2012 г., стр. 32).		
(10) Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ L 129, 29.4.2004 г., стр. 6).		
(11) Директива 2005/65/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 година за повишаване на сигурността на пристанищата (ОВ L 310, 25.11.2005 г., стр. 28).		
(12) Директива 2002/59/ЕО на Европейския парламент и на Съвета от 27 юни 2002 г. за създаване на система на Общността за контрол на движението на корабите и за информация и отменяща Директива 93/75/ЕИО на Съвета (ОВ L 208, 5.8.2002 г., стр. 10).		
(13) Делегиран регламент (ЕС) 2015/962 на Комисията от 18 декември 2014 г. за допълване на Директива 2010/40/ЕС на Европейския парламент и на Съвета по отношение на предоставянето в целия ЕС на информационни услуги в реално време за движението по пътищата (ОВ L 157, 23.6.2015 г., стр. 21).		
(14) Директива 2010/40/ЕС на Европейския парламент и на Съвета от 7 юли 2010 г. относно рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и за интерфейси с останалите видове транспорт (ОВ L 207, 6.8.2010 г., стр. 1).		

		от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	газ" по смисъла на § 1, т. 34в от допълнителните разпоредби на Закона за енергетиката
		– Предприятия за природен газ по смисъла на чл. 2, т. 1 от Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ, L 211/94 от 14 август 2009 г.)	– "Производител" по смисъла на § 1, т. 46 от допълнителните разпоредби на Закона за енергетиката
		– Оператори на съоръжения за рафиниране и преработка на природен газ	
2. Транспорт	а) въздушен транспорт	– Въздушни превозвачи по смисъла на чл. 3, т. 4 от Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ, L 97/72 от 9 април 2008 г.)	
		– Управляващи летищата органи по смисъла на чл. 2, т. 2 от Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 г. относно летищните такси (ОВ, L 70/11 от 14 март 2009 г.)	– "Летищна администрация" по смисъла на § 3, т. 15 от допълнителните разпоредби на Закона за

(15) Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г., стр. 1).
(16) Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС (ОВ L 173, 12.6.2014 г., стр. 349).
(17) Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета на 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ L 201, 27.7.2012 г., стр. 1).
(18) Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ L 88, 4.4.2011 г., стр. 45).
(19) Регламент (ЕС) 2022/2371 на Европейския парламент и на Съвета от 23 ноември 2022 г. относно сериозните трансгранични заплахи за здравето и за отмяна на Решение № 1082/2013/ЕС (ОВ L 314, 6.12.2022 г., стр. 26).
Директива 2001/83/ЕО на Европейския парламент и на Съвета от 6 ноември 2001 г. за утвърждаване на кодекс на Общността относно лекарствени продукти за хуманна употреба (ОВ L 311, 28.11.2001 г., стр. 67). Регламент (ЕС) 2022/123 на Европейския парламент и на Съвета от 25 януари 2022 г. относно засилена роля на Европейската агенция по лекарствата в готовността за действия при кризи и управлението на кризи по отношение на лекарствените продукти и медицинските изделия (ОВ L 20, 31.1.2022 г., стр. 1).
(22) Директива (ЕС) 2020/2184 на Европейския парламент и на Съвета от 16 декември 2020 г. относно качеството на водите, предназначени за консумация от човека (ОВ L 435, 23.12.2020 г., стр. 1).
(23) Директива 91/271/ЕИО на Съвета от 21 май 1991 г. за пречистването на градските отпадъчни води (ОВ L 135, 30.5.1991 г., стр. 40).

ПРИЛОЖЕНИЕ II

ДРУГИ КРИТИЧНИ СЕКТОРИ

Сектор	Подсектор	Вид субект
1. Пощенски и куриерски услуги		Доставчици на пощенски услу определението в член 2, точка 1а 97/67/ЕО, включително доставчици услуги
2. Управление на отпадъците		Предприятия, извършващи управление съгласно определението в член 3, Директива 2008/98/ЕО на Европейския Съвета (1), с изключение на предпри управлението на отпадъците не икономическа дейност
		– Летища по смисъла на чл. 2, т. 1 от Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 г. относно летищните такси (ОВ, L 70/11 от 14 март 2009 г.), включително летища, изброени в раздел 2 от приложение II към Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. относно насоките на Съюза за развитието на трансевропейската транспортна мрежа и за отмяна на Решение № 661/2010/ЕС (ОВ, L 348/1 от 20 декември 2013 г.), както и субекти, които експлоатират помощни инсталации, намиращи се в рамките на летището	– "Летищен оператор" по смисъла на § 3, т. 16 от допълнителните разпоредби на Закона за гражданското въздухоплаване – "Летище" по смисъла на § 3, т. 13 от допълнителните разпоредби на Закона за гражданското въздухоплаване
		– Оператори по контрола на управлението на движението, осъществяващи обслужване по контрол на въздушното движение по смисъла на чл. 2, т. 1 от Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета от 10 март 2004 г. за определяне на рамката за създаването на Единно европейско небе (рамков регламент) (ОВ, L 96/1 от 31 март 2004 г.)	– "Управление на въздушното движение" по смисъла на § 3, т. 44 от допълнителните разпоредби на Закона за гражданското въздухоплаване
	б) железопътен транспорт	– Управители на инфраструктура по смисъла на чл. 3, т. 2 от Директива 2012/34/ЕС на Европейския парламент и	– "Управител на железопътна инфраструктура" по смисъла на § 1, т. 2 от

3. Производство, изготвяне и ди- стрибуция 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	на Съвета от 21 ноември 2012 г. за създаване на единно европейско железопътно пространство (ОВ, L 343/32 от 14 декември 2012 г.)	допълнителните разпоредби на Закона за железопътния транспорт
4. Производство, преработка и раз- пространение 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	– Железопътни предприятия по смисъла на чл. 3, т. 1 от Директива 2012/34/ЕС на Европейския парламент и на Съвета от 21 ноември 2012 г. за създаване на единно европейско железопътно пространство (ОВ, L 343/32 от 14 декември 2012 г.), включително оператори на обслужващи съоръжения по смисъла на чл. 3, т. 12 от посочената директива	– "Железопътно предприятие" по смисъла на чл. 48 от Закона за железопътния транспорт – "Оператор на обслужващо съоръжение" по смисъла на § 1, т. 51 от допълнителните разпоредби на Закона за железопътния транспорт
5. Производство	а) Производство на медицински изделия и медицински изделия за инвитро диаг- ностика	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		
	б) Производство на компютри, електронни и оптични продукти	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел в) B, разделение 26 на NACE Rev. 2	– Предприятия за вътрешноводен, морски и крайбрежен транспорт на пътници и товари по смисъла на приложение I към Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ, L 129/6 от 29 април 2004 г.), с изключение на отделните кораби, експлоатирани от тези предприятия	– "Компания" по смисъла на § 1, т. 12 от допълнителните разпоредби на Наредбата за условията и реда за постигане сигурността на корабите, пристанищата и пристанищните райони (ДВ, бр. 99 от 2014 г.)
	в) Производство на електрически съоръже- ния	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 27 на NACE Rev. 2		
	г) Производство на машини и оборудване, некласифицирани 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 обо- рудване	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 30 на NACE Rev. 2		
Сектор	Подсектор	Вид субект		
6. Доставчици на цифрови услуги		— Доставчици на онлайн места за търговия		
		— Доставчици на онлайн търсачки	– Управителните органи на пристанища по смисъла на чл. 3, т. 1 от Директива 2005/65/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 г. за повишаване на	– "Пристанище" по смисъла на чл. 92, ал. 1 от Закона за морските пространства, вътрешните водни пътища и
		— Доставчици на платформи на услуги за социални мрежи		
7. Научни изследвания		Научноизследователски организации		

ПРИЛОЖЕНИЕ III

ТАБЛИЦА НА СЪОТВЕТСТВИЕТО

Директива (ЕС) 2016/1148	Настоящата директива
Член 1, параграф 1	Член 1, параграф 1
Член 1, параграф 2	Член 1, параграф 2
Член 1, параграф 3	-
Член 1, параграф 4	Член 2, параграф 12
Член 1, параграф 5	Член 2, параграф 13
Член 1, параграф 6	Член 2, параграфи 6 и 11
Член 1, параграф 7	Член 2, параграф 4
Член 2	Член 2, параграф 14
Член 3	Член 5
Член 4	Член 6
Член 5	-
Член 6	-
Член 7, параграф 1	Член 7, параграфи 1 и 2
Член 7, параграф 2	Член 7, параграф 4
Член 7, параграф 3	Член 7, параграф 3
Член 8, параграфи 1 до 5	Член 8, параграфи 1 до 5
Член 8, параграф 6	Член 13, параграф 4
Член 8, параграф 7	Член 8, параграф 6
Член 9, параграфи 1, 2 и 3	Член 10, параграфи 1, 2 и 3
Член 9, параграф 4	Член 10, параграф 9
Член 9, параграф 5	Член 10, параграф 10

		сигурността на пристанищата (ОВ, L 310/28 от 25 ноември 2005 г.), включително техните пристанищни съоръжения по смисъла на чл. 2, т. 11 от Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ, L 129/6 от 29 април 2004 г.), както и субекти, експлоатиращи инсталации и оборудване, разположено в рамките на пристанището	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 службата по морския трафик по смисъла на чл. 3, буква "о" от Директива 2002/59/ЕО на Европейския парламент и на Съвета от 27 юни 2002 г. за създаване на система на Общността за контрол на движението на корабите и за информация и отменяща Директива 93/75/ЕИО на Съвета (ОВ, L 208/10 от 5 август 2002 г.)	– Чл. 244а, ал. 1 и 2 от Кодекса на търговското корабоплаване – Чл. 115м, ал. 1, т. 12, 13, 14 и 15 от Закона за морските пространства, вътрешните водни пътища и пристанищата на Република България
	г) автомобилен транспорт	– Пътни органи по смисъла на чл. 2, т. 12 от Делегиран регламент (ЕС) 2015/962 на Комисията от 18 декември 2014 г. за допълване на Директива 2010/40/ЕС на Европейския парламент и на Съвета по отношение	

Член 10, параграфи 1, 2 и 3, първа алинея	Член 13, параграфи 1, 2 и 3				на предоставянето в целия ЕС на информационни услуги в реално време за движението по пътищата (ОВ, L 157/21 от 23 юни 2015 г.), които отговарят за контрола на управлението на движението	
Член 10, параграф 3, втора алинея	Член 23, параграф 9					
Член 11, параграф 1	Член 14, параграфи 1 и 2					
Член 11, параграф 2	Член 14, параграф 3					
Член 11, параграф 3	Член 14, параграф 4, първа алинея, букви а) до р) и буква т) и параграф 7					
Член 11, параграф 4	Член 14, параграф 4, първа алинея, буква с) и втора алинея				– Оператори на интелигентни транспортни системи по смисъла на чл. 4, т. 1 от Директива 2010/40/ЕС на Европейския парламент и на Съвета от 7 юли 2010 г. относно рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и за интерфейси с останалите видове транспорт (ОВ, L 207/1 от 6 август 2010 г.)	– "Интелигентни транспортни системи" по смисъла на § 1, т. 40 от допълнителните разпоредби на Закона за автомобилните превози
Член 11, параграф 5	Член 14, параграф 8					
Член 12, параграфи 1 до 5	Член 15, параграфи 1 до 5					
Член 13	Член 17					
Член 14, параграфи 1 и 2	Член 21, параграфи 1 до 4					
Член 14, параграф 3	Член 23, параграф 1					
Член 14, параграф 4	Член 23, параграф 3					
Член 14, параграф 5	Член 23, параграфи 5, 6 и 8					
Член 14, параграф 6	Член 23, параграф 7					
Член 14, параграф 7	Член 23, параграф 11					
Член 15, параграф 1	Член 31, параграф 1		3. (Изм. – ДВ, бр. 25 от 2022 г., в сила от 29.03.2022 г.) Банково		– Кредитни институции по смисъла на чл. 4, параграф 1, т. 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и за изменение на Регламент (ЕС) № 648/2012 (ОВ, L 176/1 от 27 юни 2013 г.)	
Член 15, параграф 2, първа алинея, буква а)	член 32, параграф 2, буква д)					
Член 15, параграф 2, първа алинея, буква б)	Член 32, параграф 2, буква ж)					
Член 15, параграф 2, втора алинея	Член 32, параграф 3					
Член 15, параграф 3	Член 32, параграф 4, буква б)					
Член 15, параграф 4	Член 31, параграф 3					
Член 16, параграфи 1 и 2	Член 21, параграфи 1 до 4					
Член 16, параграф 3	Член 23, параграф 1					
Член 16, параграф 4	Член 23, параграф 3					
Член 16, параграф 5	-					
Член 16, параграф 6	Член 23, параграф 6					

	Член 16, параграф 7	Член 23, параграф 7		дело			
	Член 16, параграфи 8 и 9	Член 21, параграф 5 и член 23, параграф 11		4. Инфраструктури на финансовия пазар		– Оператори на местата за търговия по смисъла на чл. 4, параграф 1, т. 24 от Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС (ОВ, L 173/349 от 12 юни 2014 г.)	Закона за пазарите на финансови инструменти
	Член 16, параграф 10	-					
	Член 16, параграф 11	Член 2, параграфи 1, 2 и 3					
	Член 17, параграф 1	Член 33, параграф 1					
	Член 17, параграф 2, буква а)	Член 32, параграф 2, буква д)					
	Член 17, параграф 2, буква б)	Член 32, параграф 4, буква б)					
	Член 17, параграф 3	Член 37, параграф 1, букви а) и б)					
	Член 18, параграф 1	Член 26, параграф 1, буква б) и параграф 2					
	Член 18, параграф 2	Член 26, параграф 3				– Централни контрагенти по смисъла на чл. 2, т. 1 от Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ, L 201/1 от 27 юли 2012 г.)	
	Член 18, параграф 3	Член 26, параграф 4					
	Член 19	Член 25					
	Член 20	Член 30					
	Член 21	Член 36					
	Член 22	Член 39					
	Член 23	Член 40		5. Здравеопазване	Здравни заведения, включително болници и частни клиники	– Доставчици на здравно обслужване по смисъла на чл. 3, буква "ж" от Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ, L 88/45 от 4 април 2011 г.)	– Чл. 21, ал. 1, 2 и 3 от Закона за здравето – Чл. 2, ал. 1, чл. 5, ал. 1, чл. 8, ал. 1, чл. 9, ал. 1, 2 и 3, чл. 10 от Закона за лечебните заведения
	Член 24	-					
	Член 25	Член 41					
	Член 26	Член 45					
	Член 27	Член 46					
	Приложение I, точка 1	Член 11, параграф 1					
	Приложение I, точка 2, буква а), подточки i)—iv)	Член 11, параграф 2, букви а) до г)					
	Приложение I, точка 2, буква а), подточка v)	Член 11, параграф 2, буква е)		6. Доставка и снабдяване с питейни		– Доставчици и снабдители с води, предназначени за консумация от човека по смисъла на чл. 2, § 1, буква "а" от Директива 98/83/ЕО на Съвета от 3 ноември 1998 г. относно качеството на водите, предназначени за	Допълнителните разпоредби на Наредба № 9 от 2001 г. за качеството на водата, предназначена за питейно-битови цели (ДВ, бр. 30 от 2001 г.)
	Приложение I, точка 2, буква б)	Член 11, параграф 4					
	Приложение I, точка 2, буква в), подточки i) и ii)	Член 11, параграф 5, буква а)					
	Приложение II	Приложение I					
	Приложение III, точки 1 и 2	Приложение II, точка 6					
	Приложение III, точка 3	Приложение I, точка 8					

а вода		консумация от човека (ОВ, L 330/32 от 5 декември 1998 г.), с изключение на снабдителите, за които снабдяването с води, предназначени за консумация от човека, е само част от общата им дейност за снабдяване с блага и стоки, които не се считат за съществени услуги	
7. Цифрова инфраструктура		– Точка за обмен в интернет (ТОИ)	
		– Доставчици на DNS услуги	
		– Регистри на имената на домейни от първо ниво	

Приложение № 2

към чл. 4, т. 2

Видове цифрови услуги

1. Онлайн място за търговия.

2. Онлайн търсачка.

3. Компютърни услуги "в облак".

Проект на Закон за изменение и допълнение на Закона за киберсигурност

ПРИЛОЖЕНИЕ I

към чл. 4, ал. 1, т. 2

СПИСЪК НА СЕКТОРИТЕ И ПОДСЕКТОРИТЕ

Сектор	Подсектор	Вид субект	Съответствие
1Енергет. тика	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) 2019/944Директива (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,	– „Оператор на съоръжение за втечнен природен газ“ по смисъла на § 1, т. 34в от допълнителните		

			точка 12 от Директива 2009/73/ЕО	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 Водор) од	– Оператори в областта на производството, съхранението и преноса на водород			
2Транс. порт	а Въздu) шен		– 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,	– „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		

		експлоатиращи спомагателни инсталации, намиращи се на летищата	
		– 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	– „Компания“ по смисъла на § 1, т. 12 от допълнителните разпоредби на Наредбата за условията и реда за постигане сигурността на корабите, пристанищата и

				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	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		
			гАвтом)обилен	– 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 Директива 2010/40/ЕС на Европейския парламент и на Съвета (14)	„Интелигентни транспортни системи“ по смисъла на § 1, т. 40 от допълнителните разпоредби на Закона за автомобилните превози		
	3.	Банков сектор	Кредитни институции съгласно определението в член 4, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета (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 консумация от човека е несъществена част от общата им дейност по дистрибуция на други стоки и продукти	§ 1, т. 1, буква „а“ от допълнителните разпоредби на Наредба № 9 от 2001 г. за качеството на 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	Допълнителни разпоредби на Наредба № 6 от 9.11.2000 г. за емисионни норми за допустимото съдържание на вредни и опасни вещества в отпадъчните води, заустван във водни обекти (обн., ДВ, бр. 97 от 28.11.2000 г.) - § 1, т. 24		

			изключение на предприятията, за които събирането, обезвреждането или пречистването на градски, битови или промишлени отпадъчни води е несъществена част от тяхната обща дейност	(„отпадъчни води от населени места“), т. 28 („производствени отпадъчни води“) и т. 35 („фекално-битови отпадъчни води“)			
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		– Доставчици на управлявани услуги – Доставчици на управлявани услуги за сигурност				

(между предприятия)			
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

ДРУГИ КРИТИЧНИ СЕКТОРИ

Сектор	Подсектор	Вид субект	Съответствие
1. Пощенски 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	ЗАКОН за управление на отпадъците Определението за „управление на отпадъците“ е транспонирано в § 1, т. 46 от Закона за

			отпадъците не е основна икономическа дейност	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, некласифицирани другаде	Предприятия, извършващи някоя от икономическите дейности съгласно определението в раздел B, разделение 28 на NACE Rev. 2		
		д)	Производство на	Предприятия, извършващи някоя от икономическите		

	моторни превозни средства, ремаркета и полуремаркета	дейности съгласно определението в раздел B, разделение 29 на NACE Rev. 2		
	e) 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		