ДИРЕКТИВИ

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)

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейската централна банка ([1]),

като взеха предвид становището на Европейския икономически и социален комитет ([2]),

след консултация с Комитета на регионите,

в съответствие с обикновената законодателна процедура ([3]),

като имат предвид, че:

(1) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([4]) има за цел да изгради способности в областта на киберсигурността в Съюза, да ограничи заплахите за мрежовите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и да гарантира непрекъснатостта на тези услуги при инциденти, като по този начин допринася за сигурността в Съюза и за ефективното функциониране на икономиката и обществото му.

(2) След влизането в сила на Директива (ЕС) 2016/1148 бе постигнат значителен напредък при повишаването на нивото на киберустойчивост на Съюза. Прегледът на посочената директива показа, че тя е послужила като катализатор за институционалния и регулаторния подход към киберсигурността в Съюза, като е проправила пътя за значителна промяна в нагласите. Директивата осигури завършването на националните рамки относно сигурността на мрежовите и информационните системи чрез създаването на национални стратегии за сигурност на мрежовите и информационните системи и създаването на национални способности и чрез изпълнението на регулаторни мерки, обхващащи съществени инфраструктури и субекти, установени от всяка държава членка. Директива (ЕС) 2016/1148 допринесе и за развитието на сътрудничеството на равнището на Съюза посредством установяването на групата за сътрудничество и мрежата от национални екипи за реагиране при инциденти с компютърната сигурност. Прегледът на Директива (ЕС) 2016/1148 обаче разкри, че независимо от тези постижения, тя има и присъщи слабости, които пречат на намирането на ефективни решения за настоящите и възникващи предизвикателства в областта на киберсигурността.

(3) Мрежовите и информационните системи се превърнаха в централен елемент на всекидневния живот на фона на бързата цифрова трансформация и взаимосвързаността на обществото, включително в трансграничния обмен. Това развитие води до разширяването на броя на киберзаплахите, пораждайки нови такива, и изисква адаптирани, координирани и новаторски реакции във всички държави членки. Броят, мащабите, сложността, честотата и въздействието на инцидентите се увеличават и представляват съществена заплаха за функционирането на мрежовите и информационните системи. В резултат на това инцидентите могат да попречат на извършването на икономически дейности в рамките на вътрешния пазар, да причинят финансова загуба, да подкопаят доверието на потребителите и

([1]) ОВ C 233, 16.6.2022 г., стр. 22.
([2]) ОВ C 286, 16.7.2021 г., стр. 170.
([3]) Позиция на Европейския парламент от 10 ноември 2022 г. (все още непубликувана в Официален вестник) и решение на Съвета от 28 ноември 2022 г.
([4]) 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, 19.7.2016 г., стр. 1).

да причинят съществени вреди на икономиката и обществото на Съюза. Затова подготвеността и ефективността в областта на киберсигурността сега са по-важни от всякога за правилното функциониране на вътрешния пазар. Освен това киберсигурността е ключов фактор, който предоставя възможност на редица критични сектори да се включат успешно в цифровата трансформация и да се възползват изцяло от икономическите, социалните и устойчивите предимства на цифровизацията.

(4) Правното основание за Директива (ЕС) 2016/1148 е член 114 от Договора за функционирането на Европейския съюз (ДФЕС), чиято цел е създаването и функционирането на вътрешния пазар чрез усъвършенстване на мерките за сближаване на националните правила. Изискванията за киберсигурност, наложени на субектите, предоставящи услуги или извършващи дейности, които са икономически значими, се различават значително в държавите членки от гледна точка на вида на изискванията, степента им на подробност и метода на надзор. Тези различия водят до допълнителни разходи и пораждат затруднения за субектите, предлагащи трансгранично стоки или услуги. Наложените от една държава членка изисквания, които са различни от наложените в друга или дори са в противоречие с тях, може съществено да засегнат подобни трансгранични дейности. Освен това възможността за недостатъчно изготвяне или прилагане на изисквания за киберсигурност в една държава членка е вероятно да има последици по отношение на нивото на киберсигурност на държави членки, по-специално предвид интензивността на трансграничния обмен. Прегледът на Директива (ЕС) 2016/1148 показва големи различия в прилагането ѝ от държавите членки, включително във връзка с нейния обхват, чието очертаване в много голяма степен бе оставено на преценката на държавите членки. Директива (ЕС) 2016/1148 предоставя на държавите членки и много широка свобода на преценка по отношение на прилагането на предвидените в нея задължения, свързани със сигурността и докладването за инциденти. Поради това тези задължения бяха приложени по значително различаващи се начини на национално равнище. Съществуват сходни различия в прилагането на разпоредбите на Директива (ЕС) 2016/1148 относно надзора и правоприлагането.

(5) Всички тези различия водят до фрагментирането на вътрешния пазар и могат да имат вредно въздействие върху функционирането му, засягайки по-специално трансграничното предоставяне на услуги и нивото на киберустойчивост поради прилагането на различни мерки. В крайна сметка тези различия могат да доведат до по-голяма уязвимост на някои държави членки спрямо киберзаплахи, което би предизвикало потенциални странични ефекти за целия Съюз. Настоящата директива има за цел да премахне тези големи различия между държавите членки, по-специално посредством предвиждането на минимални правила относно функционирането на координирана регулаторна рамка, установяването на механизми за ефективно сътрудничество между отговорните органи във всяка държава членка, актуализирането на списъка със сектори и дейности, подчинени на задълженията за киберсигурност, и предоставянето на ефективни правни средства за защита и правоприлагащи мерки, които са от ключово значение за ефективното правоприлагане на тези задължения. Поради това Директива (ЕС) 2016/1148 следва да бъде отменена и заменена с настоящата директива.

(6) С отмяната на Директива (ЕС) 2016/1148 приложното поле следва да се разшири така, че да обхване по-голяма част от секторите на икономиката, за да се осигури пълно включване на сектори и услуги от жизненоважно значение за ключови обществени и икономически дейности във вътрешния пазар. По-специално настоящата директива има за цел да преодолее недостатъците, свързани с разграничаването между оператори на основни услуги и доставчици на цифрови услуги, което е доказано остаряло, тъй като не отразява значимостта на секторите или услугите за обществените и икономическите дейности във вътрешния пазар.

(7) Съгласно Директива (ЕС) 2016/1148 държавите членки са отговорни за определянето на субектите, които отговарят на критериите за оператори на основни услуги. За да се отстранят големите различия сред държавите членки в това отношение и да се гарантира правна сигурност по отношение на мерките за управление на риска в областта на киберсигурността и задълженията за докладване по отношение на всички относими субекти, следва да се установи еднакъв критерий, определящ субектите, попадащи в обхвата на настоящата директива. Този критерий следва да се състои в прилагането на правилото за размер на предприятието, при което всички субекти, които отговарят на критериите за средни предприятия съгласно член 2 от приложението към Препоръка 2003/361/ЕО на Комисията ([5]) или надхвърлят таваните за средни предприятия, посочени в параграф 1 от същия член, и които упражняват дейност в секторите и предоставят видовете услуги или извършват дейностите, обхванати от настоящата директива, попадат в

([5]) Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

нейния обхват. Държавите членки следва също така да предвидят определени малки и микропредприятия по смисъла на член 2, параграфи 2 и 3 от посоченото приложение, които отговарят на специфични критерии, показващи ключова роля за обществото, икономиката или за определени сектори или видове услуги, да попадат в обхвата на настоящата директива.

(8) Изключването на органите на публичната администрация от обхвата на настоящата директива следва да се прилага за субекти, чиито дейности се извършват предимно в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително предотвратяването, разследването, разкриването и наказателното преследване на престъпления. Органите на публичната администрация обаче, чиито дейности са свързани само в незначителна степен с тези области, не следва да бъдат изключени от обхвата на настоящата директива. За целите на настоящата директива не се счита, че субектите с регулаторни компетенции извършват дейности в областта на правоприлагането и следователно те не са изключени от обхвата на настоящата директива на това основание. Органите на публичната администрация, които са създадени съвместно с трета държава в съответствие с международно споразумение, са изключени от обхвата на настоящата директива. Настоящата директива не се прилага за дипломатическите и консулските мисии на държавите членки в трети страни или за техните мрежови и информационни системи, доколкото тези системи се намират в помещенията на мисията или се използват за потребители в трета държава.

(9) Държавите членки следва да могат да предприемат необходимите мерки, с които да гарантират защитата на основните интереси на националната сигурност, да опазват обществения ред и обществената сигурност и да създават условия за предотвратяването, разследването, разкриването и наказателното преследване на престъпления. За тази цел държавите членки следва да могат да освободят определени субекти, които извършват дейности в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително предотвратяването, разследването, разкриването и наказателното преследване на престъпления, от някои задължения, предвидени в настоящата директива по отношение на тези дейности. Когато даден субект предоставя услуги изключително на орган на публичната администрация, който е изключен от обхвата на настоящата директива, държавите членки следва да могат да освободят този субект от определени задължения, предвидени в настоящата директива по отношение на тези услуги. Освен това нито една държава членка не следва да бъде задължавана да предоставя информация, чието разкриване би противоречало на основните интереси на нейната национална сигурност, на обществената сигурност или на отбраната. В този смисъл следва да се имат предвид правилата на Съюза или националните правила за защита на класифицираната информация, споразуменията за неразкриване на информация и неформалните споразумения за неразкриване на информация като протокола за обмен на информация с цветен код за поверителност (Traffic Light Protocol). Протоколът за обмен на информация с цветен код за поверителност следва да се разбира като средство за предоставяне на информация за всякакви ограничения по отношение на по-нататъшното разпространение на информация. Той се използва в почти всички екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) и в някои центрове за анализ и обмен на информация.

(10) Въпреки че настоящата директива се прилага за субекти, извършващи дейности по производство на електроенергия от атомни електроцентрали, някои от тези дейности могат да бъдат свързани с националната сигурност. В такъв случай дадена държава членка следва да може да упражнява своята отговорност за гарантиране на националната сигурност по отношение на тези дейности, включително дейностите в рамките на ядрената верига за създаване на стойност, в съответствие с Договорите.

(11) Някои субекти извършват дейности в областта на националната сигурност, обществената сигурност, отбраната или правоприлагането, включително предотвратяването, разследването, разкриването и наказателното преследване на престъпления, като същевременно предоставят и удостоверителни услуги. Доставчиците на удостоверителни услуги, които попадат в обхвата на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета ([6]), следва да попадат в обхвата на настоящата директива, за да се гарантира същото ниво на изисквания за сигурност и надзор като установеното преди това в посочения регламент по отношение на доставчиците на удостоверителни услуги. В съответствие с изключването на някои специфични услуги от Регламент (ЕС) № 910/2014 настоящата директива следва да не се прилага за предоставянето на удостоверителни услуги, използвани единствено в рамките на затворени системи, произтичащи от националното право или от споразумения между определен кръг от участници.

([6]) Регламент (ЕС) № 910/2014 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, 28.8.2014 г., стр. 73).

(12) Настоящата директива следва да се прилага за доставчиците на пощенски услуги по смисъла на Директива 97/67/ЕО на Европейския парламент и на Съвета ([7]), включително доставчиците на куриерски услуги, ако извършват поне една от операциите от веригата на пощенски доставки, и по-специално събирането, сортирането, транспорта или доставката на пощенски пратки, включително услугите за вземане от адрес, като същевременно се взема предвид степента на тяхната зависимост от мрежовите и информационните системи. Превозът, когато не е предприет във връзка с някоя от тези операции, следва да бъде изключен от обхвата на пощенските услуги.

(13) Като се има предвид засилването и повишената сложност на киберзаплахите, държавите членки следва да се стремят да гарантират, че субектите, които са изключени от обхвата на настоящата директива, постигат високо ниво на киберсигурност, и да подкрепят прилагането на еквивалентни мерки за управление на риска, свързан с киберсигурността, които отразяват чувствителния характер на тези субекти.

(14) Правото на Съюза в областта на защитата на данните и правото на Съюза в областта на неприкосновеността на личния живот се прилагат за всяко обработване на лични данни съгласно настоящата директива. По-специално настоящата директива не засяга Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([8]) и Директива 2002/58/ЕО на Европейския парламент и на Съвета ([9]). Поради това настоящата директива не следва да засяга, наред с другото, задачите и правомощията на органите, компетентни да следят за спазването на приложимото правото на Съюза в областта на защитата на данните и правото на Съюза в областта на неприкосновеността на личния живот.

(15) За целите на спазването на мерките за управление на риска в областта на киберсигурността и задълженията за докладване, попадащите в обхвата на настоящата директива субекти следва да бъдат класифицирани в две категории, съществени субекти и важни субекти, което да отразява степента им на критичност по отношение на техния сектор или на вида услуга, която предоставят, както и техния размер. В този смисъл следва надлежно да се вземат предвид всички съответни секторни оценки на риска или насоки от компетентните органи, когато е приложимо. Надзорните и правоприлагащите режими за тези две категории субекти следва да са различни, за да се гарантира справедлив баланс между основаните на риска изисквания и задължения, от една страна, и административната тежест, произтичаща от надзора на съответствието, от друга.

(16) За да се избегне възможността субекти, които имат предприятия партньори или са свързани предприятия, да бъдат считани за съществени или важни субекти, когато това би било непропорционално, държавите членки могат при прилагането на член 6, параграф 2 от приложението към Препоръка 2003/361/ЕО да вземат предвид степента на независимост, от която се ползва даден субект по отношение на своите партньори или свързани предприятия. По-специално държавите членки могат да вземат предвид факта, че даден субект е независим от своите партньори или свързани предприятия по отношение на мрежовите и информационните системи, които този субект използва при предоставянето на своите услуги, както и по отношение на услугите, които предоставя. Въз основа на това, когато е целесъобразно, държавите членки могат да считат, че такъв субект не отговаря на критериите за средно предприятие съгласно член 2 от приложението към Препоръка 2003/361/ЕО или не надхвърля таваните за средно предприятие, посочени в параграф 1 от същия член, ако, след като се вземе предвид степента на независимост на този субект, би се счело, че той не отговоря на критериите за средно предприятие или не надхвърля тези тавани, ако се вземат предвид само собствените му данни. Това не засяга задълженията по настоящата директива на партньорските и свързаните предприятия, които попадат в обхвата на настоящата директива.

(17) Държавите членки следва да могат да решават, че субектите, установени преди влизането в сила на настоящата директива като оператори на основни услуги в съответствие с Директива (ЕС) 2016/1148, следва да се считат за съществени субекти.

([7]) Директива 97/67/ЕО на Европейския парламент и на Съвета от 15 декември 1997 г. относно общите правила за развитието на вътрешния пазар на пощенските услуги в Общността и за подобряването на качеството на услугата (ОВ L 15, 21.1.1998 г., стр. 14).

([8]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([9]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

(18) За да се осигури ясен преглед на субектите, попадащи в обхвата на настоящата директива, държавите членки следва да изготвят списък на съществените и важните субекти, както и на субектите, предоставящи услуги по регистрация на имена на домейни. За тази цел държавите членки следва да изискват от субектите да предоставят на компетентните органи най-малко следната информация, а именно наименованието, адреса и актуалните данни за връзка, включително адресите на електронна поща, IP обхватите и телефонните номера на субекта и когато е приложимо, съответния сектор и подсектор, посочен в приложенията, както и когато е приложимо списък на държавите членки, в които те предоставят услуги, попадащи в обхвата на настоящата директива. За тази цел следва Комисията, със съдействието на Агенцията на Европейския съюз за киберсигурност (ENISA), да предостави без ненужно забавяне насоки и образци относно задължението за представяне на информация. За да се улесни изготвянето и актуализирането на списъка на съществените и важните субекти, както и субектите, предоставящи услуги по регистрация на имена на домейни, държавите членки следва да могат да установят национални механизми, чрез които субектите да се регистрират. Ако съществуват регистри на национално равнище, държавите членки могат да вземат решение относно подходящите механизми, които позволяват да се установи кои субекти попадат в обхвата на настоящата директива.

(19) Държавите членки следва да отговарят за предоставянето на Комисията поне на броя на съществените и важните субекти за всеки сектор и подсектор, посочени в приложенията, както и на съответната информация относно броя на установените субекти и разпоредбата измежду предвидените в настоящата директива, въз основа на която те са били установени и типа услуга, която предоставят. Държавите членки се насърчават да обменят с Комисията информация относно съществените и важните субекти, а в случай на мащабен киберинцидент – относимата информация, като например наименованието на съответния субект.

(20) Комисията, в сътрудничество с групата за сътрудничество и след консултация със съответните заинтересовани лица, следва да предоставя насоки за прилагането на критериите, приложими за микропредприятията и малки предприятия, за да прецени дали те попадат в обхвата на настоящата директива. Комисията следва също така да гарантира, че на микропредприятията и малките предприятия, попадащи в обхвата на настоящата директива, се предоставят подходящи насоки. Комисията, със съдействието на държавите членки, следва да предоставя информация на микропредприятията и малките предприятия в това отношение.

(21) Комисията може също така да предоставя насоки за подпомагане на държавите членки при прилагането на разпоредбите на настоящата директива относно обхвата и за оценка на пропорционалността на мерките, предприети в съответствие в настоящата директива, по-специално по отношение на субекти със сложни бизнес модели или оперативна среда, при които даден субект може едновременно да изпълнява критериите, определени както за съществени, така и за важни субекти, или може едновременно да извършва дейности, част от които попадат в обхвата на настоящата директива, а друга част са изключени от него.

(22) С настоящата директива се определя основата за мерките за управление на риска в областта на киберсигурността и задълженията за докладване в секторите от нейния обхват. С цел да се избегне фрагментирането на разпоредбите в областта на киберсигурността в правните актове на Съюза, когато се счита, че за да се гарантира високо равнище на киберсигурност, са необходими допълнителни специфични за сектора правни актове на Съюза, отнасящи се до мерки за управление на риска в областта на киберсигурността и задължения за докладване, Комисията следва да прецени дали такива разпоредби биха могли да бъдат установени в акт за изпълнение съгласно настоящата директива. Ако такъв акт за изпълнение не е подходящ за тази цел, специфични за сектора правни актове на Съюза биха могли да допринесат за гарантиране на високо равнище на киберсигурност, като същевременно се отчитат в пълна степен особеностите и сложността на съответните сектори. За тази цел настоящата директива не изключва приемането на други специфични за сектора правни актове на Съюза, в които се уреждат мерките за управление на риска в областта на киберсигурността и задължения за докладване, които отчитат надлежно потребността от всеобхватна и последователна рамка за киберсигурност. Настоящата директива не засяга съществуващите изпълнителни правомощия, предоставени на Комисията в редица сектори, включително в транспорта и енергетиката.

(23) Когато даден специфичен за сектора правен акт на Съюза съдържа разпоредби, изискващи от 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 настоящата директива задължения, тези разпоредби, включително относно надзора и правоприлагането, следва да се прилагат за

такива субекти. Ако даден специфичен за сектора правен акт на Съюза не обхваща 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 този акт.

(24) Когато разпоредбите на специфичен за сектора правен акт на Съюза изискват от съществените или важните субекти да изпълняват задължения за докладване, които имат най-малко равностоен ефект на предвидените в настоящата директива задължения за докладване, при разглеждането на уведомленията за инциденти следва да се гарантират съгласуваност и ефективност. За тази цел разпоредбите относно уведомленията за инциденти от специфичния за сектора правен акт на Съюза следва да предоставят на ЕРИКС, компетентните органи или единните звена за контакт по въпросите на киберсигурността (единни звена за контакт) съгласно настоящата директива незабавен достъп до уведомленията за инциденти, подадени в съответствие със специфичния за сектора правен акт на Съюза. По-специално такъв незабавен достъп може да бъде осигурен, ако уведомленията за инциденти се препращат без ненужно забавяне на ЕРИКС, компетентния орган или единното звено за контакт съгласно настоящата директива. Когато е целесъобразно, държавите членки следва да въведат механизъм за автоматично и пряко докладване, който да гарантира систематичен и незабавен обмен на информация с ЕРИКС, компетентните органи или единните звена за контакт относно разглеждането на такива уведомления за инциденти. С цел опростяване на докладването и прилагане на механизма за автоматично и пряко докладване държавите членки могат, в съответствие със специфичния за сектора правен акт на Съюза, да използват единна входяща точка.

(25) В специфичните за сектора правни актове на Съюза, които предвиждат мерки за управление на риска в областта на киберсигурността или задължения за докладване, които имат най-малко равностоен ефект на предвидените в настоящата директива, може да се предвиди, че компетентните органи по силата на такива актове упражняват своите надзорни и правоприлагащи правомощия във връзка с такива мерки или задължения със съдействието на компетентните органи съгласно настоящата директива. Съответните компетентни органи биха могли да установят договорености за сътрудничество за тази цел. В такива договорености за сътрудничество биха могли да се уточнят, наред с другото, процедурите за координиране на надзорните дейности, включително процедурите за разследвания и проверки на място в съответствие с националното право, както и да се предвиди механизъм за обмен между компетентните органи на съответната информация относно надзора и правоприлагането, включително достъп до свързана с киберпространството информация, поискана от компетентните органи съгласно настоящата директива.

(26) Когато специфичните за сектора правни актове на Съюза изискват или предоставят стимули за субектите да уведомяват за значителни киберзаплахи, държавите членки следва също така да насърчават споделянето на значителни киберзаплахи с ЕРИКС, компетентните органи или единните звена за контакт съгласно настоящата директива, за да се гарантира по-високо равнище на осведоменост на тези образувания относно картината на киберзаплахите и да им се даде възможност да реагират ефективно и своевременно, в случай че значителните киберзаплахи се осъществят.

(27) В бъдещите специфични за сектора правни актове на Съюза следва надлежно да се вземат предвид определенията и рамката за надзор и правоприлагане, установени в настоящата директива.

(28) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета ([10]) следва да се счита за специфичен за сектора правен акт на Съюза във връзка с настоящата директива с оглед на финансовите субекти. Разпоредбите на Регламент (ЕС) 2022/2554 във връзка с управлението на риска в областта на информационните и комуникационните технологии (ИКТ), управлението на инцидентите при ИКТ и по-специално докладването за съществени инциденти с ИКТ, както и тези относно тестването на оперативната устойчивост на цифровите технологии, споразуменията за обмен на информация и риска в областта на ИКТ, пораждан от участието на трети страни, следва да се прилагат вместо предвидените в настоящата директива. Затова държавите членки не следва да прилагат разпоредбите на настоящата директива относно управлението на риска в областта на киберсигурността и задълженията за докладване и надзор и правоприлагането по отношение финансови субекти, обхванати от Регламент (ЕС) 2022/2554. Същевременно е от значение да се поддържат тясна връзка и обмен на информация с финансовия сектор съгласно настоящата директива. За тази цел Регламент (ЕС) 2022/2554 позволява на Европейските надзорни органи (ЕНО) и компетентните органи съгласно посочения регламент да участват в дейностите на групата за сътрудничество, както и да обменят информация и да сътрудничат с единните звена за контакт, както и с ЕРИКС и компетентните органи съгласно настоящата директива. Компетентните органи съгласно Регламент (ЕС) 2022/2554 следва също да предоставят подробности за съществени инциденти с ИКТ и, когато е целесъобразно, значителни киберзаплахи на

([10]) 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 (вж. страница 1 от настоящия брой на Официален вестник).

ЕРИКС, на компетентните органи или на единните звена за контакт съгласно настоящата директива. Това е постижимо чрез осигуряване на незабавен достъп до уведомленията за инциденти и препращането им, пряко или чрез единна входяща точка. Освен това държавите членки следва да продължат да включват финансовия сектор в своите стратегии за киберсигурност, а дейностите на ЕРИКС могат да обхващат и него.

(29) За да се избегнат пропуски и дублиране на задълженията в областта на киберсигурността, наложени на субектите в сектора на въздухоплаването, националните органи, определени съгласно регламенти (ЕО) № 300/2008 ([11]) и (ЕС) 2018/1139 ([12]) на Европейския парламент и на Съвета, и компетентните органи съгласно настоящата директива следва да си сътрудничат във връзка с прилагането на мерките за управление на риска в областта на киберсигурността и надзора на съответствието с тези мерки на национално равнище. Спазването от страна на даден субект на изискванията за сигурност, определени в регламенти (ЕО) № 300/2008 и (ЕС) 2018/1139 и в съответните делегирани актове и актове за изпълнение, приети съгласно тези регламенти, може да се счита от компетентните органи съгласно настоящата директива като отговарящо на съответните изисквания, определени в настоящата директива.

(30) С оглед на взаимовръзките между киберсигурността и физическата сигурност на субектите следва да се осигури съгласуван подход между Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета ([13]) и настоящата директива. За постигането на тази цел субектите, които са установени като критични субекти съгласно Директива (ЕС) 2022/2557 следва да се считат за съществени субекти съгласно настоящата директива. Освен това всяка държава членка следва да гарантира, че националните ѝ стратегия за киберсигурност предвижда рамка на политика за засилена координация в рамките на тази държава членка между компетентните ѝ органи съгласно настоящата директива и тези съгласно Директива (ЕС) 2022/2557 в контекста на обмена на информация относно рискове, киберзаплахи и инциденти, както и относно несвързани с киберпространството рискове, заплахи и инциденти, и упражняването на надзорни задачи. Компетентните органи съгласно настоящата директива и Директива (ЕС) 2022/2557 следва да си сътрудничат и да обменят информация без ненужно забавяне, по-специално във връзка с установяването на критични субекти, рискове, киберзаплахи и инциденти, както и несвързани с киберпространството рискове, заплахи и инциденти, засягащи критичните субекти, включително мерките за киберсигурност и физическите мерки, предприети от критичните субекти, и резултатите от надзорните дейности, извършени по отношение на тези субекти.

Освен това, за да се рационализират надзорните дейности между компетентните органи съгласно настоящата директива и Директива (ЕС) 2022/2557, и за да се сведе до минимум административната тежест за засегнатите субекти, тези компетентни органи следва да се стремят да хармонизират образците за уведомяване за инциденти и надзорните процеси. Когато е целесъобразно, компетентните органи съгласно Директива (ЕС) 2022/2557 следва да могат да поискат от компетентните органи съгласно настоящата директива да упражняват своите надзорни и правоприлагащи правомощия във връзка със субект, който също така е установен като критичен субект съгласно Директива (ЕС) 2022/2557. За целта компетентните органи съгласно настоящата директива и Директива (ЕС) 2022/2557 следва да си сътрудничат и да обменят информация по възможност в реално време.

(31) Субектите, принадлежащи към сектора на цифровата инфраструктура, по същество се основават на мрежови и информационни системи и поради това задълженията, наложени на тези субекти съгласно настоящата директива, следва да третират по всеобхватен начин физическата сигурност на тези системи като част от техните мерки за управление на риска в областта на киберсигурността и задължения за докладване. Тъй като тези въпроси са обхванати от настоящата директива, задълженията, предвидени в глави III, IV и VI от Директива (ЕС) 2022/2557, не се прилагат за такива субекти.

([11]) 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, 9.4.2008 г., стр. 72).

([12]) Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета от 4 юли 2018 г. относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за изменение на регламенти (ЕО) № 2111/2005, (ЕО) № 1008/2008, (ЕС) № 996/2010, (ЕС) № 376/2014 и на директиви 2014/30/ЕС и 2014/53/ЕС на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 552/2004 и (ЕО) № 216/2008 на Европейския парламент и на Съвета и Регламент (ЕИО) № 3922/91 на Съвета (ОВ L 212, 22.8.2018 г., стр. 1).

([13]) Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. относно устойчивостта на критични субекти и за отмяна на Директива 2008/114/ЕО (вж. страница 164 от настоящия брой на Официален вестник).

(32) Поддържането и запазването на надеждна, устойчива и сигурна система за имена на домейни (DNS) са ключови фактори за запазването на целостта на интернет и са от съществено значение за неговото непрекъснато и стабилно функциониране, от което зависят цифровата икономика и обществото. Ето защо настоящата директива следва да се прилага за регистри за имена на домейни от първо ниво (TLD) и доставчици на DNS услуги, които трябва да се разбират като субекти, предоставящи публично достъпни рекурсивни услуги за преобразуване на имена на домейни за крайни интернет ползватели или услуги за овластено преобразуване на имена на домейни за използване от трета страна. Настоящата директива следва да не се прилага за базови сървъри за имена на домейни.

(33) Компютърните услуги „в облак“ следва да обхващат цифрови услуги, които дават 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. Компютърните ресурси включват ресурси като мрежи, сървъри или друга инфраструктура, операционни системи, софтуер, средства за съхранение, приложения и услуги. Моделите на услугите за изчисления в облак включват, наред с другото, инфраструктура като услуга (IaaS), платформа като услуга (PaaS), софтуер като услуга (SaaS) и мрежа като услуга (NaaS). Моделите на внедряване на компютърни услуги „в облак“ следва да включват частен, общностен, публичен и хибриден облак. Моделите за предоставяне и внедряване на компютърни услуги „в облак“ имат същото значение като условията за ползване и моделите на внедряване, определени съгласно стандарта ISO/IEC 17788:2014. Възможността потребителят на компютърни услуги „в облак“ едностранно и самостоятелно да си набавя компютърен капацитет, като например сървърно време или мрежово хранилище, без каквато и да е човешка намеса от страна на доставчика на компютърни услуги „в облак“, може да се опише като администриране при поискване.

Понятието „широк отдалечен достъп“ се използва, за да се опише, че услугите „в облак“ се предоставят в мрежата и достъпът до тях се осъществява чрез механизми, насърчаващи използването на разнородни платформи с „тънки“ и „дебели“ клиенти, включително мобилни телефони, таблети, лаптопи и работни станции. Понятието „променлив по мащаб“ означава, че компютърните ресурси се предоставят гъвкаво от доставчиците на компютърни услуги „в облак“, независимо от географското местоположение на ресурсите, за да бъдат отразени промените в търсенето. Понятието „еластичен набор“ се използва за описание на компютърните ресурси, които се предоставят и използват в зависимост от търсенето, за да може бързо да се увеличават или намаляват ресурсите, които са на разположение, в зависимост от работното натоварване. Изразът „които могат да бъдат ползвани съвместно“ се използва за описание на компютърните ресурси, които се предоставят на множество ползватели, които имат общ достъп до услугата, но обработването се извършва отделно за всеки ползвател, въпреки че услугата се предоставя от едно и също електронно оборудване. Понятието „разпределен“ се използва, за да се опишат компютърни ресурси, които са разположени на различни свързани в мрежа компютри или устройства и които осъществяват комуникация и координация помежду си посредством съобщения.

(34) Предвид възникването на новаторски технологии и нови бизнес модели се очаква на вътрешния пазар да се появят нови модели за предоставяне и внедряване на компютърни услуги „в облак“ в отговор на развиващите се потребителски нужди. В този контекст компютърните услуги „в облак“ могат да се предоставят под формата на силно „разпределени“ услуги, които се извършват още по-близо до мястото на генериране и събиране на данните, като по този начин техният традиционен модел ще бъде заменен от модел с висока степен на разпределеност („периферни изчисления“).

(35) Услугите, предлагани от доставчиците на услуги на центрове за данни, невинаги могат да бъдат предоставяни под формата на компютърна услуга „в облак“. Следователно центровете за данни невинаги съставляват част от инфраструктурата на компютърни услуги „в облак“. За да бъдат обхванати всички рискове за сигурността на мрежовите и информационните системи, настоящата директива следва съответно да обхваща също доставчици на услуги, специфични за центровете за данни, които не са компютърни услуги „в облак“. За целите на настоящата директива понятието „услуга на център за данни“ следва да обхваща предоставянето на услуга, включващо конструкции или групи конструкции, предназначени за централизирано разполагане, свързване и експлоатация на информационно и мрежово технологично оборудване, предоставящо услуги за съхранение, обработване и пренос на данни, заедно с всички съоръжения и инфраструктурата за електроразпределение и контрол на околната среда. Понятието „услуга на център за данни“ следва да не се прилага по отношение на вътрешни корпоративни центрове за данни, притежавани и използвани от съответния субект за собствени цели.

(36) Научноизследователските дейности играят ключова роля в разработването на нови продукти и процеси. Много от тези дейности се извършват от субекти, които споделят, разпространяват или използват резултатите от своите научни изследвания за търговски цели. Следователно тези субекти могат да бъдат важни участници във веригите за създаване на стойност, което превръща сигурността на техните мрежови и информационни системи в неразделна част от цялостната киберсигурност на вътрешния пазар. Научноизследователските организации следва да се разбират като включващи субекти, които съсредоточават основната част от дейността си върху извършването на приложна

научноизследователска или развойна дейност по смисъла на методическо ръководство „Фраскати“ на Организацията за икономическо сътрудничество и развитие от 2015 г.: Насоки за събиране и докладване на данни относно научните изследвания и експерименталното развитие, с цел използването на резултатите от тях за търговски цели, като например производството или разработването на продукт или процес, предоставянето на услуга и предлагането им на пазара.

(37) Нарастващата взаимозависимост е резултат от нарастващия трансграничен и взаимообвързан характер на мрежата за доставка на услуги, използваща ключови инфраструктури в целия Съюз в сектори като енергетика, транспорт, цифрова инфраструктура, питейна вода и отпадъчна вода, здравеопазване, някои аспекти на публичната администрация, както и космическото пространство, доколкото става въпрос за предоставянето на определени услуги, зависещи от наземни инфраструктури, притежавани, управлявани и използвани от държавите членки или от частноправни субекти, т.е. без инфраструктурите, притежавани, управлявани и използвани от Съюза или от негово име като част от космическата му програма. Тази взаимозависимост означава, че всяко смущение, дори и такова, което първоначално се свежда до един субект или сектор, може да има стъпаловидни ефекти в по-широк план, потенциално водещи до широкообхватни и трайни отрицателни последствия за доставката на услуги на вътрешния пазар. Засилените кибератаки по време на пандемията от COVID-19 показаха колко са уязвими нашите все по-взаимозависими общества за рискове с ниска вероятност.

(38) С оглед на различията в националните структури на управление и с цел да се запазят вече съществуващи секторни правила или надзорни и регулаторни органи на Съюза, държавите членки следва да могат да определят или създават един или повече компетентни органи, отговарящи за киберсигурността и за надзорните задачи съгласно настоящата директива.

(39) За да се улесни трансграничното сътрудничество и комуникация сред органите и да се осигури възможност за ефективно изпълнение на настоящата директива, е необходимо всяка държава членка да определи единно звено за контакт, което да отговаря за координацията на въпросите, свързани със сигурността на мрежовите и информационните системи, и за трансграничното сътрудничество на равнището на Съюза.

(40) Единните звена за контакт следва да гарантират ефективно трансгранично сътрудничество със съответните органи на други държави членки и когато е целесъобразно, с Комисията и ENISA. Поради това на единните звена за контакт следва да се възложи задачата да предават уведомленията за значителни инциденти с трансгранично въздействие на единните звена за контакт на други засегнати държави членки, по искане на ЕРИКС или на компетентния орган. На национално равнище единните звена за контакт следва да дават възможност за безпроблемно междусекторно сътрудничество с други компетентни органи. Единните звена за контакт могат да са и адресатите за относима информация за инциденти, засягащи финансови субекти, постъпваща от компетентните органи съгласно Регламент (ЕС) 2022/2554, която те следва при необходимост да могат да препращат на ЕРИКС или на компетентните органи съгласно настоящата директива.

(41) Държавите членки следва да разполагат с достатъчно технически и организационен капацитет, за да предотвратяват и идентифицират инцидентите и рисковете, да реагират на тях и да се възстановяват от тях, както и да смекчават въздействието им. Ето защо държавите членки следва да определят или посочат един или повече ЕРИКС съгласно настоящата директива и да гарантират, че те разполагат с подходящи ресурси и технически възможности. ЕРИКС следва да отговарят на изискванията, определени в настоящата директива, за да се гарантират ефективни и съвместими способности за справяне с инциденти и рискове и да се осигури ефективно сътрудничество на равнището на Съюза. Държавите членки следва да могат да определят като ЕРИКС и съществуващи екипи за незабавно реагиране при компютърни инциденти („CERT“). С цел да се подобри връзката на доверие между субектите и ЕРИКС, когато ЕРИКС е част от компетентния орган, държавите членки следва да могат да обмислят функционалното разделение между изпълняваните от ЕРИКС оперативни задачи, особено свързаните с обмена на информация и оказването на подкрепа за субектите, и надзорните дейности на компетентните органи.

(42) На ЕРИКС са възложени действията при инцидент. Това включва обработването на големи обеми от понякога чувствителни данни. Държавите членки следва да гарантират, че ЕРИКС разполагат с инфраструктура за обмен и обработка на информация, както и с добре оборудван персонал, което гарантира поверителността и надеждността на техните операции. ЕРИКС биха могли също така да приемат кодекси за поведение в това отношение.

(43) По отношение на личните данни ЕРИКС следва да могат да предоставят, в съответствие с Регламент (ЕС) 2016/679, при поискване от страна на съществен или важен субект, активно сканиране на мрежовите и информационните системи, използвани за предоставянето на услугите на субекта. Когато е приложимо, държавите членки следва да имат за цел да гарантират еднакво равнище на технически възможности за всички секторни ЕРИКС. Държавите членки следва да могат да поискат помощ от ENISA при създаването на своите ЕРИКС.

(44) ЕРИКС следва да имат способността по искане на даден съществен или важен субект да наблюдават свързаните с интернет активи както в помещенията, така и извън тях, за да установят, разберат и управляват цялостните организационни рискове на субекта по отношение на новоустановени нарушения на сигурността по веригата на доставки или критични уязвимости. Субектът следва да бъде насърчаван да съобщава на ЕРИКС дали поддържа привилегирован интерфейс за управление, тъй като това би могло да повлияе на бързината на предприемане на действия за смекчаване на последиците.

(45) Предвид значението на международното сътрудничество в областта на киберсигурността, ЕРИКС следва да имат възможността да участват в мрежите за международно сътрудничество в допълнение към участието им в мрежата на ЕРИКС, създадена с настоящата директива. Поради това за целите на изпълнението на своите задачи ЕРИКС и компетентните органи следва да могат да обменят информация, включително лични данни, с националните екипи за реагиране при инциденти с компютърната сигурност или компетентните органи на трети държави, при условие че са изпълнени условията съгласно правото на Съюза в областта на защитата на данните за предаването на лични данни на трети държави, наред с другото, тези по член 49 от Регламент (ЕС) 2016/679.

(46) От съществено значение е осигуряването на подходящи ресурси за постигане на целите на настоящата директива и осигуряването на възможност за компетентните органи и ЕРИКС за изпълнение на задачите, установени в нея. Държавите членки могат да въведат на национално равнище механизъм за финансиране за покриване на необходимите разходи във връзка с изпълнението на задачите на публичните субекти, отговарящи за киберсигурността в държавата членка съгласно настоящата директива. Този механизъм следва да е в съответствие с правото на Съюза, да бъде пропорционален и недискриминационен и да отчита различните подходи за предоставяне на сигурни услуги.

(47) Мрежата на ЕРИКС следва да продължи да допринася за укрепване на доверието и да насърчава бързото и ефективно оперативно сътрудничество между държавите членки. За да се засили оперативното сътрудничество на равнището на Съюза, мрежата на ЕРИКС следва да обмисли възможността да покани органи и агенции на Съюза, участващи в политиката в областта на киберсигурността, като например Европол, да участват в нейната работа.

(48) С цел постигане и поддържане на високо ниво на киберсигурност националните стратегии за киберсигурност, изисквани съгласно настоящата директива, следва да се състоят от съгласувани рамки, в които се определят стратегически цели и приоритети в областта на киберсигурността, както и управлението за тяхното постигане. Тези стратегии може да се състоят от един или повече законодателни или незаконодателни инструменти.

(49) Политиките за киберхигиена осигуряват основите за защита на инфраструктурите на мрежовите и информационните системи, хардуера, софтуера и сигурността на онлайн приложенията и данните за бизнеса или крайните ползватели, на които разчитат субектите. Политиките за киберхигиена, съдържащи общ набор от основни практики, включително актуализации на софтуера и хардуера, промени в паролата, управление на нови инсталации, ограничаване на профилите за достъп на ниво администратор и създаване на резервни копия на данни, позволяват проактивна рамка за готовност и цялостната безопасност и сигурност в случай на инциденти или киберзаплахи. ENISA следва да наблюдава и анализира политиките на държавите членки в областта на киберхигиената.

(50) Осведомеността в областта на киберсигурността и киберхигиената са от съществено значение за повишаване на равнището на киберсигурност в рамките на Съюза, по-специално с оглед на нарастващия брой свързани устройства, които все по-често се използват при кибератаки. Следва да се положат усилия за повишаване на цялостната осведоменост за рисковете, свързани с такива устройства, докато оценките на равнището на Съюза биха могли да спомогнат за гарантиране на общо разбиране на тези рискове в рамките на вътрешния пазар.

(51) Държавите членки следва да насърчават използването на всяка иновативна технология, включително изкуствен интелект, чието използване би могло да подобри откриването и предотвратяването на кибератаки, като даде възможност за по-ефективно използване на ресурси спрямо кибератаки. Поради това държавите членки следва да насърчават в своята национална стратегия за киберсигурност дейности в областта на научноизследователската и развойната дейност, за да се улесни използването на такива технологии, по-специално тези, свързани с автоматизирани или полуавтоматизирани инструменти в областта на киберсигурността, и когато е целесъобразно, споделянето на данни, необходими за обучението на потребителите на такива технологии и за подобряването им. Използването на всяка иновативна технология, включително изкуствен интелект, следва да бъде в съответствие с правото на Съюза в областта на защитата на данните, включително принципите на защитата на данните – точност, свеждане на данните до минимум, справедливост и прозрачност, както и сигурността на данните, като например най-съвременно криптиране. Изискванията за защита на данните на етапа на проектирането и по подразбиране, определени в Регламент (ЕС) 2016/679, следва да се спазват напълно.

(52) Инструментите и приложенията за киберсигурност с отворен код могат да допринасят за по-висока степен на откритост и да имат положително въздействие върху ефективността на индустриалните иновации. Отворените стандарти улесняват оперативната съвместимост между инструментите за сигурност и са от полза за сигурността на заинтересованите страни от промишлеността. Инструментите и приложенията за киберсигурност с отворен код могат да привлекат вниманието на по-широката общност на разработчиците, което ще позволи диверсификация на доставчиците. Отвореният код може да доведе до по-прозрачен процес на проверка на инструментите, свързани с киберсигурността, и процес на откриване на уязвимости, обусловен от общността. Поради това държавите членки следва да могат да насърчават използването на софтуер с отворен код и отворени стандарти чрез провеждане на политики, свързани с използването на свободно достъпни данни и отворен код като част от сигурността чрез прозрачност. Политиките за насърчаване на въвеждането и устойчивото използване на инструменти за киберсигурност с отворен код са от особено значение за малките и средните предприятия, изправени пред значителни разходи за изпълнение, които биха могли да бъдат сведени до минимум чрез намаляване на необходимостта от специфични приложения или инструменти.

(53) Комуналните услуги все повече се свързват с цифровите мрежи в градовете с цел подобряване на градските транспортни мрежи, подобряване на водоснабдяването и съоръженията за обезвреждане на отпадъци и повишаване на ефективността на осветлението и отоплението на сградите. Тези цифровизирани комунални услуги са уязвими на кибератаки и поради своята взаимосвързаност съществува опасност в случай на успешна кибератака да се навреди сериозно на гражданите. Държавите членки следва да разработят политика, насочена към развитието на такива свързани или интелигентни градове и тяхното потенциално въздействие върху обществото, като част от своята национална стратегия за киберсигурност.

(54) През последните години Съюзът е изправен пред експоненциално увеличение на атаките със софтуер за изнудване, при които зловредният софтуер криптира данни и системи и изисква откуп за освобождаване. Нарастващата честота и сериозност на атаките със софтуер за изнудване може да се дължи на няколко фактора, като например различни модели на атака, престъпни бизнес модели около „софтуера за изнудване като услуга“ и криптовалутите, изисквания за откуп и увеличаване на атаките по веригата на доставки. Като част от своята национална стратегия за киберсигурност държавите членки следва да развиват политика, насочена към справяне с нарастващия брой атаки със софтуер за изнудване.

(55) Публично-частните партньорства (ПЧП) в областта на киберсигурността могат да осигурят подходяща рамка за обмен на знания, споделяне на най-добри практики и установяване на общо равнище на разбиране между всички заинтересовани страни. Държавите членки следва да насърчават политиките, подкрепящи установяването на ПЧП, специфични за киберсигурността. Тези политики следва да изяснят, наред с другото, обхвата и участващите заинтересовани страни, модела на управление, наличните възможности за финансиране и взаимодействието между участващите заинтересовани страни, що се отнася до ПЧП. ПЧП могат да използват експертния опит на субектите от частния сектор, за да съдействат на компетентните органи при разработването на съвременни услуги и процеси, включително обмен на информация, ранни предупреждения, упражнения с киберзаплахи и инциденти, управление на кризи и планиране на устойчивост.

(56) В своите национални стратегии относно киберсигурността държавите членки следва да обърнат внимание на специфичните потребности на малките и средните предприятия в областта на киберсигурността. В целия Съюз малките и средните предприятия представляват голям дял от промишления и бизнес пазар и често се борят да се приспособят към новите бизнес практики в един по-свързан свят и към цифровата среда, със служители, работещи от дома, и с дейност, която все повече се извършва онлайн. Някои малки и средни предприятия са изправени пред специфични предизвикателства, свързани с киберсигурността, като например ниското ниво на осведоменост в областта на киберсигурността, липсата на ИТ сигурност от разстояние, високите разходи за решения в областта на киберсигурността и повишеното равнище на заплаха, като например софтуер за изнудване, за което следва да получават насоки и подкрепа. Малките и средните предприятия все повече се превръщат в обект на атаки по веригата на доставки поради не толкова строгите си мерки за управление на риска в областта на киберсигурността, и за управление на атаки, както и поради ограничените си ресурси за сигурност. Подобни атаки по веригата на доставки не само оказват въздействие върху малките и средните предприятия и техните отделни операции, но могат да имат и

каскаден ефект върху по-големи атаки срещу субекти, на които те са били доставчици. Чрез своите национални стратегии за киберсигурност държавите членки следва да помагат на малките и средните предприятия да се справят с предизвикателствата, пред които са изправени техните вериги на доставки. Държавите членки следва да имат звено за контакт за малките и средните предприятия на национално или регионално равнище, което или предоставя насоки и помощ на малките и средните предприятия, или ги насочва към съответните органи за насоки и съдействие по въпроси, свързани с киберсигурността. Държавите членки се насърчават също така да предлагат услуги, като конфигуриране на уебсайтове и регистриране, на микропредприятията и малките предприятия, които не разполагат с такива възможности.

(57) В рамките на своите национални стратегии за киберсигурност държавите членки следва да приемат политики за насърчаване на активната киберзащита като част от по-широка отбранителна стратегия. Вместо да се реагира, активната киберзащита се състои от превенция, откриване, наблюдение, анализ и смекчаване на нарушенията на сигурността на мрежата по активен начин, в съчетание с използването на способности, разположени във и извън мрежата, която е жертва на кибератаката. Това може да включва предоставяне от страна на държавите членки на безплатни услуги или инструменти за някои субекти, включително проверки на самообслужване, инструменти за откриване и услуги по отстраняване. Способността за бързо и автоматично споделяне и разбиране на информация и анализ на заплахи, предупрежденията за кибердейности и действията за реагиране са от решаващо значение за осигуряване на единство на усилията за успешно предотвратяване, откриване, противодействие и блокиране на атаки срещу мрежови и информационни системи. Активната киберзащита се основава на отбранителна стратегия, която изключва офанзивни мерки.

(58) Тъй като злонамереното използване на уязвимостите в мрежовите и информационните системи може да причини значителни смущения и вреди, бързото установяване и отстраняване на такива уязвимости е важен фактор за намаляване на риска. Затова субектите, които изграждат или администрират мрежови и информационни системи, следва да установят подходящи процедури за справяне с уязвимостите, които са открити. Тъй като уязвимостите често се откриват и оповестяват от трети страни, производителят или доставчикът на ИКТ продукти или ИКТ услуги следва да въведе и необходимите процедури за получаване на информация за уязвимости от трети страни. В това отношение международните стандарти ISO/IEC 30111 и ISO/IEC 29147 предоставят насоки за справянето с уязвимости и за тяхното оповестяване. От особено значение е засилването на координацията между докладващите физически и юридически лица и производителите или доставчиците на ИКТ продукти или ИКТ услуги, за да се улесни доброволната рамка за оповестяване на уязвимости. С координираното оповестяване на уязвимостите се определя структуриран процес, чрез който уязвимостите се докладват на производителя или доставчика на потенциално уязвимите ИКТ продукти или ИКТ услуги по начин, позволяващ му да диагностицира и отстрани уязвимостта преди разкриването на подробна информация за нея на трети страни или на обществеността. Координираното оповестяване на уязвимостите следва да включва и координиране между докладващото физическо или юридическо лице и производителя или доставчика на потенциално уязвимите ИКТ продукти или ИКТ услуги по отношение на графика за отстраняване и публикуване на уязвимостите.

(59) Комисията, ENISA и държавите членки следва да продължат да насърчават привеждането в съответствие с международните стандарти и съществуващите най-добри практики в сектора в областта на управлението на риска в областта на киберсигурността, например в областта на оценките на сигурността на веригата на доставки, обмена на информация и разкриването на уязвимости.

(60) Държавите членки, в сътрудничество с ENISA, следва да предприемат мерки за улесняване на координираното оповестяване на уязвимостите, като установят съответна национална политика. Като част от националната си политика държавите членки следва да се стремят да вземат мерки, доколкото е възможно, срещу предизвикателствата, пред които са изправени изследователите в областта на уязвимостта, включително потенциалната опасност да им бъде търсена наказателна отговорност, в съответствие с националното право. Като се има предвид, че физическите и юридическите лица, които изследват уязвимости, биха могли в някои държави членки да бъдат изложени на наказателна и гражданска отговорност, държавите членки се насърчават да приемат насоки по отношение на липсата на наказателно преследване на изследователите в областта на информационната сигурност и освобождаването от гражданска отговорност за тези дейности.

(61) Държавите членки следва да определят един от своите ЕРИКС като „координатор“, при необходимост действащ като доверен посредник между докладващите физически или юридически лица и производителите или доставчиците на ИКТ продукти или ИКТ услуги, които е вероятно да бъдат засегнати от уязвимостта. Задачите на определения за координатор ЕРИКС следва да включват идентифициране и установяване на контакт със засегнатите субекти, подпомагане на физическите или юридическите лица, докладващи за уязвимост, договаряне на срокове за оповестяване и управление на уязвимостите, които засягат множество субекти (многостранно координирано

оповестяване на уязвимостите). Когато докладваната уязвимост би могла да окаже значително въздействие върху субекти в повече от една държава членка, определените за координатори ЕРИКС следва да си сътрудничат в рамките мрежата на ЕРИКС, когато е целесъобразно.

(62) Достъпът до вярна и своевременна информация относно уязвимостите, засягащи ИКТ продукти и ИКТ услуги, допринася за подобрено управление на риска в областта на киберсигурността. Източниците на публично достъпна информация относно уязвимостите са важен инструмент за субектите и ползвателите на техните услуги, но също и за компетентните органи и ЕРИКС. Поради тази причина ENISA следва да създаде европейска база данни за уязвимостите, където субектите, независимо дали попадат в обхвата на настоящата директива, и техните доставчици на мрежови и информационни системи, както и компетентните органи и ЕРИКС, да могат доброволно да разкриват и регистрират публично известни уязвимости с цел да се даде възможност на ползвателите да предприемат подходящи смекчаващи мерки. Целта на тази база данни е да се отговори на единствените по рода си предизвикателства, породени от рисковете за субекти на Съюза. Освен това ENISA следва да установи подходяща процедура по отношение на процеса на публикуване, за да даде на субектите време да предприемат мерки за смекчаване на своята уязвимост и да използват най-съвременните мерки за управление на риска в областта на киберсигурността както и машинночетими набори от данни и съответните интерфейси. За да се насърчи културата на разкриване на уязвимости, разкриването не следва да има неблагоприятни последици за докладващото физическо или юридическо лице.

(63) При все че подобни регистри или бази данни за уязвимости съществуват, те се предоставят и поддържат от установени извън Съюза субекти. Една поддържана от ENISA Европейска база данни за уязвимостите би осигурила повишена прозрачност относно процеса на публикуване преди официалното разкриване на уязвимостта, както и устойчивост в случаи на смущение или прекъсване на предоставянето на подобни услуги. За да се избегне дублиране на усилията и да се постигне взаимно допълване доколкото е възможно, ENISA следва да разгледа възможността за сключване на споразумения за структурирано сътрудничество с подобни регистри или бази данни, които попадат под юрисдикцията на трети държави. По-специално ENISA следва да проучи възможността за тясно сътрудничество с операторите на системата за общи уязвимости и експозиции (CVE).

(64) Групата за сътрудничество следва да подкрепя и улеснява стратегическото сътрудничество и обмена на информация, както и изграждането на доверие между държавите членки. Групата за сътрудничество следва да съставя работна програма на всеки две години. Работната програма следва да включва действията, които групата за сътрудничество да предприема за изпълнение на своите цели и задачи. Времевата рамка за изготвяне на първата работна програма съгласно настоящата директива следва да е синхронизирана с времевата рамка на последната работна програма, изготвена съгласно Директива (ЕС) 2016/1148, за да се избегнат потенциални смущения в работата на групата за сътрудничество.

(65) При разработването на документите с насоки групата за сътрудничество следва постоянно да картографира националните решения и опит, да извършва оценка на въздействието на резултатите от своята работа върху националните подходи, да обсъжда предизвикателствата при изпълнението и да формулира конкретни препоръки, в частност относно улесняване на съгласуването между държавите членки във връзка с транспониране на настоящата директива, като тези препоръки трябва да се следват посредством по-доброто прилагане на съществуващите правила. Групата за сътрудничество би могла също така да картографира решенията на национално равнище, за да насърчава съвместимостта на решенията в областта на киберсигурността, прилагани във всеки конкретен сектор в Съюза. Това е приложимо в особена степен за секторите, които имат международен или трансграничен характер.

(66) Групата за сътрудничество следва да остане гъвкав форум и да може да реагира на променящите се и новите приоритети на политиките и предизвикателствата пред тях, като същевременно взема предвид наличността на ресурсите. Тя би могла да организира редовни съвместни заседания с относимите частни заинтересовани страни от Съюза с цел обсъждане на дейностите, извършвани от групата за сътрудничество, и събиране на данни и информация относно възникващите предизвикателства пред политиките. Освен това групата за сътрудничество следва да извършва редовно оценка на актуалното състояние на киберзаплахите или инцидентите, като например софтуера за изнудване. С цел подобряване на сътрудничество на равнището на Съюза групата за сътрудничество следва да разгледа възможността да покани съответните работещи в областта на политиките за киберсигурност институции, органи,

служби и агенции на Съюза, като например Европейския парламент, Европол, Европейския комитет по защита на данните, Агенцията за авиационна безопасност на Европейския съюз, създадена с Регламент (ЕС) 2018/1139, и Агенцията на Европейския съюз за космическата програма, създадена с Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета ([14]), да участват в нейната работа.

(67) Компетентните органи и ЕРИКС следва да могат да участват в схеми за обмен на длъжностни лица от други държави членки в рамките на конкретна рамка и където е приложимо, при спазване на изискването за надеждност на служители, участващи в такива схеми за обмен, с цел подобряване на сътрудничеството и укрепване на доверието между държавите членки. Компетентните органи следва да предприемат необходимите мерки, за да дадат възможност на длъжностните лица от други държави членки да играят ефективна роля в действията на приемащия компетентен орган или приемащия ЕРИКС.

(68) Държавите членки следва да допринасят за създаването на Механизма на ЕС за реакция при кризи в областта на киберсигурността, предвиден в Препоръка (ЕС) 2017/1584 на Комисията ([15]), посредством съществуващите мрежи за сътрудничество, особено Европейската мрежа на организациите за връзка при киберкризи (EU-CyCLONe), мрежата на ЕРИКС и групата за сътрудничество. EU-CyCLONe и мрежата на ЕРИКС следва да си сътрудничат въз основа на процедурни правила, определящи реда и условията на това сътрудничество, и да избягват всякакво дублиране на задачите. В процедурния правилник на EU-CyCLONe следва допълнително да бъдат посочени редът и условията, при които следва да функционира мрежата, включително ролите на мрежите, средствата на сътрудничество, взаимодействията с други относими действащи лица и образците за обмена на информация, както и средствата за комуникация. При управлението на кризи на равнището на Съюза съответните страни следва да се основават на интегрираните договорености на ЕС за реакция на политическо равнище при кризи съгласно Решение за изпълнение (ЕС) 2018/1993 на Съвета ([16]) (договорености IPCR). За целта Комисията следва да използва процеса ARGUS за многосекторна координация на кризи на високо равнище. Ако кризата засяга важно измерение на външната дейност или общата политика за сигурност и отбрана, следва да бъде активиран Механизмът за реакция при кризи на Европейската служба за външна дейност.

(69) В съответствие с приложението към Препоръка (ЕС) 2017/1584 „мащабен киберинцидент“ следва да 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. В зависимост от причината и въздействието си, мащабните киберинциденти може да се разраснат и да се превърнат в същински кризи, непозволяващи правилното функциониране на вътрешния пазар или представляващи сериозни рискове за публичната сигурност и безопасност за субектите или гражданите в няколко държави членки или в Съюза като цяло. Предвид широкомащабния обхват и в повечето случаи, трансграничния характер на такива инциденти, държавите членки и съответните институции, органи, служби и агенции на Съюза следва да си сътрудничат на техническо, оперативно и политическо равнище за правилно координиране на отговора в Съюза

(70) Мащабните киберинциденти и кризите на равнището на Съюза изискват координирани действия, за да се гарантира бърза и ефективна реакция поради високата степен на взаимозависимост между секторите и държавите членки. Наличието на устойчиви на киберзаплахи мрежови и информационни системи и наличието, поверителността и целостта на данните са от жизненоважно значение за сигурността на Съюза и за защитата на неговите граждани, предприятия и институции срещу инциденти и киберзаплахи, както и за повишаване на доверието на физическите лица и организациите в способността на Съюза да насърчава и защитава глобално, отворено, свободно, стабилно и сигурно киберпространство, основано на правата на човека, основните свободи, демокрацията и принципите на правовата държава.

([14]) Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета от 28 април 2021 г. за създаване на космическа програма на Съюза и Агенция на Европейския съюз за космическата програма и за отмяна на регламенти (ЕС) № 912/2010, (ЕС) № 1285/2013 и (ЕС) № 377/2014 и на Решение № 541/2014/ЕС (ОВ L 170, 12.5.2021 г., стр. 69).

([15]) Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

([16]) Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договорености за интегрирана реакция на ЕС при политическа криза (ОВ L 320, 17.12.2018 г., стр. 28).

(71) EU-CyCLONe следва да работи като посредник между техническото и политическото равнище по време на мащабни киберинциденти и кризи и следва да засилва сътрудничеството на оперативно равнище и да подпомага вземането на решения на политическо равнище. В сътрудничество с Комисията, като се има предвид компетентността на Комисията в областта на управлението на кризи, EU-CyCLONe следва да се основава на констатациите на мрежата на ЕРИКС и да използва собствения си капацитет за изготвяне на анализ на въздействието на мащабни киберинциденти и кризи.

(72) Кибератаките са трансгранични по своя характер и даден значителен инцидент може да наруши и увреди критичните информационни инфраструктури, от които зависи гладкото функциониране на вътрешния пазар. Препоръка (ЕС) 2017/1584 разглежда ролята на всички заинтересовани страни. Освен това Комисията отговаря, в рамките на Механизма за гражданска защита на Съюза, създаден с Решение № 1313/2013/ЕС на Европейския парламент и на Съвета ([17]), за действията за обща готовност, включително управлението на Координационния център за реагиране при извънредни ситуации и Общата система за спешна комуникация и информация, поддържането и по-нататъшното развитие на ситуационната осведоменост и капацитета за анализ, както и създаването и управлението на способности за мобилизиране и изпращане на експертни екипи в случай на искане за помощ от държава членка или трета държава. Комисията отговаря също така за предоставянето на аналитични доклади за договореностите IPCR съгласно Решение за изпълнение (ЕС) 2018/1993, включително във връзка със ситуационната осведоменост и подготвеност в областта на киберсигурността, както и за осведомеността за състоянието и реакцията при кризи в областта на селското стопанство, неблагоприятните метеорологични условия, картографирането и прогнозите за конфликти, системите за ранно предупреждение за природни бедствия, извънредни ситуации, свързани със здравето на хората, наблюдението на заразни болести, здравето на растенията, химическите инциденти, безопасността на храните и фуражите, здравето на животните, миграцията, митниците, извънредни ситуации в ядрената и радиологичната област и енергията.

(73) При необходимост 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 и мрежата на ЕРИКС, както и на EU-CyCLONe. Тези споразумения следва да гарантират интересите на Съюза и адекватна защита на данните. Това не следва да изключва правото на държавите членки да си сътрудничат с трети държави по отношение на управлението на уязвимости и управлението на рисковете, свързани с киберсигурността, улеснявайки докладването и общия обмен на информация в съответствие с правото на Съюза.

(74) С цел да се улесни ефективното прилагане на настоящата директива по отношение, наред с другото, на управлението на уязвимостите, мерките за управление на риска в областта на киберсигурността, задълженията за докладване и споразуменията за обмен на информация в областта на киберсигурността, държавите членки могат да си сътрудничат с трети държави и да предприемат дейности, които се считат за подходящи за тази цел, включително обмен на информация относно киберзаплахи, инциденти, уязвимости, средства и методи, тактики, техники и процедури, подготвеност и учения за управление на кризи в областта на киберсигурността, обучение, изграждане на доверие и структурирани споразумения за обмен на информация.

(75) Следва да се въведат партньорски проверки, за да се подпомогне извличането на поуки от споделения опит, да се укрепи взаимното доверие и да се постигне високо общо ниво на киберсигурност. Партньорските проверки могат да доведат до ценни изводи и препоръки за укрепване на цялостните способности в областта на киберсигурността, като се създаде друг функционален път за обмен на най-добри практики между държавите членки и се допринесе за повишаване на равнищата на зрялост на държавите членки в областта на киберсигурността. Освен това партньорските проверки следва да отчитат резултатите от подобни механизми, като например системата за партньорски проверки на мрежата на ЕРИКС, както и следва да добавят стойност и да избягват дублирането. Прилагането на партньорските проверки следва да не засяга законодателството на Съюза или националните закони в областта на защитата на поверителната и класифицираната информация.

(76) Групата за сътрудничество следва да създаде методология за самооценка за държавите членки, която да има за цел да обхване фактори като равнището на изпълнение на мерките за управление на риска в областта на киберсигурността и задълженията за докладване, равнището на способностите и ефективността на изпълнението на задачите на компетентните органи, оперативните способности на ЕРИКС, степента на прилагане на взаимната помощ, степента на прилагане на споразуменията за обмен на информация в областта на киберсигурността или специфични въпроси от трансгранично или междусекторно естество. Държавите членки следва да бъдат насърчавани да извършват редовни самооценки и да представят и обсъждат резултатите от своята самооценка в рамките на групата за сътрудничество.

([17]) Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

(77) Отговорността по гарантиране на сигурността на мрежовите и информационните системи принадлежи в голяма степен на съществените и важните субекти. Следва да се насърчава и развива култура на управление на риска, включваща оценките на риска и изпълнението на мерки за управление на риска в областта на киберсигурността, съобразени със съществуващите рискове.

(78) Мерките за управление на риска в областта на киберсигурността следва да отчитат степента на зависимост на съществения или важния субект от мрежовите и информационните системи и следва да включват мерки за идентифициране на всякакви рискове от инциденти с цел предотвратяване, откриване и реагиране на инциденти, както и ограничаване на тяхното въздействие. Сигурността на мрежовите и информационните системи следва да включва сигурността на данните, които се съхраняват, предават и обработват. Мерките за управление на риска в областта на киберсигурността следва да предвиждат системен анализ, при който се отчита човешкият фактор, за да се получи пълна картина на сигурността на мрежовата и информационната система.

(79) Тъй като заплахите за сигурността на мрежовите и информационните системи могат да имат различен произход, мерките за управление на риска в областта на киберсигурността следва да се основават на подход, обхващащ всички опасности, който има за цел да защити мрежовите и информационните системи и физическа среда на тези системи от събития като кражба, пожар, наводнение, телекомуникационни повреди или прекъсване на захранването, или от всякакъв неразрешен физически достъп и щети и намеса в информацията на съществения или важния субект и неговите съоръжения за обработка на информация, които биха могли да засегнат отрицателно наличността, автентичността, цялостността или поверителността на съхраняваните, пренасяните или обработваните данни или на услугите, предлагани от мрежови и информационни системи или достъпни чрез тях. Поради това мерките за управление на риска в областта на киберсигурността, следва да са насочени и към физическата сигурност и сигурността на средата на мрежовите и информационните системи като включват мерки за защита на тези системи от сривове в системата, човешка грешка, злонамерени действия или природни явления в съответствие с европейските и международните стандарти, като включените в серията ISO/IEC 27000. В това отношение, като част от своите мерки за управление на риска в областта на киберсигурността съществените и важните субекти следва също така да обърнат внимание на сигурността на човешките ресурси и да разполагат с подходящи политики за контрол на достъпа. Тези мерки следва да са съобразени с Директива(ЕС) 2022/2557.

(80) С цел доказване на спазването на мерките за управление на риска в областта на киберсигурността и при липсата на подходящи европейски схеми за сертифициране на киберсигурността, приети в съответствие с Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([18]), държавите членки следва, като се консултират с групата за сътрудничество и Европейската група за сертифициране на киберсигурността, да насърчават използването на съответните европейски и международни стандарти от съществените и важните субекти или да изискват от субектите да използват сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси.

(81) С цел да се избегне налагането на непропорционална финансова и административна тежест върху съществените и важните субекти, мерките за управление на риска в областта на киберсигурността следва да бъдат пропорционални на риска, който съществува по отношение на съответната мрежова и информационна система, като се отчитат последните достижения в областта на тези мерки и когато е приложимо, съответните европейски и международни стандарти, както и разходите за тяхното прилагане.

(82) Мерките за управление на риска в областта на киберсигурността следва да бъдат пропорционални на степента на излагане на рискове на субекта и на общественото и икономическото въздействие, което даден инцидент би оказал. При установяването на мерки за управление на риска, свързани с киберсигурността, приспособени към съществените и важните субекти, следва надлежно да се вземе предвид различната изложеност на риск на съществените и важните субекти, като например критичността на субекта, рисковете, включително обществените рискове, на които е изложен, размерът на субекта и вероятността от възникване на инциденти и тяхната сериозност, включително тяхното обществено и икономическо въздействие.

([18]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

(83) Съществените и важните субекти следва да гарантират сигурността на мрежовите и информационните системи, които използват в своите дейности. Тези системи са предимно частни мрежови и информационни системи, управлявани от вътрешен ИТ персонал на съществените и важните субекти, или такива, чиято сигурност е възложена на външни изпълнители. Мерките за управление на риска в областта на киберсигурността и задълженията за докладване, предвидени в настоящата директива, следва да се прилагат по отношение на съответните съществени и важни субекти без оглед на това дали те извършват вътрешно поддръжка на своите мрежови и информационни системи или възлагат поддръжката на външни изпълнители.

(84) Като се има предвид трансграничният им характер, за доставчиците на DNS услуги, за регистрите на имена на домейни от първо ниво, за доставчиците на компютърни услуги „в облак“, за доставчиците на услуги на центрове за данни, за доставчиците на мрежи за предоставяне на съдържание, за доставчиците на управлявани услуги, за доставчиците на управлявани услуги за сигурност, за доставчиците на онлайн места за търговия, на онлайн търсачки и на платформи на услуги за социални мрежи и за доставчиците на удостоверителни услуги следва да се прилага висока степен на хармонизация на равнището на Съюза. Поради това изпълнението на мерките за управление на риска в областта на киберсигурността по отношение на посочените субекти следва да бъде улеснено чрез акт за изпълнение.

(85) Справянето с рискове, коренящи се във веригата на доставки на даден субект и отношенията му с доставчиците, като например доставчици на услуги по съхранение или обработка на данни или доставчици на управлявани услуги за сигурност и производители на софтуер, е от особено значение предвид преобладаващия брой на инцидентите, при които субекти са били жертва на кибератаки или сигурността на техните мрежови и информационни системи бива компрометирана от злонамерени извършители чрез експлоатиране на уязвимостите, засягащи продукти и услуги на трети страни. Затова съществените и важните субекти следва да преценяват и вземат предвид цялостното качество и устойчивост на продуктите и услугите, внедрените в тях мерки за управление на риска, свързан с киберсигурността, и практиките на своите снабдители и доставчици на услуги в областта на киберсигурността, включително техните процедури за сигурно разработване. Съществените и важните субекти следва по-специално да бъдат насърчавани да включват мерки за риска в областта на киберсигурността в договорните споразумения със своите преки снабдители и доставчици на услуги. Тези субекти биха могли да вземат предвид рисковете, произтичащи от други равнища на снабдители и доставчиците на услуги.

(86) Сред доставчиците на услуги, доставчиците на управлявани услуги за сигурност в области като реагиране при инциденти, тестване за проникване, одити за сигурността и консултантски услуги, играят особено важна роля в оценката на усилията на субектите за предотвратяване, идентифициране, реагиране на инциденти или възстановяване от такива. Самите тези доставчици на управлявани услуги за сигурност обаче също са цел на кибератаки и поради тяхното тясно интегриране в дейностите на субектите пораждат особен риск за киберсигурността. Ето защо съществените и важните субекти следва да подхождат с повишено внимание към избора на доставчик на управлявани услуги за сигурност.

(87) В контекста на своите надзорни задачи компетентните органи могат също да се ползват от услуги в областта на киберсигурността, като например одити на сигурността, тестване за проникване или реагиране при инциденти.

(88) Съществените и важните субекти следва да намерят решения и за рискове, произтичащи от взаимодействията и отношенията им с други заинтересовани страни в рамките на една по-широка екосистема, включително по отношение на противодействието на индустриалния шпионаж и защитата на търговските тайни. Тези субекти по-специално следва да предприемат подходящи мерки, за да гарантират, че сътрудничеството им с академичните и научноизследователските институции е в съответствие с техните политики в областта на киберсигурността и следва добрите практики по отношение на сигурния достъп до информация и нейното разпространение като цяло, както и по-специално по отношение на защитата на интелектуалната собственост. По подобен начин, с оглед на важността и стойността на данните за дейността на съществените и важните субекти, тези субекти трябва да предприемат всички необходими мерки за управление на риска в областта на киберсигурността, когато ползват услуги на трети страни за преобразуването и анализа на данните.

(89) Съществените и важните субекти следва да възприемат широк спектър основни киберхигиенни практики като принципи на нулево доверие, софтуерни актуализации, конфигурация на устройства, сегментиране на мрежи, управление на самоличността и достъпа или повишаване на осведомеността на ползвателите, или да организират обучения на служителите и повишаване на осведомеността по отношение на киберзаплахи, фишинг или техники за социално инженерство. Освен това тези субекти следва да оценяват собствените си способности за киберсигурност и когато целесъобразно да се стремят към интеграцията на технологии за повишаване на киберсигурността, като изкуствен интелект или системи за машинно самообучение, за да повишат своите способности и сигурността на мрежовите и информационните системи.

(90) За да се отговори допълнително на рисковете по веригата на доставка и да се подпомогнат съществените и важните субекти, упражняващи дейност в обхванати от настоящата директива сектори, правилно да управляват веригата на доставка и свързаните с доставчика рискове, групата за сътрудничество, в сътрудничество с Комисията и ENISA и когато е целесъобразно след консултация със съответните заинтересовани лица, включително от промишлеността, следва да извърши координирани оценки на риска за сигурността на критични вериги за доставки, както това бе вече направено за 5G мрежите в съответствие с Препоръка (ЕС) 2019/534 на Комисията ([19]), с цел да се установи за всеки сектор кои са критичните ИКТ услуги, ИКТ системи или ИКТ продукти, относимите заплахи и уязвимости. Тези координирани оценки на риска за сигурността следва да установяват мерки, планове за смекчаване и най-добри практики за противодействие на критични зависимости, потенциални единични точки на срив, заплахи, уязвими места и други рискове, свързани с веригата на доставки, и следва да проучват начини за допълнително насърчаване на по-широкото им възприемане от съществените и важните субекти. Потенциалните нетехнически рискови фактори, например неправомерното влияние на трета държава върху снабдителите и доставчиците на услуги, по-специално в случай на алтернативни модели на управление, включват скрити уязвимости или скрити възможности за достъп и потенциални системни смущения при доставките, особено в случай на технологично закрепостяване или зависимост от доставчика.

(91) С оглед на характеристиките на съответния сектор, в координираните оценки на риска за сигурността на критичните вериги на доставки следва да се вземат предвид техническите и, когато е уместно, нетехническите фактори, включително определените в Препоръка (ЕС) 2019/534, в координираната в ЕС оценка на риска на киберсигурността на 5G мрежите и в инструментариума на ЕС за киберсигурност на 5G технологиите, договорен от групата за сътрудничество. За да се установят веригите на доставки, които следва да са предмет на координирана оценка на риска за сигурността, следва да бъдат взети предвид следните критерии: i) степента, в която съществените и важните субекти използват и разчитат на конкретни критични ИКТ услуги, ИКТ системи или ИКТ продукти; ii) значението на конкретни критични ИКТ услуги, ИКТ системи или ИКТ продукти за изпълнението на критични или чувствителни функции, включително обработването на лични данни; iii) наличието на алтернативни ИКТ услуги, ИКТ системи или ИКТ продукти; iv) устойчивостта на цялостната верига на доставки на ИКТ услуги, ИКТ системи или ИКТ продукти през целия им жизнен цикъл срещу смущаващи събития и v) за възникващи ИКТ услуги, ИКТ системи или ИКТ продукти, тяхната потенциална бъдеща значимост за дейностите на субектите. Освен това следва да се обърне специално внимание на ИКТ услугите, ИКТ системите или ИКТ продуктите, които подлежат на специфични изисквания, произтичащи от трети държави.

(92) С цел да се рационализират задълженията, наложени на доставчиците на обществени електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги и на доставчиците на удостоверителни услуги, свързани със сигурността на техните мрежови и информационни системи, както и за да се даде възможност на тези субекти и компетентните органи по Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета ([20]) и Регламент (ЕС) № 910/2014 съответно да се възползват от установената с настоящата директива правна рамка, включително определянето на ЕРИКС, отговарящ за действията при инцидент, участието на съответните компетентни органи в работата на групата за сътрудничество и мрежата на ЕРИКС, тези субекти следва да бъдат включени в обхвата на настоящата директива. Ето защо съответстващите разпоредби, предвидени в Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972, отнасящи се до налагането на мерки за сигурност и уведомяване по отношение на тези видове субекти, следва да бъдат заличени. Правилата относно задълженията за докладване, предвидени в настоящата директива, не следва да засягат Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО.

(93) Задълженията, свързани с киберсигурността, предвидени в настоящата директива, следва да се считат за допълващи изискванията, наложени на доставчиците на удостоверителни услуги съгласно Регламент (ЕС) № 910/2014. От доставчиците на удостоверителни услуги следва да се изисква да предприемат всички подходящи и пропорционални мерки за управление на рисковете за техните услуги, включително по отношение на клиентите и доверяващите се трети страни, и да докладват за инциденти съгласно настоящата директива. Тези задължения за киберсигурност и докладване следва да се отнасят и до физическата защита на предоставяните услуги. Продължават да се прилагат изискванията за доставчиците на квалифицирани удостоверителни услуги, определени в член 24 от Регламент (ЕС) № 910/2014.

([19]) Препоръка (ЕС) 2019/534 на Комисията от 26 март 2019 г. относно киберсигурността на 5G мрежите (ОВ L 88, 29.3.2019 г., стр. 42).

([20]) Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (ОВ L 321, 17.12.2018 г., стр. 36).

(94) Държавите членки могат да възложат ролята на компетентни органи за удостоверителни услуги на надзорните органи по Регламент (ЕС) № 910/2014, за да се гарантира продължаването на действащите практики и да се надгражда върху знанията и опита, придобити при прилагането на посочения регламент. В такъв случай компетентните органи съгласно настоящата директива следва да си сътрудничат тясно и своевременно с тези надзорни органи чрез обмен на съответна информация, за да се гарантира ефективен надзор и спазване от страна на доставчиците на удостоверителни услуги на изискванията, предвидени в настоящата директива и в Регламент (ЕС) № 910/2014. Когато е приложимо, ЕРИКС или компетентният орган съгласно настоящата директива следва незабавно да информира надзорния орган по Регламент (ЕС) № 910/2014 за всяка значителна киберзаплаха или киберинцидент с въздействие върху удостоверителните услуги, за която/който е подадено уведомление, както и за всяко нарушение от страна на доставчик на удостоверителни услуги на настоящата директива. За целите на докладването държавите членки могат да използват, когато е приложимо, единната входяща точка, създадена за постигане на общо и автоматично докладване на инциденти както пред надзорния орган по Регламент (ЕС) № 910/2014, така и пред ЕРИКС или компетентния орган съгласно настоящата директива.

(95) Когато е целесъобразно и за да се избегнат ненужни смущения, съществуващите национални насоки, приети за транспониране на правилата, свързани с мерките за сигурност по членове 40 и 41 от Директива (ЕС) 2018/1972, следва да се вземат предвид при транспонирането на настоящата директива, като по този начин се надгражда върху вече придобитите знания и умения съгласно Директива (ЕС) 2018/1972 относно мерките за сигурност и уведомленията за инциденти. ENISA може също така да разработи насоки относно изискванията за сигурност и задълженията за докладване за доставчиците на обществени електронни съобщителни мрежи или обществено-достъпни електронни съобщителни услуги с цел улесняване на хармонизацията и прехода и свеждането до минимум на смущенията. Държавите членки могат да възложат ролята на компетентни органи в областта на електронните съобщения на националните регулаторни органи съгласно Директива (ЕС) 2018/1972, за да се гарантира продължаването на действащите практики и да се надгражда върху знанията и опита, придобити в резултат на прилагането на посочената директива.

(96) Предвид нарастващото значение на междуличностните съобщителни услуги без номерà по смисъла на Директива (ЕС) 2018/1972 е необходимо да се гарантира, че и за тях се прилагат подходящи изисквания за сигурност с оглед на тяхната специфика и икономическо значение. Тъй като повърхностите за атаки продължават да се разширяват, междуличностни съобщителни услуги без номерà, като например услуги за изпращане на съобщения, стават популярни вектори на атака. Злонамерени извършители използват платформите с цел комуникация и привличане на жертви за отваряне на компрометирани уеб страници, поради което увеличават вероятността от инциденти, свързани с използването на лични данни, а оттам и със сигурността на мрежовите и информационните системи. Доставчиците на междуличностни съобщителни услуги без номерà следва да осигурят ниво на сигурност на мрежовите и информационните системи, съответстващо на съществуващите рискове. Като се има предвид, че доставчиците на междуличностни съобщителни услуги без номерà обикновено не упражняват действителен контрол върху преноса на сигнали по мрежи, степента на риска, на който са изложени такива услуги, в някои отношения може да се разглежда като по-ниска от тази за традиционните електронни съобщителни услуги. Същото се отнася и за междуличностните съобщителни услуги по смисъла на Директива (ЕС) 2018/1972, при които се използват номерà и не се упражнява действителен контрол върху преноса на сигнали.

(97) Вътрешният пазар разчита на функционирането на интернет повече от всякога. Услугите на почти всички съществени и важни субекти са зависими от предоставяните по интернет услуги. За да се осигури гладкото предоставяне на услуги от страна на съществените и важните субекти, от значение е всички доставчици на обществени електронни съобщителни мрежи да имат въведени подходящи мерки за управление на риска в областта на киберсигурността и да докладват за свързаните с тях значителни инциденти. Държавите членки следва да гарантират, че сигурността на обществените електронни съобщителни мрежи се поддържа и че техните жизненоважни интереси в областта на сигурността са защитени от саботаж и шпионаж. Тъй като международната свързаност подобрява и ускорява конкурентната цифровизация на Съюза и неговата икономика, инцидентите, засягащи подводни комуникационни кабели, следва да бъдат докладвани на ЕРИКС или, когато е приложимо, на компетентния орган. Националната стратегия за киберсигурност следва, когато е приложимо, да взема предвид киберсигурността на подводните комуникационни кабели и да включва картографиране на потенциалните рискове за киберсигурността и мерките за смекчаване, за да се гарантира най-високо равнище на тяхната защита.

(98) С цел да се защити сигурността на обществените електронни съобщителни мрежи и на обществено-достъпните електронни съобщителни услуги следва да се насърчава използването на технологии за криптиране, по-специално на криптиране от край до край, както и на концепции за сигурност, ориентирани към данните, като картография, сегментиране, маркиране, политика на достъп и управление на достъпа, както и автоматизирани решения за достъп. Когато е необходимо, използването на криптиране, по-специално криптиране от край до край, следва да стане задължително за доставчиците на обществени електронни съобщителни мрежи или на обществено-достъпни електронни съобщителни услуги в съответствие с принципите на сигурност и поверителност по подразбиране и на етапа на проектиране за целите на настоящата директива. Използването на криптиране от край до край следва да е съобразено с правомощията на държавите членки да гарантират защитата на своите съществени свързани със сигурността интереси и обществена сигурност, а също и да дава възможност за предотвратяване, разследване, установяване и наказателно преследване на престъпления в съответствие с правото на Съюза. Това обаче не следва да води до отслабване на криптирането от край до край, което е изключително важна технология за ефективната защита на данните, поверителността и сигурността на комуникациите.

(99) За да се гарантира сигурността и да се предотвратят злоупотреби и манипулации на обществените електронни съобщителни мрежи и на обществено-достъпните електронни съобщителни услуги, следва да се насърчава използването на сигурни стандарти за маршрутизация, за да се гарантира целостта и стабилността на функциите за маршрутизация в екосистемата на доставчиците на услуги за достъп до интернет.

(100) За да се запазят функционалността и целостта на интернет и да се насърчават сигурността и устойчивостта на DNS, съответните заинтересовани страни, включително субектите от частния сектор на Съюза, доставчиците на обществено-достъпни електронни съобщителни услуги, по-специално доставчиците на услуги за достъп до интернет и доставчиците на онлайн търсачки, следва да бъдат насърчавани да приемат стратегия за диверсификация на преобразуването на DNS. Освен това държавите членки следва да насърчават разработването и използването на публична и сигурна европейска услуга за преобразуването на DNS.

(101) С настоящата директива се определя многоетапен подход по отношение на докладването на значителни инциденти с цел да се постигне подходящ баланс между бързото докладване, което подпомага ограничаването на потенциалното разпространение на значителни инциденти и позволява на съществените и важните субекти да потърсят подкрепа, от една страна, и задълбоченото докладване, което подпомага извличането на ценни изводи от отделни инциденти и подобряването с течение на времето на киберустойчивостта на отделни субекти или цели сектори, от друга страна. В тази връзка в настоящата директива следва да се включи докладване на инциденти, които, въз основа на извършена от засегнатия субект първоначална оценка, биха могли да доведат до съществено оперативно смущение в услугите или финансови загуби за същия субект, или засягат други физически или юридически лица, причинявайки значителни материални или нематериални вреди. Такава първоначална оценка следва, наред с другото, да взема предвид засегнатите мрежови и информационни системи, по-специално тяхното значение при предоставянето на услуги от страна субекта, тежестта и техническите характеристики на киберзаплахата и всички заложени уязвимости, които се използват, както и опитът на субекта със сходни инциденти. Показатели като степента, до която е засегнато функционирането на услугата, продължителността на даден инцидент или броят на засегнатите получатели на услуги, биха могли да играят важна роля при определянето на това дали оперативното смущение в услугата е сериозно.

(102) Когато съществените и важните субекти узнаят за значителен инцидент, те трябва да подадат ранно предупреждение без ненужно забавяне, при всички положения в рамките на 24 часа. Това ранно предупреждение следва да бъде последвано от уведомление за инцидент. Съответните субекти следва да подадат уведомление за инцидент без ненужно забавяне и при всички случаи в срок от 72 часа, след като са узнали за значимия инцидент, с цел по-специално да актуализират информацията, подадена чрез ранното предупреждение, и да посочат първоначална оценка на значителния инцидент, включително неговата тежест и въздействие, както и показатели за компрометираност, когато има такива. Окончателният доклад следва да се представи не по-късно от един месец след уведомлението за инцидента. В ранното предупреждение следва да се посочва единствено информацията, която е необходима на ЕРИКС или, когато е приложимо, компетентния орган, запознат със значителния инцидент, като позволява на засегнатия субект да потърси помощ, ако е необходимо. Това ранно предупреждение, когато е приложимо, следва да посочва дали се подозира, че значителният инцидент е причинен от незаконни или злонамерени действия, и дали има вероятност той да има трансгранично въздействие. Държавите членки следва да гарантират, че задължението за подаване на това ранно предупреждение или на последващото уведомление за инцидент не отклонява ресурсите на уведомяващия субект от дейности, свързани с действия при инцидент, които следва да бъдат приоритизирани с цел да се предотврати това задълженията за докладване на инцидент да отклонят ресурси от реагирането при значителни инциденти или да компрометират по друг начин усилията на субекта в това

отношение. В случай на текущ инцидент към момента на представяне на окончателния доклад, държавите членки следва да гарантират, че засегнатите субекти представят доклад за напредъка по това време и окончателен доклад в срок от един месец от тяхната реакция при значителния инцидент.

(103) Когато е приложимо, съществените и важните субекти следва да съобщават без ненужно забавяне на получателите на техните услуги всички мерки или средства за защита, които тези получатели могат да предприемат за ограничаване на произтичащите от значителна киберзаплаха рискове. Когато е целесъобразно и по-специално когато има вероятност значителната киберзаплаха да се осъществи, тези субекти следва също така да информират получателите на техните услуги за самата заплаха. Изискването да се уведомяват тези получатели за значителни киберзаплахи следва да се изпълнява на база полагане на максимални усилия, но не следва да освобождава тези субекти от задължението да предприемат за своя сметка подходящи и незабавни мерки за предотвратяване или отстраняване на такива заплахи и да възстановят нормалното ниво на сигурност на услугата. Предоставянето на получателите на услуги на такава информация относно значителни киберзаплахи следва да бъде безплатно и формулирано на лесен за разбиране език.

(104) Доставчиците на обществени електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги следва да внедрят сигурност на етапа на проектирането и по подразбиране, и да информират получателите на техните услуги за значителни киберзаплахи и за мерките, които те могат да предприемат, за да защитят сигурността на своите устройства и съобщения, например чрез използване на специални типове софтуер или технологии за криптиране.

(105) Проактивният подход към киберзаплахите е жизненоважен компонент на управлението на риска в областта на киберсигурността, който следва да даде възможност на компетентните органи ефективно да предотвратяват материализирането на киберзаплахи в инциденти, които могат да причинят значителни материални или нематериални вреди. За тази цел уведомяването за киберзаплахи е от ключово значение. За тази цел субектите се насърчават да докладват доброволно за киберзаплахи.

(106) С цел да се опрости докладването на информация съгласно изискванията на настоящата директива, както и да се намали административната тежест за субектите, държавите членки следва да предоставят технически средства за подаване на съответната информация, която трябва да се докладва, като например единна входяща точка, автоматизирани системи, онлайн формуляри, лесни за ползване интерфейси, образци, специализирани платформи за използване от субектите, независимо дали попадат в обхвата на настоящата директива. Финансирането от Съюза в подкрепа на прилагането на настоящата директива, по-специално в рамките на програмата „Цифрова Европа“, създадена с Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета ([21]), би могло да включва подкрепа за единните входящи точки. Освен това, субектите често се оказват в положение, при което, даден инцидент трябва да бъде докладван, поради конкретните му характеристики, на различни органи в резултат на задължения за уведомяване, включени в различни правни инструменти. Подобни случаи пораждат допълнителна административна тежест и биха могли също да доведат и до несигурност с оглед на формата и процедурите на такива уведомления. Когато е създадена единна входяща точка държавите членки се насърчават също така да използват тази единна входяща точка за уведомяване за инциденти, свързани със сигурността, което се изисква съгласно други законодателни актове на Съюза, като например Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО. Използването на такава единна входяща точка за докладване на инциденти, свързани със сигурността, съгласно Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО не следва да засяга прилагането на разпоредбите на Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО, по-специално тези, свързани с независимостта на посочените в тях органи. ENISA следва, съвместно с групата за сътрудничество и посредством насоки, да разработи общи образци на уведомления с цел опростяване и оптимизиране на информацията, която трябва да се докладва съгласно правото на Съюза, и намаляване на административната тежест за уведомяващите субекти.

(107) Когато съществуват подозрения, че даден инцидент е свързан с тежки престъпления — съобразно правото на Съюза или националното право, държавите членки следва да насърчават съществените и важните субекти, на основание на приложими наказателнопроцесуални правила в съответствие с правото на Съюза, да докладват за такива инциденти на съответните правоприлагащи органи. Когато е целесъобразно и без да се засягат приложимите за Европол правила за защита на личните данни, е желателно координацията между компетентните органи и правоприлагащите органи на различни държави членки да бъде улеснявана от Европейския център за борба с киберпрестъпността (EC3) и ENISA.

([21]) Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на програмата „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240 (ОВ L 166, 11.5.2021 г., стр. 1).

(108) В много случаи вследствие на инциденти се засягат лични данни. В този контекст компетентните органи следва да си сътрудничат и да обменят информация относно всички съответни въпроси с органите, посочени в Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО.

(109) Поддържането на точни и пълни бази данни с данни за регистрация на имена на домейни („данни WHOIS“) и предоставянето на законен достъп до такива данни са от съществено значение за гарантиране на сигурността, стабилността и устойчивостта на DNS, което на свой ред допринася за по-високо ниво на киберсигурност в Съюза. За тази конкретна цел от регистрите на имена на имена на домейни от първо ниво и от субектите, предоставящи услуги за регистрация на имена на домейни, следва да се изисква да обработват определени данни, необходими за постигането на тази цел. Това обработване следва да съставлява правно задължение по смисъла на член 6, параграф 1, буква в) от Регламент (ЕС) 2016/679. Това задължение не засяга възможността за събиране на данни за регистрация на имена на домейни за други цели, например въз основа на договорни споразумения или правни изисквания, установени в друго право на Съюза или национално право. Това задължение има за цел да се постигне пълен и точен набор от регистрационни данни и не следва да води до многократно събиране на едни и същи данни. Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да си сътрудничат, за да се избегне дублирането на тази задача.

(110) Наличността и своевременната достъпност на тези данни за регистрация на имена на домейни за законно търсещите достъп лица е от съществено значение за предотвратяването и борбата със злоупотребите с DNS, както и за предотвратяването, разкриването и реагирането на инциденти. Под законно търсещи достъп лица се разбира всяко физическо или юридическо лице, което подава искане съгласно правото на Съюза или националното право. Те могат да включват органи, които са компетентни съгласно настоящата директива, и органи, които съгласно правото на Съюза или националното право са компетентни за предотвратяването, разследването, разкриването или наказателното преследване на престъпления, както и CERT или ЕРИКС. От регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да бъде изисквано да позволяват законен достъп до конкретни данни за регистрация на имена на домейни, които са необходими за целите на заявлението за достъп на законно търсещите достъп, в съответствие с правото на Съюза и националното право. Искането на законно търсещите достъп лица следва да бъде придружено от изложение на мотивите, което позволява да се прецени необходимостта от достъп до данните.

(111) За да се гарантира наличността на точни и пълни данни за регистрация на домейни, регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистриране на имена на домейни, следва да събират и гарантират целостта и наличността на данните за регистрация на име на домейни. По-специално регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистриране на имена на домейни, следва да установят политики и процедури за събиране и поддържане на точни и пълни данни за регистрация на имена на домейни, както и да предотвратяват и поправят неточни такива данни в съответствие с правото на Съюза в областта на защитата на данните. Тези политики и процедури следва да отчитат, доколкото е възможно, стандартите, разработени от многостранните структури за управление на международно равнище. Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да приемат и прилагат съразмерни процедури за проверка на данните за регистрация на имена на домейни. Тези процедури следва да отразяват най-добрите практики, използвани в сектора, и, доколкото е възможно, постигнатия напредък в областта на електронната идентификация. Примерите за процедури за проверка могат да включват предварителни проверки, извършени по време на регистрацията, и последващи проверки, извършени след регистрацията. Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва по-специално да проверят поне едно от средствата за контакт с регистранта.

(112) От регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да се изисква да правят публично достъпни данните за този вид регистрация, които са попадат извън обхвата на правото на Съюза в областта на защитата на данните, като например отнасящите се до юридическите лица данни, в съответствие с преамбюла на Регламент (ЕС) 2016/679. За юридическите лица регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да оповестяват публично най-малко името на регистранта и телефонния номер за контакт. Адресът на електронната поща за връзка също следва да бъде публикуван, при условие че не съдържа лични данни, като например в случай на псевдоними за електронна поща или функционални профили. Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да позволяват също законосъобразен достъп до конкретни данни за регистрация на имена на домейни относно физическите лица на законно търсещите достъп, в съответствие с правото на Съюза в областта на защитата на данните. Държавите членки изискват от регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, да отговарят без ненужно забавяне на искания за разкриване на данни за регистрация на имена на домейни от първо ниво от законно търсещите достъп. Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни, следва да установят политики и процедури за

публикуването и разкриването на данни за регистрация, включително клаузи за нивото на обслужване за отговаряне на искания за достъп от законно търсещите достъп. Тези политики и процедури следва да отчитат, доколкото е възможно, всякакви насоки и стандарти, разработени от многостранните структури за управление на международно равнище. Процедурите за достъп биха могли да включват и използването на интерфейс, портал или друг технически инструмент за предоставяне на ефикасна система за заявяване и получаване на достъп до данни за регистрация. С цел насърчаване на хармонизираните практики във вътрешния пазар Комисията може да предоставя насоки относно такива процедури, без да се засягат правомощията на Европейския комитет по защита на данните, които вземат предвид, доколкото е възможно, стандартите, разработени от многостранните структури за управление на международно равнище. Държавите членки следва да гарантират, че всички видове достъп до лични и неперсонални данни за регистрация на домейни са безплатни.

(113) Субектите, попадащи в обхвата на настоящата директива, следва да се считат за попадащи под юрисдикцията на държавата членка, в която са установени. Въпреки това, доставчици на обществени електронни съобщителни мрежи или доставчици на обществено достъпни електронни съобщителни услуги, следва да се счита, че попадат под юрисдикцията на държавата членка, в която предоставят своите услуги; Доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, субектите, предоставящи услуги за регистрация 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, се считат за попадащи под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Съюза. Органи на публичната администрация следва да се счита, че попадат под юрисдикцията на държавата членка, която ги е създала. Ако предоставя услуги или е установен в повече от една държава членка, даден субект следва да попада под отделните и успоредни юрисдикции на всяка от тези държави членки. Компетентните органи на тези държави членки следва да си сътрудничат, да се подпомагат взаимно и, когато е подходящо, да провеждат съвместни надзорни действия. Когато държавите членки упражняват своята юрисдикция, те не следва да налагат правоприлагащи мерки или санкции повече от веднъж за едно и също поведение в съответствие с принципа *ne bis in idem*.

(114) За да се вземе предвид трансграничният характер на услугите и операциите на доставчиците на DNS услуги, регистрите на имената на домейни от първо ниво, субектите, предоставящи услуги за регистрация 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, само една държава членка следва да има юрисдикция по отношение на тези субекти. Юрисдикцията следва да се предоставя на държавата членка, в която засегнатият субект има своето основно място на установяване в Съюза. Критерият за място на установяване за целите на настоящата директива предполага ефективно и действително упражняване на дейност въз основа на стабилни правила. Правната форма на тези договорености, независимо дали става въпрос за клон или дъщерно дружество с правосубектност, не е определящ фактор в това отношение. Изпълнението на този критерий не следва да зависи от това дали съответните мрежови и информационни системи са физически разположени на определено място; наличието и използването на тези системи не представляват сами по себе си такова основно място на установяване и следователно не са решаващ критерии за определяне на основното място на установяване. Основното място на установяване следва да се счита, че е в държавата членка, където преимуществено в Съюза се вземат решенията относно мерките за управление на риска в областта на киберсигурността. То обикновено съответства на мястото на централното управление на субектите в Съюза. Ако такава държава членка не може да бъде определена или ако такива решения не са взети в Съюза, следва да 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 следва се счита държавата членка, в която субектът се е установил с най-голям брой служители в Съюза. Когато услугите се извършват от група предприятия, основното място на установяване на контролиращото предприятие следва да се счита за основно място на установяване на групата предприятия.

(115) Когато обществено достъпна рекурсивна DNS услуга се предоставя от доставчик на обществени електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги само като част от услугата за достъп до интернет, следва да се счита, че субектът попада под юрисдикцията на всички държави членки, в които се предоставят неговите услуги.

(116) Когато 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 центрове за данни, доставчик на мрежи за предоставяне на съдържание, доставчик на управлявани услуги, доставчик на управлявани услуги за сигурност или доставчик на онлайн място за търговия, на онлайн търсачка или на платформа за услуги на социални мрежи, който не е установен в Съюза, предлага услуги в рамките на Съюза, той следва да определи представител в Съюза. За да се установи дали този субект предлага услуги в Съюза, следва да се установи дали той възнамерява да предлага услуги на лица на територията на една или повече държави членки. Сама по себе си достъпността в Съюза на уебсайт на субект или на негов посредник или на адрес на електронна поща или други данни за контакт, или използването на език, който широко се използва в третата държава, в която е установен субектът, следва да се счита за недостатъчна, за да бъде потвърдено подобно намерение. Въпреки това фактори като използване на език или валута, които широко се използват в една или повече държави членки, с възможност за поръчване на услуги на този език, или посочването на потребители или ползватели на територията на Съюза, биха могли да указват, че субектът възнамерява да предлага услуги в Съюза. Представителят следва да действа от името на субекта, а компетентните органи или ЕРИКС следва да имат възможност да се обърнат към представителя. Представителят следва да е определен изрично чрез упълномощаване в писмена форма от доставчика да действа от негово име във връзка със задълженията му, предвидени в настоящата директива, включително за докладването на инциденти.

(117) За да се осигури ясен преглед на доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, субектите, предоставящи услуги за регистрация 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, които предоставят услуги в целия Съюз, попадащи в обхвата на настоящата директива, ENISA следва да създаде и поддържа регистър на тези субекти въз основа на информацията, получена от държавите членки, когато е приложимо чрез националните механизми, създадени за да се регистрират субектите сами. Единните звена за контакт следва да препращат на ENISA информацията и всички промени в нея. С цел да се гарантира точността и пълнотата на информацията, която следва да бъде включена в този регистър, държавите членки могат да представят на ENISA наличната във всякакви национални регистри информация за тези субекти. ENISA и държавите членки следва да предприемат мерки за улесняване на оперативната съвместимост на тези регистри, като същевременно гарантират защитата на поверителната или класифицираната информация. ENISA следва да установи подходящи протоколи за класификация и управление на информацията, с цел да се гарантира сигурността и поверителността на разкритата информация и да се ограничи достъпът, съхранението и предаването на такава информация до целевите потребители.

(118) Когато съгласно настоящата директива се обменя, докладва или споделя по друг начин информация, която е класифицирана в съответствие с правото на Съюза или националното право, следва да се прилагат съответните правила относно боравенето с класифицирана информация. Освен това ENISA следва да разполага с инфраструктура, процедури и правила за работа с чувствителна и класифицирана информация в съответствие с приложимите правила за сигурност за защита на класифицирана информация на ЕС.

(119) Предвид нарастването на сложността и професионализма на киберзаплахите качеството на мерките за разкриване на такива заплахи и тяхното предотвратяване в голяма степен зависи от редовното споделяне между субектите на информация за заплахите и уязвимостите. Обменът на информация допринася за повишаването на осведомеността за киберзаплахите, което на свой ред подобрява капацитета на субектите да предотвратяват материализирането на такива заплахи в инциденти и позволява на субектите по-добре да ограничават въздействието на инцидентите и да възстановяват функциите си по-ефикасно. При липсата на насоки на равнището на Съюза различни фактори изглежда са възпрепятствали такъв обмен на информация, най-вече несигурността относно съвместимостта с правилата за конкуренцията и отговорността.

(120) Субектите следва да бъдат насърчавани и подпомагани от държавите членки колективно да вложат своите лични познания и практически опит на стратегическо, тактическо и оперативно равнище с цел подобряване на способностите си по адекватен начин да предотвратяват, откриват, реагират или възстановяват от инциденти или да смекчават тяхното въздействие. Затова е необходимо на равнището на Съюза да се даде възможност за възникването на споразумения за доброволен обмен на информация в областта на киберсигурността. За тази цел държавите членки следва активно да подпомагат и насърчават субектите като тези, които предоставят услуги и научни изследвания в областта на киберсигурността, както и съответните субекти, които не попадат в обхвата на настоящата директива, да участват в такива споразумения за споделяне на информация за киберсигурността. Тези споразумения следва да бъдат установени в съответствие с правилата на Съюза в областта на конкуренцията и правото на Съюза в областта на защитата на данните.

(121) Обработването на личните данни, в степента, необходима и пропорционална за гарантиране на сигурността на мрежовите и информационните системи от съществени и важни субекти, може да се счита за законосъобразно въз основа на факта, че това обработване е в съответствие с правно задължение, което се прилага спрямо администратора, в съответствие с изискванията на член 6, параграф 1, буква в) и член 6, параграф 3 от Регламент (ЕС) 2016/679. Обработването на лични данни може да бъде необходимо и за законните интереси, преследвани от съществени и важни субекти, както и от доставчици на технологии и услуги в областта на сигурността, действащи от името на тези субекти, в съответствие с член 6, параграф 1, буква е) от Регламент (ЕС) 2016/679, включително когато това обработване е необходимо за споразумения за обмен на информация в областта на киберсигурността или за доброволно съобщаване на съответната информация в съответствие с настоящата директива. Мерки, свързани с предотвратяването, разкриването, идентифицирането, ограничаването, анализирането и отговора на инциденти, мерки за повишаване на осведомеността във връзка с конкретни киберзаплахи, обмен на информация в контекста на отстраняване на уязвимостите и координирано разкриване на уязвимостите, доброволен обмен на информация за тези инциденти и за киберзаплахи и уязвимости, показатели за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране може да изискват обработването на определени категории лични данни, като например IP адреси, унифицирани указатели на ресурс (URL), имена на домейни, адреси на електронна поща и, когато те разкриват лични данни, електронни времеви печати. Обработването на лични данни от компетентните органи, единните звена за контакт и ЕРИКС може да съставлява правно задължение или да се счита за необходимо за изпълнението на задача от обществен интерес или за упражняването на официалните правомощия, които са предоставени на администратора съгласно член 6, параграф 1, буква в) или д) и член 6, параграф 3 от Регламент (ЕС) 2016/679, или за преследване на законен интерес на съществените и важните субекти, както е посочено в член 6, параграф 1, буква е) от посочения регламент. Освен това в националното право може да се определят правила, позволяващи на компетентните органи, единните звена за контакт и ЕРИКС, доколкото това е необходимо и пропорционално за целите на гарантирането на сигурността на мрежовите и информационните системи на съществените и важните субекти, да обработват специални категории лични данни в съответствие с член 9 от Регламент (ЕС) 2016/679, по-специално чрез предвиждане на подходящи и конкретни мерки за защита на основните права и интереси на физическите лица, включително технически ограничения за повторното използване на такива данни и използването на най-съвременни мерки за сигурност и опазване на неприкосновеността на личния живот, като псевдонимизация или криптиране, когато анонимизирането може значително да засегне преследваната цел.

(122) За да се засилят надзорните правомощия и надзорните мерки, подпомагащи осигуряването на ефективно изпълнение, настоящата директива следва да предостави минимален списък с надзорни мерки и средства, чрез които компетентните органи могат да осъществяват надзор върху съществените и важните субекти. Освен това с настоящата директива следва да се разграничат надзорните режими за съществените и за важните субекти, за да гарантира справедлив баланс на задълженията за субектите и за компетентните органи. Поради това съществените субекти следва да подлежат на всеобхватен предварителен и последващ надзорен режим, докато важните субекти следва да подлежат на облекчен, единствено последващ надзорен режим. Поради това от важните субекти не следва да се изисква систематично да документират спазването на мерките за управление на риска в областта на киберсигурността, а компетентните органи следва да прилагат реактивен подход с последващ надзор, поради което няма да имат общо задължение за осъществяване на надзор върху тези субекти. Последващият надзор на важните субекти може да бъде задействан от доказателства, признаци или информация, доведени до знанието на компетентните органи, за които тези органи считат, че са налице потенциални нарушения на настоящата директива. Например тези доказателства, признаци или информация могат да бъдат такива, които са предоставени на компетентните органи от други органи, субекти, граждани, медии или други източници, да бъдат публично достъпна информация или могат да произтичат от други дейности, извършвани от компетентните органи при изпълнението на техните задачи.

(123) Изпълнението на надзорните задачи от компетентните органи не следва ненужно да възпрепятства стопанската дейност на съответния субект. Когато компетентните органи изпълняват своите надзорни задачи по отношение на съществените субекти, включително извършването на проверки на място и дистанционни проверки, разследването на нарушения на настоящата директива, провеждането на одити на сигурността или сканиране на сигурността, те следва да сведат до минимум въздействието върху стопанската дейност на съответния субект.

(124) При упражняването на предварителен надзор компетентните органи следва да могат да вземат решения относно приоритизирането по пропорционален начин на използването на надзорните мерки и средства, с които разполагат. Това предполага компетентните органи да могат да вземат решение за такова приоритизиране въз основа на методологии за надзор, които да следват основан на риска подход. По-конкретно, тези методологии биха могли да включват критерии или стойностни показатели за класифициране на съществените субекти в рискови категории и на съответните надзорни мерки и средства, препоръчвани за всяка рискова категория, като например използване, честота или вид на проверките на място, целеви одити на сигурността, или сканирания на сигурността, вид на информацията, която трябва да се изисква, и степен на изчерпателност на тази информация. Тези надзорни методологии биха могли

също да бъдат придружени от работни програми и да бъдат оценявани и преразглеждани редовно, включително по аспекти като разпределението на ресурсите и нуждите. По отношение на органите на публичната администрация надзорните правомощия следва да се упражняват в съответствие с националните законодателни и институционални рамки.

(125) Компетентните органи следва да гарантират, че техните надзорни задачи по отношение на съществените и важните субекти се изпълняват от обучени специалисти, които следва да притежават необходимите умения за изпълнението на тези задачи, по-специално по отношение на извършването на проверки на място и дистанционни проверки, включително установяването на слабости в базите данни, хардуера, защитните стени, криптирането и мрежите. Тези инспекции и надзорът следва да се извършват по обективен начин.

(126) В надлежно обосновани случаи, когато му е известно наличието на значителна киберзаплаха или непосредствен риск, компетентният орган следва да може да взема незабавни решения за правоприлагане с цел предотвратяване или реагиране на инцидент.

(127) За да се осъществи ефективното правоприлагане, следва да бъде създаден минимален списък с правомощия по правоприлагане, които могат да бъдат упражнени за нарушение на мерките за управление на риска в областта на киберсигурността и задълженията за докладване, предвидени в настоящата директива, като се установи ясна и последователна рамка за такова правоприлагане в Съюза. Дължимо внимание следва да се обърне на естеството, тежестта и продължителността на нарушението на настоящата директива, причинените материални или нематериални вреди, умишления или неумишлен характер на нарушението, действията, предприети за предотвратяване или намаляване на претърпените материални или нематериални вреди, степента на отговорност или евентуални относими предходни нарушения, степента на сътрудничество с компетентния орган и всякакъв друг утежняващ или смекчаващ фактор. Правоприлагащите мерки, включително административни глоби, следва да бъдат пропорционални и да подлежат на подходящи процедурни гаранции в съответствие с общите принципи на правото на Съюза и Хартата на основните права на Европейския съюз („Хартата“), включително правото на ефективни правни средства за защита и на справедлив съдебен процес, презумпцията за невиновност и правото на защита.

(128) Настоящата директива не изисква от държавите членки да предвиждат наказателна или гражданска отговорност по отношение на физическите лица, отговорни да гарантират, че даден субект спазва настоящата директива за вреди, понесени от трети страни в резултат на нарушение на настоящата директива.

(129) За да се гарантира ефективното прилагане на предвидените съгласно настоящата директива задължения, всеки компетентен орган следва да разполага с правомощието да налага или изисква налагането на административни глоби.

(130) Когато административната глоба се налага на съществен или важен субект, който е предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с членове 101 и 102 от ДФЕС за тези цели. При налагане на административна глоба на лице, което не е предприятие, компетентният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето когато определя подходящия размер на глобата. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни глоби. Налагането на административна глоба не засяга прилагането на други правомощия от компетентните органи или на други санкции, предвидени съгласно националните разпоредби, транспониращи настоящата директива.

(131) Държавите членки следва да могат да определят правилата относно наказателните санкции за нарушения на националните правила, транспониращи настоящата директива. Налагането на наказателни санкции за нарушения на тези национални правила и на свързани с това административни санкции обаче не следва да води до нарушаване на принципа *ne bis in idem* съгласно тълкуването на Съда на Европейския съюз.

(132) Когато административните наказания не са хармонизирани в настоящата директива или при необходимост в други случаи, например при сериозно нарушение на настоящата директива, държавите членки следва да прилагат система, която предвижда ефективни, пропорционални и възпиращи санкции. Естеството на тези санкции и това дали са наказателни или административни следва да бъде определено съгласно националното право.

(133) За допълнително засилване на ефективността и силата за разубеждение на правоприлагащите мерки, приложими за нарушения на настоящата директива, компетентните органи следва да разполагат с правомощия да спрат временно или да изискат временно спиране на удостоверение или разрешение относно всички съответни предоставени услуги или част от тях, или относно дейностите, извършвани от съществен субект, както и да изискват налагането на временна забрана за упражняване на управленски функции от всяко физическо лице, изпълняващо управленски функции на равнището на главно изпълнително длъжностно лице или законен представител. Предвид тежестта и въздействието върху дейностите на субектите и в крайна сметка върху ползвателите, тези временни спирания или забрани следва да се прилагат само пропорционално на тежестта на нарушението и да отчитат обстоятелствата при всеки отделен случай, включително дали нарушението е било с предумишлен или непредумишлен характер, както и всякакви действия, предприети за предотвратяване или ограничаване на материалните или нематериалните вреди. Тези временни спирания или забрани следва да се прилагат единствено като крайна мярка, т.е. само след като останалите съответни правоприлагащи мерки, предвидени от настоящата директива, са били изчерпани, и само докато засегнатият субект предприеме необходимото действие за отстраняване на недостатъците или изпълнение на изискванията на компетентния орган, за които се отнасят тези временни спирания или забрани. Налагането на такива временни спирания или забрани следва да подлежи на подходящи процедурни гаранции в 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.

(134) С цел да се гарантира, че субектите изпълняват задълженията си, предвидени в настоящата директива, държавите членки следва да си сътрудничат и да се подпомагат взаимно по отношение на надзорните и правоприлагащи мерки, по-специално когато даден субект предоставя услуги в повече от една държава членка или когато неговите мрежови и информационни системи се намират в държава членка, различна от тази, в която предоставя услуги. Когато предоставя помощ, компетентният орган, към който е отправено искането, следва да предприеме надзорни или правоприлагащи мерки в съответствие с националното право. За да се гарантира гладкото функциониране на взаимопомощта съгласно настоящата директива, компетентните органи следва да използват групата за сътрудничество като форум за обсъждане на случаи и конкретни искания за помощ.

(135) За да се гарантира ефективен надзор и правоприлагане, по-специално в случаи с трансгранично измерение, държавата членка, която е получила искане за взаимопомощ, следва, в рамките на това искане, да предприеме подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или притежава мрежова и информационна система на територията на същата държава членка.

(136) Настоящата директива следва да установи правила за сътрудничество между компетентните органи и надзорните органи съгласно Регламент (ЕС) 2016/679 с цел справяне нарушенията на настоящата директива, свързани с личните данни.

(137) Настоящата директива следва да има за цел да гарантира високо равнище на отговорност при мерките за управление на риска в областта на киберсигурността и задълженията за докладване на равнището на съществените и важните субекти. Поради това управителните органи на съществените и важните субекти следва да одобряват мерките за управление на риска в областта на киберсигурността, и да наблюдават тяхното изпълнение.

(138) За да се гарантира високо общо ниво на киберсигурност в целия Съюз въз основа на настоящата директива, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от ДФЕС във връзка с допълването на настоящата директива, като се уточнява от кои категории съществени и важни субекти се изисква да използват някои сертифицирани ИКТ продукти, ИКТ услуги и ИКТ процеси или да получат сертификат по европейска схема за сертифициране на киберсигурността. От особена важност е по време на подготвителната работа Комисията да проведе подходящи консултации, включително на експертно равнище, и те да бъдат извършени в съответствие с принципите, заложени в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество ([22]). По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

([22]) ОВ L 123, 12.5.2016 г., стр. 1.

(139) За да се гарантират еднакви условия за изпълнение на настоящата директива, на Комисията следва да бъдат предоставени изпълнителни правомощия за определяне на процедурните правила, необходими за работата на групата за сътрудничество, както и на техническите и методологичните и секторните изисквания относно мерките за управление на риска в областта на киберсигурността и за допълнително уточняване на вида на информацията, формата и процедурата за уведомяване за инциденти, киберзаплахи и ситуации, близки до инциденти, и за съобщения за значителни киберзаплахи, както и за случаи, в които даден инцидент трябва да се счита за значим. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета ([23]).

(140) Комисията следва периодично да извършва преглед на настоящата директива, след като се консултира със заинтересованите страни, по-специално с цел установяване дали е целесъобразно да предложи изменения предвид промените в обществените, политически, технологични или пазарни условия. Като част от тези прегледи Комисията следва да прави оценка на значението на големината на съответните субекти и на секторите, подсекторите и вида субекти, посочени в приложенията към настоящата директива, за функционирането на икономиката и обществото във връзка с киберсигурността. Комисията следва да оцени, наред с другото, дали доставчиците, които попадат в обхвата на настоящата директива и които са определени като много големи онлайн платформи по смисъла на член 33 от Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета ([24]), могат да бъдат установени като съществени субекти съгласно настоящата директива.

(141) С настоящата директива се създават нови задачи за ENISA, като по този начин се засилва нейната роля, и може също така да се наложи ENISA да изпълнява своите съществуващи задачи съгласно Регламент (ЕС) 2019/881 на едно по-високо равнище от преди. За да се гарантира, че ENISA разполага с необходимите финансови и човешки ресурси, за да изпълнява съществуващите и новите задачи, както и за да отговаря на всяко по-високо равнище на изпълнение на тези задачи, произтичащи от засилената ѝ роля, нейният бюджет следва да бъде съответно увеличен. Освен това, за да се гарантира ефективно използване на ресурсите, на ENISA следва да се предостави по-голяма гъвкавост по отношение на начина, по който тя може да разпределя ресурси във вътрешен план за целта на ефективното изпълнение на нейните задачи и отговаряне на очакванията.

(142) Доколкото целта на настоящата директива, а именно постигане на високо общо ниво на киберсигурност в Съюза, не може да бъде постигната в достатъчна степен от държавите членки, а поради последиците от действието може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейски съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящата директива не надхвърля необходимото за постигане на тази цел.

(143) Настоящата директива зачита основните права и е съобразена с принципите, признати в Хартата, по-специално правото на зачитане на личния живот и комуникациите, защитата на личните данни, свободата на стопанска инициатива, правото на собственост, правото на ефективни правни средства за защита и на справедлив съдебен процес, презумпцията за невиновност и правото на защита. Правото на ефективни правни средства за защита обхваща и получателите на услуги, предоставяни от съществени и важни субекти. Настоящата директива следва да бъде прилагана в съответствие с посочените права и принципи.

(144) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([25]) и прие своето становище на 11 март 2021 г. ([26]),

([23]) Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

([24]) Регламент (ЕС) 2022/2065 на Европейския парламент и на Съвета от 19 октомври 2022 г. относно единния пазар на цифрови услуги и за изменение на Директива 2000/31/ЕО (ОВ L 277, 27.10.2022 г. , стр. 1).

([25]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

([26]) ОВ C 183, 11.5.2021 г., стр. 3.

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

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.

2. За тази цел с настоящата директива се установяват:

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);

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;

в) правила и задължения относно обмена на информация за киберсигурността;

г) задължения за надзор и правоприлагане за държавите членки.

Член 2

Обхват

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 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.

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;

ii) доставчици на удостоверителни услуги;

iii) регистри на имена на домейни от първо ниво и доставчици на системни услуги за имена на домейни;

б) субектът е единствен доставчик в дадена държава членка на услуга, която е от съществено значение за поддържането на критични обществени и икономически дейности;

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

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;

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;

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.

3. Независимо от размера им, настоящата директива се прилага за субекти, установени като критични субекти съгласно Директива(ЕС) 2022/2557.

4. Независимо от размера им, настоящата директива се прилага за субекти, предоставящи услуги за регистрация на имена на домейни.

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. 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 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.

9. Параграфи 7 и 8 не се прилагат, когато даден субект действа като доставчик на удостоверителни услуги.

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.

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.

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.

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.

([27]) Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 17.12.2011 г., стр. 1).

([28]) Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8).

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 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.

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 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. 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).

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 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

б) Комисията за съответната информация относно броя на съществените 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).

Член 4

Специфични за сектора правни актове на Съюза

1. Когато специфични за сектора правни актове на Съюза изискват 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 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.

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.

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 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) „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 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;

([29]) 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, 14.11.2012 г., стр. 12).

18) „точка за обмен в интернет“ означава мрежово средство, което дава възможност за свързване на повече от две независими мрежи (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 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;

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;

([30]) 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, 17.9.2015 г., стр. 1).

([31]) Директива 2005/29/ЕО на Европейския парламент и на Съвета от 11 май 2005 г. относно нелоялни търговски практики от страна на търговци към потребители на вътрешния пазар и изменение на Директива 84/450/ЕИО на Съвета, Директиви 97/7/ЕО, 98/27/ЕО и 2002/65/ЕО на Европейския парламент и на Съвета, и Регламент (ЕО) № 2006/2004 на Европейския парламент и на Съвета („Директива за нелоялни търговски практики“) (ОВ L 149, 11.6.2005 г., стр. 22).

([32]) Регламент (ЕС) 2019/1150 на Европейския парламент и на Съвета от 20 юни 2019 г. за насърчаване на справедливост и прозрачност за бизнес ползвателите на посреднически онлайн услуги (ОВ L 186, 11.7.2019 г., стр. 57).

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;

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;

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;

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) „научноизследователска организация“ означава субект, чиято основна цел е да извършва приложна научноизследователска или развойна дейност с цел използване на резултатите от тези научни изследвания за търговски цели, но който не включва образователни институции.

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 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:

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 обществото 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 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 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, 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.

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 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) 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.

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 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 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.

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;

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;

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.

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.

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 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, 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.

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.

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;

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, 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;

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 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.

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 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 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.

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.

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 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 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;

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 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 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.

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 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:

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:

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. 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.

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 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.

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 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.

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.

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 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-голямия 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 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, 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.

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.

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;

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 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:

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. 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.

Член 30

Доброволно уведомяване за относима информация

1. Държавите членки гарантират, че в допълнение към задължението за уведомяване, 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.

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.

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;

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.

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 д), е) или ж) компетентните органи заявяват целта на своето искане и уточняват исканата информация.

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;

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 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;

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 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.

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;

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;

8. Компетентните органи излагат подробни мотиви за своите правоприлагащи мерки. Преди да 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.

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 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.

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;

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 пояснят исканата информация.

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 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.

5. Член 32, параграфи 6, 7 и 8 се прилагат *mutatis mutandis* за надзорните и правоприлагащи мерки, предвидени в настоящия член за важните субекти.

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.

Член 34

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.

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).

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.

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 съществуващият 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.

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.

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.

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.

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.

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 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.

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 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.

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.

Член 41

Транспониране

1. До 17 октомври 2024 г. държавите членки приемат и публикуват разпоредбите, необходими, за 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.

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*.

Член 46

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в Страсбург на 14 декември 2022 година

За Европейския парламент	*За Съвета*
Председател	*Председател*
R. METSOLA	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 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])
		— 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
		— 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

Сектор	Подсектор	Вид субект
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 обслужващи 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, експлоатирани 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])
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])
		— Централни контрагенти (ЦК) съгласно определението в член 2, точка 1 от Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета ([17])

Сектор	Подсектор	Вид субект
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])
		— 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 В, 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
7. Отпадъчни води		Предприятия, които събират, обезвреждат или пречистват градски, битови или промишлени отпадъчни води съгласно определението в член 2, точки от 1, 2 и 3 от Директива 91/271/ЕИО на Съвета ([23]), с изключение на предприятията, за които събирането, обезвреждането или пречистването на градски, битови или промишлени отпадъчни води е несъществена част от тяхната обща дейност
8. Цифрова инфраструктура		— Доставчици на точки за обмен в интернет
		— Доставчици на DNS услуги, с изключение на оператори на коренови сървъри за имена
		— Регистри на имената на домейни от първо ниво
		— Доставчици на услуги за изчисления в облак
		— Доставчици на услуги на центрове за данни
		— Доставчици на мрежи за доставка на съдържание
		— Доставчици на удостоверителни услуги
		— Доставчици на обществени електронни съобщителни мрежи
		— Доставчици на обществено достъпни електронни съобщителни услуги
9. Управление на услуги в областта на ИКТ (между предприятия)		— Доставчици на управлявани услуги — Доставчици на управлявани услуги за сигурност

Сектор	Подсектор	Вид субект
10. Публична администрация		— Органи на публичната администрация на централното държавно управление, определени от държава членка в съответствие с националното 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).

([6]) 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).

([7]) 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).

([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).
(20) 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).
(21) 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 услуги съгласно определението в член 2, точка 1а от Директива 97/67/ЕО, включително доставчици на куриерски услуги
2. Управление на отпадъците		Предприятия, извършващи управление на отпадъците съгласно определението в член 3, точка 9 от Директива 2008/98/ЕО на Европейския парламент и на Съвета ([1]), с изключение на предприятия, за които управлението на отпадъците не е основна икономическа дейност
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
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
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
	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
	в) Производство на електрически съоръжения	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 оборудване	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
		— Доставчици на платформи на услуги за социални мрежи
7. Научни изследвания		Научноизследователски организации

([1]) Директива 2008/98/ЕО на Европейския парламент и на Съвета от 19 ноември 2008 г. относно отпадъците и за отмяна на определени директиви (ОВ L 312, 22.11.2008 г., стр. 3).

([2]) Регламент (ЕО) № 1907/2006 на Европейския парламент и на Съвета от 18 декември 2006 г. относно регистрацията, оценката, разрешаването и ограничаването на химикали (REACH), за създаване на Европейска агенция по химикали, за изменение на Директива 1999/45/ЕО и за отмяна на Регламент (ЕИО) № 793/93 на Съвета и Регламент (ЕО) № 1488/94 на Комисията, както и на Директива 76/769/ЕИО на Съвета и директиви 91/155/ЕИО, 93/67/ЕИО, 93/105/ЕО и 2000/21/ЕО на Комисията (ОВ L 396, 30.12.2006 г., стр. 1).

([3]) Регламент (ЕО) № 178/2002 на Европейския парламент и на Съвета от 28 януари 2002 г. за установяване на общите принципи и изисквания на законодателството в областта на храните, за създаване на Европейски орган за безопасност на храните и за определяне на процедури относно безопасността на храните (ОВ L 31, 1.2.2002 г., стр. 1).

([4]) Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1).

([5]) Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ L 117, 5.5.2017 г., стр. 176).

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
Член 10, параграфи 1, 2 и 3, първа алинея	Член 13, параграфи 1, 2 и 3
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
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

Директива (ЕС) 2016/1148	Настоящата директива
Член 14, параграф 6	Член 23, параграф 7
Член 14, параграф 7	Член 23, параграф 11
Член 15, параграф 1	Член 31, параграф 1
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
Член 16, параграфи 8 и 9	Член 21, параграф 5 и член 23, параграф 11
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
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
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)

Директива (ЕС) 2016/1148	Настоящата директива
Приложение I, точка 2, буква а), подточка v)	Член 11, параграф 2, буква е)
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