ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 16.12.2020 г.
COM(2020) 823 final

2020/0359 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

(текст от значение за ЕИП)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Настоящото предложение е част от пакет от мерки за допълнително подобряване на устойчивостта и капацитета за реагиране при инциденти на публичноправните и частноправните субекти, компетентните органи и Съюза като цяло в областта на киберсигурността и защитата на критичната инфраструктура. То е съобразено с приоритетите на Комисията за привеждане на Европа в готовност за цифровата ера и за изграждането на приспособена към бъдещите предизвикателства икономика, която работи в интерес на хората. Киберсигурността е приоритет в реакцията на Комисията по отношение на кризата с COVID-19. Пакетът включва нова стратегия относно киберсигурността, имаща за цел укрепване на стратегическата самостоятелност на Съюза за подобряване на неговата устойчивост и колективна реакция, както и за изграждане на отворен и глобален интернет. Накрая, в пакета се съдържа предложение за директива относно устойчивостта на критичните оператори на основни услуги, имаща за цел да ограничи физическите заплахи срещу такива оператори.

Настоящото предложение надгражда и отменя Директива (ЕС) 2016/1148 за сигурност на мрежите и информационните системи (Директивата за МИС), която е първата част от общото за целия ЕС законодателство за киберсигурността и която предоставя правни мерки за повишаване на цялостното ниво на киберсигурността в Съюза. Директивата за МИС 1) допринесе за подобряване на способностите в областта на киберсигурността на национално равнище посредством изискването от държавите членки да приемат национални стратегии за киберсигурност и да определят органи в тази сфера; 2) засили сътрудничеството между държавите членки на равнището на Съюза, като въведе различни форуми, улесняващи обмена на стратегическа и оперативна информация; и 3) подобри киберустойчивостта на публичноправните и частноправните субекти в седем конкретни сектора (енергетика, транспорт, банково дело, инфраструктури на финансовия пазар, здравеопазване, доставка и снабдяване с питейна вода и цифрови инфраструктури), както и в рамките на три цифрови услуги (онлайн местата за търговия, онлайн търсачките и компютърните услуги „в облак“), изисквайки от държавите членки да гарантират, че операторите на основни услуги и доставчиците на цифрови услуги са въвели изисквания за киберсигурност и докладват за инциденти.

С предложението се осъвременява съществуващата правна рамка, като се отчитат повишената цифровизация на вътрешния пазар през последните години и развиващата се картина на заплахите за киберсигурността. Тези две тенденции на развитие се засилиха допълнително след началото на кризата с COVID-19. В предложението се предвиждат и действия по отношение на някои слабости, които попречиха на Директивата за МИС да разгърне пълния си потенциал.

Независимо от забележителните постижения на Директивата за МИС, която проправи пътя за значителна промяна в нагласите във връзка с институционалния и регулаторния подход към киберсигурността в редица държави членки, проличаха и нейните ограничения. Цифровата трансформация на обществото (ускорена от кризата с COVID-19) разшири картината на заплахите и поражда нови предизвикателства, изискващи съобразени и новаторски реакции. Кибератаките идват от широк кръг източници в ЕС и извън него, а броят и сложността им продължават да нарастват.

В оценката за функционирането на Директивата за МИС, извършена за целите на оценката на въздействие, бяха установени следните проблеми: 1) ниското равнище на

киберустойчивост на предприятията, извършващи дейност в ЕС; 2) нееднаквите равнища на устойчивост в отделните държави членки и сектори; както и (3) ниското равнище на съвместна ситуационна осведоменост и липса на съвместна реакция при кризи. Например някои главни болници в някои държави членки не попадат в обхвата на Директивата за МИС, поради което от тях не се изисква да прилагат произтичащите мерки за сигурност, докато в други държави членки почти всеки доставчик на здравно обслужване е обхванат от изискванията за сигурност на МИС.

Като инициатива в рамките на Програмата за пригодност и резултатност на регулаторната рамка (REFIT) предложението има за цел да намали регулаторната тежест за компетентните органи и разходите на публичноправните и частноправните субекти за привеждане в съответствие. Това най-вече се постига чрез премахване на задължението на компетентните органи да установяват операторите на основни услуги и чрез увеличаване на нивото на хармонизация на изискванията за сигурност и докладване, с цел да се улесни спазването на регулаторните изисквания за субектите, предоставящи трансгранични услуги. Същевременно на компетентните органи ще бъдат възложени редица нови задачи, включващи надзор върху субектите, които до момента не са обхванати от Директивата за МИС.

- **Съгласуваност с действащите разпоредби в тази област на политиката**

Настоящото предложение е част от по-широк набор от съществуващи правни инструменти и предстоящи инициативи на равнището на Съюза, имащи за цел да повишат устойчивостта на публичноправните и частноправните субекти срещу заплахи.

В областта на киберсигурността това са най-вече Директива (ЕС) 2018/1972 за установяване на Европейски кодекс за електронни съобщения (чиито свързани с киберсигурността разпоредби ще бъдат заменени с разпоредбите на разглежданото предложение) и предложението за Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор (COM(2020) 595 final), което ще се счита за *lex specialis* за разглежданото предложение, щом и двата акта влязат в сила.

В областта на физическата сигурност предложението допълва предложението за Директива относно устойчивостта на критичните субекти, с която се преработва Директива 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (Директивата за ЕКИ), създаваща в Съюза процес на установяване и означаване на европейски критични инфраструктури и определяща подход за подобряване на тяхната защита. През юли 2020 г. Комисията прие стратегията на ЕС за Съюза на сигурност[1], в която се признава нарастващата взаимосвързаност и взаимозависимост между физическите и цифровите инфраструктури. В нея се подчертава нуждата от по-съгласуван и последователен подход между Директивата за ЕКИ и Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

Ето защо предложението е тясно съгласувано с предложението за Директива относно устойчивостта на критичните субекти, имаща за цел да повиши устойчивостта на този вид субекти срещу физическите заплахи в голям брой сектори. Предложението цели да гарантира, че компетентните органи съгласно двата правни акта при необходимост

[1] COM(2020)605 final.

предприемат допълнителни мерки и обменят информация относно устойчивостта в киберпространството и извън него, както и че особено критичните оператори в секторите, които следва да се считат за „основни“ съгласно разглежданото предложение, са предмет и на по-общи задължения за подобряване на устойчивостта с акцент върху рисковете извън киберпространството.

- **Съгласуваност с други политики на Съюза**

Както бе посочено в съобщението „Изграждане на цифровото бъдеще на Европа“[2], за Европа е от решаващо значение да се възползва от всички предимства на цифровата ера и да укрепи своята промишленост и иновационен капацитет в рамките на безопасни и етични граници. В Европейската стратегия за данните се определят четири стълба — защита на данните, основни права, безопасност и киберсигурност — като основни необходими условия за общество, което разполага с възможността за използване на данни.

В резолюция от 12 март 2019 г. Европейският парламент призовава *„[…] Комисията да оцени необходимостта от допълнително разширяване на обхвата на Директивата за МИС, така че да бъдат включени и други сектори и услуги от критично значение, които не са обхванати от специфично за сектора законодателство“*[3]. В своето заключение от 9 юни 2020 г. Съветът приветства *„[…] плановете на Комисията да осигури съгласувани правила за пазарните оператори и да улесни създаването на сигурен, надежден и подходящ обмен на информация относно заплахите и инцидентите, включително чрез преразглеждане на Директивата за мрежова и информационна сигурност (Директивата за МИС), за да се търсят възможности за по-добра устойчивост на киберпространството и по-ефективни мерки за противодействие на кибератаките, особено по отношение на основните икономически и обществени дейности, като същевременно се зачитат правомощията на държавите членки, включително отговорността за тяхната национална сигурност“*[4]. Освен това предложеният правен акт не засяга прилагането на правилата за конкуренция, предвидени в Договора за функционирането на Европейския съюз (ДФЕС).

Предвид факта, че значителна част от заплахите за киберсигурността произхождат от страни извън ЕС, е необходим съгласуван подход към международното сътрудничество. Настоящата директива ще бъде референтен модел, който ще бъде разпространяван в контекста на сътрудничеството на ЕС с трети държави, по-специално при предоставянето на външна техническа помощ.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

- **Правно основание**

Правното основание за Директивата за МИС е член 114 от Договора за функционирането на Европейския съюз, чиято цел е създаването или функционирането на вътрешния пазар чрез усъвършенстване на мерките за сближаване на националните

[2] COM(2020)67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_BG.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/bg/pdf

правила. Както постановява Съдът на ЕС в своето решение по дело C-58/08, Vodafone и др., прибягването до член 114 ДФЕС е обосновано при наличие на разлики между националните правни рамки, които дават пряко отражение върху функционирането на вътрешния пазар. Съдът също така постановява, че когато акт, приет на основание член 114 ДФЕС вече е отстранил всички препятствия пред търговията в хармонизираната с него област, законодателят на Съюза не може да бъде лишен от възможността да адаптира този акт към всяка промяна в обстоятелствата или към развитието на познанието с оглед на възложената му задача да гарантира защитата на признатите от Договора общи интереси. Накрая, Съдът постановява, че мерките за сближаване, обхванати от член 114 ДФЕС, имат за цел да предоставят свобода на преценка относно техниката на сближаване, която в зависимост от общия контекст и конкретните обстоятелства относно подлежащата на хармонизация материя е най-подходяща за постигане на желания резултат. Предложеният правен акт ще премахне пречките пред вътрешния пазар и ще подобри неговото изграждане и функциониране за основните и значими субекти чрез: установяването на ясни общо приложими правила относно приложното поле на Директивата за МИС, като хармонизира правилата, приложими в областта на управлението на риска, свързан с киберсигурността, и докладването за инциденти. Настоящите различия в тази област — както на законодателно равнище и на равнището на надзора, така и на национално равнище и на равнището на ЕС — представляват пречки за вътрешния пазар, тъй като субектите, извършващи трансгранични дейности, подлежат на различни и вероятно припокриващи се регулаторни изисквания и/или към тях се прилагат такива изисквания, което е в ущърб на упражняването на тяхната свобода на установяване и на предоставяне на услуги. Различните правила имат отрицателно отражение и върху условията за конкуренция във вътрешния пазар, когато става въпрос за субекти от един и същи вид в различни държави членки.

- **Субсидиарност (при неизключителна компетентност)**

Устойчивостта на киберсигурността в Съюза не може да бъде ефективна, ако подходът към нея е различен при отделните национално или регионално обособени системи. С Директивата за МИС тази слабост бе преодоляна отчасти, като бе установена рамка за сигурността на мрежите и информационните системи на национално равнище и на равнището на Съюза. Нейното транспониране и прилагане обаче разкри също така присъщи слабости и ограничения на някои разпоредби или подходи, като например неясното определяне на обхвата на директивата, водещо до съществени различия в степента и задълбочеността на фактическа намеса на ЕС на равнището на държавите членки. Освен това, от началото на кризата с COVID-19 европейската икономика развиоще по-голяма отпреди зависимост от мрежите и информационните системи, като секторите и услугите са все по-взаимосвързани. Намесата на ЕС отвъд настоящите мерки на Директивата за МИС е обоснована главно от: i) все по-трансграничния характер на свързаните с МИС заплахи и предизвикателства; ii) потенциала на действията на Съюза да подобрят и улеснят ефективните и координирани национални политики; и iii) значението на съгласувани и съвместни действия на политиките за ефективната защита на данните и поверителността.

- **Пропорционалност**

Предложените в настоящата директива правила не надхвърлят необходимото за задоволителното постигане на конкретните цели. Предвиденото съгласуване и

оптимизиране на мерките за сигурност и задълженията за докладване са свързани с исканията на държавите членки и предприятията за подобряване на настоящата рамка.

В предложението се отчитат вече съществуващите практики в държавите членки. Усъвършенстваното равнище на защита, постигнато чрез такива оптимизирани и координирани изисквания, е пропорционално на все по-нарастващите рискове на дневен ред, в това число онези, съдържащи трансграничен елемент; те са основателни и като цяло отговарят на интереса на субектите, свързан с гарантирането на непрекъснатостта и качеството на техните услуги. Разходите за осигуряване на систематично сътрудничество сред държавите членки биха били ниски в сравнение с икономическите и обществените загуби и вреди, причинени от инциденти с киберсигурността. Освен това, консултациите със заинтересованите страни, проведени в контекста на прегледа на Директивата за МИС, включително резултатите от откритата обществена консултация и от целеви допитвания, показват подкрепа за преработването на Директивата за МИС в очертаната по-горе рамка.

- **Избор на инструмент**

Предложението допълнително ще оптимизира наложените на предприятията задължения и ще осигури тяхното по-високо ниво на хармонизация. Същевременно предложението има за цел да предостави на държавите членки гъвкавостта, необходима да се отчетат националните особености (като например възможността да се определят допълнителни основни или значими субекти извън предвидената с правния акт основана група). Ето защо бъдещият правен инструмент следва да бъде директива, тъй като тя позволява подобрено целево хармонизиране, както и известна степен на гъвкавост за компетентните органи.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИ ОЦЕНКИ, КОНСУЛТАЦИИ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИ НА ВЪЗДЕЙСТВИЕТО

- **Последващи оценки/проверки за пригодност на действащото законодателство**

Комисията извърши оценка на функционирането на Директивата за МИС[5]. Тя анализира нейната релевантност, добавена стойност за ЕС, съгласуваност, ефективност и ефикасност. Основните констатации от анализа са следните:

- Обхватът на Директивата за МИС е твърде ограничен по отношение на обхванатите сектори, главно поради: i) повишената цифровизация през последните години и по-високата степен на взаимосвързаност, ii) факта, че понастоящем този обхват вече не отразява всички цифровизирани сектори, предоставящи ключови услуги за икономиката и обществото като цяло.
- В Директивата за МИС няма достатъчно яснота относно обхвата на операторите на основни услуги, като в разпоредбите ѝ не се изяснява в достатъчна степен националната компетентност с оглед на доставчиците на цифрови услуги. Това доведе до положение, в което някои видове субекти не бяха идентифицирани като такива във всички държави членки, поради което от тях не се изисква да въвеждат мерки за сигурност и да докладват за инциденти.

[5] [Приложение 5 към оценката на въздействието]

- С Директивата за МИС на държавите членки се предоставя широка свобода на преценка при определянето на изискванията за сигурност и докладването на инциденти към операторите на основни услуги (наричани нататък „ООУ“). Оценката показва, че в някои случаи държавите членки са приложили тези изисквания по значително различаващи се начини, като са създали допълнителна тежест за дружествата, извършващи дейност в повече от една държава членка.
- Режимът на надзор и правоприлагане на Директивата за МИС е неефективен. Държавите членки например с много голяма неохота са налагали санкции на субекти, които не са въвели изискванията за сигурност или не са докладвали за инциденти. Това може да има отрицателни последствия за киберустойчивостта на отделните субекти.
- Финансовите и човешките ресурси, заделени от държавите членки за изпълнение на техните задачи (като например определянето на операторите на основни услуги или надзора върху тях), и следователно различните равнища на зрялост при справяне с рисковете за киберсигурността, се различават в значителна степен. Това допълнително увеличава различията в киберустойчивостта между държавите членки.
- Държавите членки не обменят систематично информация помежду си, което има неблагоприятни последици по-специално за ефективността на мерките за киберсигурност и за степента на съвместна ситуационна осведоменост на равнището на ЕС. Случаят е такъв и при обмена на информация между частноправни субекти, както и при обмена между структурите за сътрудничество на равнището на ЕС и частноправните субекти.

- **Консултации със заинтересованите страни**

Комисията се консултира с широк кръг от заинтересовани страни. Държавите членки и заинтересованите страни бяха поканени да участват в откритата обществена консултация и в допитванията и работни форуми, организирани от Wavestone, Центъра за европейски политически изследвания и ICF, на които Комисията възложи провеждането на проучване в подкрепа на прегледа на Директивата за МИС. Сред консултираните заинтересовани страни бяха компетентните органи, службите и агенциите на Съюза, работещи по киберсигурността, операторите на основни услуги, доставчиците на цифрови услуги, субекти, предоставящи услуги извън обхвата на настоящата Директивата за МИС, търговски сдружения, потребителски организации и граждани.

Освен това Комисията бе в постоянен контакт с компетентните органи, отговарящи за прилагането на Директивата за МИС. Групата за сътрудничество обширно разгледа различни междуотраслови и секторни аспекти на прилагането. Накрая, по време на своите посещения в страните във връзка с МИС през 2019 г. и 2020 г. Комисията интервюира 154 публичноправни и частноправни субекта, както и 117 компетентни органа.

- **Събиране и използване на експертни становища**

Комисията възложи на консорциум от Wavestone, Центъра за европейски политически изследвания и ICF да я подкрепи при прегледа на Директивата за МИС[6]. Изпълнителят не само е осъществил контакт със заинтересованите страни, пряко засегнати от Директивата за МИС, посредством целеви запитвания и работни форуми, но също така се е консултирал с широк набор от експерти в областта на киберсигурността, като изследователи и отраслови специалисти по киберсигурност.

- **Оценка на въздействието**

Настоящото предложение е придружено от оценка на въздействието[7], внесена в Комитета за регулаторен контрол (КРК) на 23 октомври 2020 г. и получила положително становище с коментари от КРК на 20 ноември 2020 г. КРК препоръча подобрения в някои области с оглед на: 1) по-добро отразяване на ролята на трансграничните ефекти в анализа на проблемите; 2) по-добро обяснение на това как би изглеждал успехът за инициативата; 3) допълнително обосноваване на списъка с варианти на политиката; 4) допълнително пояснение за разходите на предлаганите мерки. Оценката на въздействието бе коригирана с оглед на тези бележки, както и на по-подробни коментари от КРК. Тя вече включва по-подробни разяснения на ролята на трансграничните ефекти в областта на киберсигурността, по-ясен общ преглед на начините за измерване на успеха, по-подробно разяснение на замисъла и логиката в основата на различните варианти на политиката и действията, разгледани в рамките на тези варианти, по-подробно разяснение на аспектите, анализирани във връзка със секторния обхват на Директивата за МИС, както и допълнителни разяснения относно разходите.

Комисията разгледа няколко варианта на политиката за подобряване на правната рамка в областта на киберустойчивостта и реагирането при инциденти:

- „Да не се предприема нищо“: Директивата за МИС би останала непроменена и не биха били предприети други мерки с незаконодателен характер за насочване към проблемите, установени при оценката на Директивата за МИС.
- Вариант 1: Не би имало промени на законодателно равнище. Вместо това Комисията би издала препоръки и насоки (например относно установяването на операторите на основни услуги, изискванията за сигурност, процедурите за уведомяване за инциденти и надзора), след консултация с групата за сътрудничество, Агенцията на ЕС за киберсигурност (ENISA) и, когато е приложимо, мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС).
- Вариант 2: Този вариант включва целеви изменения на Директивата за МИС, в това число разширяване на обхвата и няколко други изменения, имащи за цел да осигурят някои незабавни решения на установените проблеми, като предвидят повече яснота и допълнителна хармонизация (като например разпоредби за хармонизиране на праговете за установяване). В изменената

[6] Проучване в подкрепа на прегледа на Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (Директива за МИС) — № 2020-665. Wavestone, Център за европейски политически изследвания и ICF.

[7] **[Връзките към окончателните документи и резюмето следва да бъдат добавени.]**

Директивата за МИС все пак биха се запазили основните градивни елементи, подход и обосновка.

- Вариант 3: Този вариант предполага системни и структурни промени на Директивата за МИС (посредством нова директива), предвиждащи по-фундаментална промяна на подхода към обхващане на по-широк сегмент от икономиките в Съюза, но при по-фокусиран надзор, насочен към големите и ключовите участници. Той би оптимизирал и наложените на предприятията задължения и би осигурил тяхното по-високо ниво на хармонизация, би създал по-ефективни условия за оперативните аспекти и би установил ясна основа за усъвършенствани споделени отговорности и отчетност на различните заинтересованите страни по отношение на мерките за киберсигурност.

В оценката на въздействието се заключава, че предпочитание се дава на вариант 3 (т.е. на системните и структурните промени на рамката за МИС). По отношение на ефективността предпочитаният вариант отчетливо ще определи едно по-широко приложно поле на Директивата за МИС, обхващащо по-представителна част от икономиките и обществата в ЕС, както и оптимизиране на изискванията, успоредно с по-ясно определена рамка за надзор и правоприлагане, които ще имат за цел повишаване на равнището на съответствие. Този вариант обхваща и мерки, имащи за цел да подобрят подходите за изграждане на политики на равнището на държавите членки и да променят парадигмата за тях, като насърчат нови рамки за управлението на риска при взаимоотношенията с доставчиците и координираното оповестяване на уязвимости. С предпочитания вариант на политика същевременно се установява ясна основа за споделени отговорности и отчетност, като се предвиждат механизми, имащи за цел засилване на доверието сред държавите членки, както по отношение на органите, така и на сектора, насърчавайки обмена на информация и осигурявайки по-оперативен подход, като например механизмите за взаимопомощ и за партньорска проверка. Този вариант би предвидил също рамка на ЕС за управление на кризи, основаваща се на наскоро създадената оперативна мрежа на ЕС, и би осигурил по-голямо участие на ENISA, в рамките на настоящия ѝ мандат, чрез извършването на точен общ преглед на състоянието на киберсигурността в Съюза.

От гледна точка на ефикасността, при все че би включвал допълнителни разходи за изпълнение и правоприлагане за предприятията и държавите членки, предпочитаният вариант би довел също до ефикасни съгласувания и полезни взаимодействия и разполага с най-добрия потенциал от всички анализирани варианти на политиката за осигуряване на повишено и съгласувано равнище на киберустойчивостта на ключови субекти в Съюза, което в крайна сметка би довело до икономия на разходи както за предприятията, така и за обществото. Този вариант на политика би довел до известна допълнителна административна тежест и разходи за привеждане в съответствие за органите на държавите членки. От друга страна обаче в средносрочен и дългосрочен план той би донесъл също значителни ползи чрез повишеното сътрудничество между държавите членки, в това число на оперативно равнище, и би насърчил — чрез взаимопомощ, механизми за партньорска проверка и подобряване на обзора върху ключовите предприятия и взаимодействието с тях — цялостното подобряване на способностите в областта на киберсигурността на национално и регионално равнище. Предпочитаният вариант на политика би осигурил в по-голяма степен и съгласуваността с други области на законодателството, инициативи или мерки на политиките, включително със специфични за секторите разпоредби *lex specialis*.

Намирането на решения за продължаващия понастоящем недостиг на подготвеност в областта на киберсигурността на равнището на държавите членки, дружествата и други

организации би довело до подобрения на ефективността и намаляване на допълнителните разходи, произтичащи от инциденти с киберсигурността.

- За съществените и значими субекти повишаването на степента на подготвеност в областта на киберсигурността би довело до смекчаване на потенциалните загуби на приходи поради смущения — включително поради промишлен шпионаж — и би намалило големите разходи за смекчаване на заплахите ad-hoc. Подобни ползи вероятно ще надделеят над необходимите инвестиционни разходи. Намаляването на фрагментирането на вътрешния пазар би подобрило и условията на равнопоставеност сред операторите.
- За държавите членки то допълнително би намалило риска от увеличаване на бюджетните разходи за смекчаване на заплахите ad-hoc и допълнителните разходи в случай на извънредни ситуации, свързани с инциденти с киберсигурността.
- За гражданите намирането на решения при инцидентите с киберсигурността се очаква да доведе до намаляване на загубите на приходи поради икономически смущения.

Повишените равнища на киберсигурност в държавите членки и способността на дружествата и органите да отговорят бързо на инцидент и да ограничат въздействието му най-вероятно ще доведат до повишаване на цялостното доверие на гражданите в цифровата икономика, което може да има положително въздействие върху растежа и инвестициите.

Повишаването на цялостното ниво на киберсигурност може да доведе до повишена сигурност като цяло и до безпрепятствено непрекъснато функциониране на основни услуги, които са от критично значение за обществото. Инициативата може да допринесе и за оказване на други видове обществено въздействие, като например понижени равнища на киберпрестъпността и тероризма и повишена гражданска защита. Повишаването на степента на подготвеност в областта на киберсигурността за предприятията и останалите организации може да доведе до избягване на потенциални финансови загуби в резултат на кибератаки, като по този начин ще предотврати нуждата от съкращаване на наети лица.

Повишаването на цялостното ниво на киберсигурността би довело и до превенция на рисковете/вредите, свързани с околната среда, в случай на атака срещу основна услуга. Това особено би се отнасяло до секторите на енергетиката, доставката и снабдяването с вода или транспорта. С укрепването на способностите в областта на киберсигурността инициативата би довела до по-широка употреба на последните поколения инфраструктури и услуги в областта на ИКТ, които също са по-устойчиви за околната среда, както и до замяната на неефикасната и по-малко сигурна остаряла инфраструктура. Очаква се това да допринесе и за намаляване на броя на скъпоструващите киберинциденти, като освободи ресурси, налични за устойчиви инвестиции.

- **Пригодност и опростяване на законодателството**

Предложението предвижда общо изключване на микросубектите и малките субекти от обхвата на МИС и по-лек надзорен режим с последващ (*ex-post*) надзор, прилаган спрямо голям брой от новите субекти съгласно преразгледания обхват (т. нар. значими субекти). Цел на мерките е да сведат до минимум и да балансират тежестта, на която са

подложени дружествата и органите на публичната администрация. Освен това предложението заменя сложна система за установяване на операторите на основни услуги с общоприложимо задължение и въвежда по-високо нивото на хармонизация на задълженията за сигурност и докладване, което би намалило тежестта за изпълнение, особено за субекти, предоставящи трансгранични услуги.

Предложението свежда до минимум разходите за привеждане в съответствие за малките и средните предприятия, тъй като от субектите се изисква да предприемат само онези мерки, необходими за гарантиране на ниво на сигурност на мрежите и информационните системи, които съответстват на съществуващия риск.

- **Основни права**

ЕС е поел ангажимент да осигури високи стандарти за защита на основните права. Всички насърчавани с настоящата директива доброволни договорености за обмен на информация между субектите биха се осъществявали в надеждна среда при пълно спазване на разпоредбите на Съюза за защита на данните, и особено на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[8].

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

Вж. финансовия фиш

5. ДРУГИ ЕЛЕМЕНТИ

- **Планове за изпълнение и механизъм за мониторинг, оценка и докладване**

Предложението включва общ план за мониторинг и оценка на въздействието върху конкретните цели, което изисква Комисията да извърши преглед поне [54 месеца] след датата на влизане в сила и да докладва на Европейския парламент и на Съвета за своите основни констатации.

Прегледът трябва да се извърши в съответствие с Насоките на Комисията за по-добро законотворчество.

- **Подробно разяснение на конкретните разпоредби на предложението**

Предложението е структурирано около няколко основни области на политиките, които са взаимосвързани и служат на целта да се повиши нивото на киберсигурност в Съюза.

Предмет и обхват (членове 1 и 2)

Директивата по-специално: а) установява задължения за държавите членки да приемат национална стратегия за киберсигурност, да определят компетентни национални органи, единни звена за контакт и ЕРИКС; б) предвижда държавите членки да определят за субектите, обозначени като съществени в приложение I и като значими в приложение II, задължения за управление на свързания с киберсигурността, и за докладване; в) предвижда държавите членки да определят задължения относно обмена на информация за киберсигурността.

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

Директивата се прилага по отношение на някои публичноправни или частноправни съществени субекти, упражняващи дейност в изброените в приложение I сектори (енергетика; транспорт; банково дело; инфраструктури на финансовия пазар; здравеопазване, питейна вода; отпадъчни води; цифрова инфраструктура; публична администрация и космическо пространство), както и на някои значими субекти, упражняващи дейност в изброените в приложение II сектори (пощенски и куриерски услуги; управление на отпадъците; производство на изделия и вещества и дистрибуция на химикали; производство, преработка и разпространение на храни; производствени и цифрови доставчици). Микропредприятията и малките предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. са изключени от обхвата на директивата, с изключение на доставчиците на електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги, доставчиците на удостоверителни услуги, регистрите на имената на домейни от първо ниво (TLD) и публичната администрация, както и на някои други субекти, като например единствени доставчици на дадена услуга в дадена държава членка.

Национални рамки за киберсигурност (членове 5—11)

От държавите членки се изисква да приемат национална стратегия за киберсигурност, в която са определени стратегическите цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на киберсигурност.

Директивата установява и рамка за координирано оповестяване на уязвимости и изисква държавите членки да определят ЕРИКС, които да действат като надеждни посредници и да улесняват взаимодействието между докладващите субекти и производителите или доставчиците на ИКТ продукти и услуги. ENISA трябва да разработи и поддържа Европейски регистър на уязвимостите за откритите такива.

От държавите членки се изисква да въведат национални рамки за управление на кризи в областта на киберсигурността, по-специално чрез определяне на национални компетентни органи, отговарящи за управлението на мащабни инциденти и кризи в тази област.

От държавите членки се изисква и да определят един или повече национални компетентни органи по киберсигурност за надзорните задачи съгласно настоящата директива, както и национално единно звено за контакт по киберсигурността (SPOC), което да изпълнява функция на свръзка, за да се осигури трансгранично сътрудничество на органите на държавите членки. От държавите членки се изисква също така да определят екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС).

Сътрудничество (членове 12—16)

С Директивата се създава група за сътрудничество с цел подкрепа и улесняване на стратегическото сътрудничество и обмен на информация между държавите членки и изграждане на доверие сред тях. Създава се и мрежа на ЕРИКС, с цел да се допринесе за изграждането на доверие между държавите членки и да се насърчи бързото и ефективно оперативно сътрудничество.

Създава се Европейска мрежа за връзка на организациите при кибернетични кризи (EU — CyCLONe) с цел подпомагане на координираното управление на мащабни

инциденти и кризи, свързани с киберсигурността, и осигуряване на редовния обмен на информация сред държавите членки и институциите на ЕС.

От ENISA се изисква да публикува в сътрудничество с Комисията двугодишен доклад за състоянието на киберсигурността в Съюза.

От Комисията се изисква да установи система за партньорска проверка, позволяваща редовни такива проверки на ефективността на политиките на държавите членки в областта на киберсигурността.

Управление на риска, свързан с киберсигурността, и задължения за докладване (членове 17—23)

Директивата изисква от държавите членки да гарантират, че управителните органи на всички субекти в обхвата одобряват мерките за управление на риска за киберсигурността, предприети от съответните субекти, и преминават свързано с киберсигурността специфично обучение.

От държавите членки се изисква да гарантират, че попадащите в обхвата субекти предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за киберсигурността на мрежите и информационните системи. Те трябва да гарантират също, че субектите уведомяват националните компетентни органи или ЕРИКС за всеки инцидент с киберсигурността, оказващ значимо въздействие върху предоставяната от тях услуга.

В регистрите на имената на домейни от първо ниво (TLD) и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво, следва да се събират и поддържат точни и пълни данни за регистрацията на имена на домейни. Освен това от тези субекти се изисква да предоставят ефикасен достъп до данните за регистрация на домейни за законно търсещите достъп.

Юрисдикция и регистрация (членове 24 и 25)

По правило съществените и значимите субекти се считат за попадащи под юрисдикцията на държавата членка, в която предоставят услугите си. Някои видове субекти обаче (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 и доставчиците на мрежи за предоставяне на съдържание, както и някои доставчици на цифрово съдържание) се считат за попадащи под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Съюза. Целта е да се гарантира, че тези субекти не се сблъскват с множество различни правни изисквания, тъй като те в особено висока степен предлагат трансгранични услуги. ENISA трябва да създаде и поддържа регистър на последния вид субекти.

Обмен на информация (членове 26 и 27)

Държавите членки трябва да предвидят разпоредби, позволяващи на субектите да участват в свързан с киберсигурността обмен на информация в рамките на конкретни договорености за обмен на информация за киберсигурността, в изпълнение на член 101 от ДФЕС. Освен това държавите членки трябва да позволят на субектите извън обхвата на настоящата директива да докладват доброволно значими инциденти, киберзаплахи или ситуации, близки до инциденти.

Надзор и правоприлагане (членове 28—34)

От компетентните органи се изисква да упражняват надзор върху субектите, попадащи в обхвата на директивата, и по-специално да гарантират спазването от тяхна страна на изискванията за сигурност и уведомяване за инциденти. Разграничава се между режим на предхождащ надзор (ex-ante) за съществените субекти и режим на последващ надзор (ex-post) за значимите субекти, като във втория случай от компетентните органи се изисква да предприемат действия, когато са получили доказателства или индикации, че значим субект не спазва изискванията за сигурност и уведомяване за инциденти.

Директивата изисква от държавите членки също да налагат административни глоби на съществените и значимите субекти и да определят някои максимални глоби.

От държавите членки се изисква при необходимост да си сътрудничат и да се подпомагат взаимно, когато субектите предоставят услуги в повече от една държава членка или когато основното място на установяване на субекта или негов представител се намира в дадена държава членка, но неговите мрежи и информационни системи са разположени в една или повече други държави членки.

2020/0359 (COD)

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

(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 Европейския икономически и социален комитет[9],

като взеха предвид становището на Комитета на регионите[10],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета[11] има за цел да изгради способности в областта на киберсигурността в Съюза, да ограничи заплахите за мрежите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и да гарантира непрекъснатостта на тези услуги при инциденти с киберсигурността, като по този начин допринася за ефективното функциониране на икономиката и обществото на Съюза.

(2) След влизането в сила на Директива (ЕС) 2016/1148 бе постигнат значителен напредък при повишаването на нивото на устойчивост на киберсигурността на Съюза. Прегледът на тази директива показа, че 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 чрез определянето на национални стратегии за киберсигурност, създаването на национални способности и изпълнението на регулаторни мерки, обхващащи съществени инфраструктури и участници, установени от всяка държава членка. Тя допринесе и за развитието на сътрудничеството на равнището на Съюза посредством установяването на групата за сътрудничество[12] и мрежа от национални екипи за реагиране при

---

9 ОВ С [...], [...] г., стр. [...].

10 ОВ С [...], [...] г., стр. [...].

11 Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194/1, 19.7.2016 г., стр. 1).

12 Член 11 от Директива (ЕС) 2016/1148.

инциденти с компютърната сигурност („мрежата на ЕРИКС“)[13]. 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 съвременните и възникващи предизвикателства в областта на киберсигурността.

(3) Мрежите 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 набора от заплахи, пораждайки нови такива, и изисква адаптирани, координирани и новаторски реакции във всички държави членки. Броят, мащабите, сложността, честотата и въздействието на свързаните със сигурността инциденти се увеличават и представляват крупна заплаха за функционирането на мрежите и информационните системи. В резултат на това киберинцидентите могат да попречат на извършването на стопански дейности в рамките на вътрешния пазар, да причинят финансови загуби, да подкопаят доверието на потребителите и да причинят големи 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.

(4) Правното основание за Директива (ЕС) 1148/2016 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 икономически относими дейности, 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 предприятията, 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 тези трансгранични дейности. Освен това възможността за неоптимално изготвяне или прилагане на стандарти за киберсигурност в една държава членка е вероятно да има последици по отношение на нивото на киберсигурност на държави членки, особено предвид интензивния трансграничен 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. Подобни различия в прилагането възникнаха и по отношение на разпоредбите на директивата 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 устойчивост в областта на киберсигурността поради прилагането на различни стандарти. Настоящата

[13] Член 12 от Директива (ЕС) 2016/1148.

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 ефективното 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 санкции, способстващи за ефективното правоприлагане на тези задължения. Поради това Директива (ЕС) 2016/1148 следва да бъде отменена и заменена с настоящата директива.

(6) Настоящата директива не засяга възможностите на всяка държава членка да предприема необходимите мерки, с които да гарантира защитата на основните интереси на своята сигурност, да опазва обществения ред и обществената сигурност и да създава условия за разследването, разкриването и наказателното преследване на престъпления, в съответствие с правото на Съюза. Съгласно член 346 ДФЕС нито една държава членка не може да бъде задължавана да предоставя информация, чието разкриване би противоречало на основните интереси на нейната обществена сигурност. В този контекст имат значение националните правила и тези на Съюза 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)[14].

(7) С отмяната на Директива (ЕС) 2016/1148 приложното поле следва да се разшири така, че да обхване по-голяма част от секторите на икономиката с оглед на доводите, изложени в съображения 4—6. Ето защо обхватът по отношение на секторите от Директива (ЕС) 2016/1148 следва да бъде разширен, за да се осигури пълно включване на секторите и услугите от жизненоважно значение за ключови обществени и икономически дейности във вътрешния пазар. Правилата не следва да се различават в зависимост от това дали субектите са оператори на основни услуги или доставчици на цифрови услуги. Това разграничаване е доказано остаряло, тъй като не отразява настоящата значимост на секторите или услугите за обществените и икономическите дейности във вътрешния пазар.

(8) В съответствие с Директива (ЕС) 2016/1148, държавите членки са отговорни за определянето на субектите, които отговарят на критериите и се квалифицират като оператори на основни услуги („процес по определяне“). За да се отстранят големите различия сред държавите членки в това отношение и да се гарантира правната сигурност относно изискванията за управление на риска и задълженията за докладване по отношение на всички относими субекти, следва да се установи еднакъв критерий, определящ субектите, попадащи в приложното поле на настоящата директива. Този критерий следва да се състои в прилагането на правилото за размер на предприятието, при което всички средни и големи предприятия, съгласно определението в Препоръка 2003/361/ЕО на Комисията[15], упражняващи дейност в секторите или предоставящи видовете услуги,

[14] Протоколът за обмен на информация с цветен код за поверителност (TLP) е средство за обменящото информация лице да уведоми своята аудитория за евентуални ограничения за по-нататъшното разпространение на тази информация. Използва се в почти всички общности на ЕРИКС и в някои Центрове за анализ и обмен на информация (ЦАОИ).

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

обхванати от настоящата директива, попадат в нейния обхват. От държавите членки не следва да се изисква да съставят списък със субектите, изпълняващи този общоприложим критерий по отношение на размера.

(9) При все това малки субекти или микросубекти, които изпълняват определени критерии, сочещи че те имащи ключова роля за икономиките и обществата на държавите членки или за конкретни сектори или видове услуги, също следва да бъдат обхванати от настоящата директива. Държавите членки следва да отговарят за съставянето на списък с такива субекти, който да предоставят на Комисията.

(10) Комисията, в сътрудничество с групата за сътрудничество, може да издава насоки за прилагането на критериите, приложими за микропредприятията и малки предприятия.

(11) В зависимост от сектора, в който упражняват дейност, или вида на предоставяната от тях услуга, попадащите в обхвата на настоящата директива субекти следва да бъдат класифицирани в две категории: съществени и значими. При тази категоризация следва да се отчитат степента на критичност на сектора или на вида услуга, както и степента на зависимост на други сектори или видове услуги. Както съществените, така и значимите субекти следва да бъдат подчинени на едни и същи изисквания за управление на риска и задължения за докладване. Режимите на надзор и санкции за тези две категории субекти следва да са различни, за да се гарантира справедлив баланс между изискванията и задълженията, от една страна, и административната тежест, произтичаща от надзора на изпълнението, от друга.

(12) Специфичните за сектора инструменти и законодателство могат да допринесат за осигуряване на високи нива на киберсигурност, като същевременно отчитат особеностите и сложността на тези сектори. Когато специфичен за сектора правен акт на Съюза изисква съществените или значимите субекти да приемат мерки за управление на риска, свързан с киберсигурността, или да уведомяват за инциденти или значителни киберзаплахи и тези изисквания имат поне равностоен ефект на предвидените в настоящата директива задължения, следва да се прилагат тези специфични за сектора разпоредби, включително относно надзора и правоприлагането. Комисията може да издава насоки във връзка с прилагането на *lex specialis*. Настоящата директива не изключва приемането на допълнителни специфични за сектора актове на Съюза, в които се уреждат мерките за управление на риска, свързан с киберсигурността, и уведомяванията за инциденти. Настоящата директива не засяга съществуващите изпълнителни правомощия, предоставени на Комисията в редица сектори, включително в транспорта и енергетиката.

(13) Регламент XXXX/XXXX на Европейския парламент и на Съвета[16] следва да се счита за специфичен за сектора правен акт на Съюза във връзка с настоящата директива с оглед на субектите във финансовия сектор. Разпоредбите на Регламент XXXX/XXXX във връзка с мерките за управление на риска в областта на информационните и комуникационните технологии (ИКТ), управлението на инцидентите при ИКТ и особено уведомяването за инциденти, както и тези относно изпитването на оперативната устойчивост на цифровите технологии,

16 *[да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

споразуменията за обмен на информация и риска при ИКТ, пораждан от участието на трети страни, следва да се прилагат вместо установените съгласно настоящата директива. Затова държавите членки не следва да прилагат разпоредбите на настоящата директива относно управлението на риска, свързан с киберсигурността, и задълженията за докладване, обмен на информация и надзор и правоприлагането по отношение на които и да е финансови субекти, обхванати от Регламент XXXX/XXXX. Същевременно е от значение да се поддържат тясна връзка и обмен на информация с финансовия сектор съгласно настоящата директива. За тази цел Регламент XXXX/XXXX позволява на всички финансови надзорни органи, Европейските надзорни органи (ЕНО) за финансовия сектор и националните компетентни органи съгласно Регламент XXXX/XXXX да участват в обсъжданията на стратегическите цели и на техническите аспекти на работата на групата за сътрудничество, както и да обменят информация и да сътрудничат с единните звена за контакт, определени в изпълнение на настоящата директива, и с националните ЕРИКС. Компетентните органи съгласно Регламент XXXX/XXXX следва да предоставят подробности за големи инциденти с ИКТ и на единните звена за контакт, определени в изпълнение на настоящата директива. Освен това държавите членки следва да продължат да включват финансовия сектор в своите стратегии за киберсигурност, а дейностите на националните ЕРИКС могат да обхващат и него.

(14) С оглед на взаимовръзките между киберсигурността и физическата сигурност на субектите следва да се осигури съгласуван подход между Директива (ЕС) XXX/XXX на Европейския парламент и на Съвета[17] и настоящата директива. За постигането на тази цел държавите членки следва да гарантират, че критичните и равностойни на тях субекти съгласно Директива (ЕС) XXX/XXX се считат за съществени субекти по силата на настоящата директива. Държавите членки следва също така да гарантират, че стратегиите им за киберсигурност предвиждат рамка за политики за усъвършенствана координация между компетентния орган съгласно настоящата директива и компетентния орган съгласно Директива (ЕС) XXX/XXX в контекста на обмена на информация относно инциденти и киберзаплахи и упражняването на задачи по надзор. Органите съгласно двете директиви следва да си сътрудничат и да обменят информация, по-специално във връзка с установяването на критични субекти, киберзаплахи, рискове за киберсигурността, инциденти, засягащи критичните субекти, както и относно предприети от тези субекти мерки за киберсигурност. При поискване от компетентните органи съгласно Директива (ЕС) XXX/XXX на компетентните органи съгласно настоящата директива следва да бъде разрешено да упражняват своите правомощия по надзор и правоприлагане спрямо съществен субект, определен като критичен. За целта двата органа следва да си сътрудничат и да обменят информация.

(15) Поддържането и запазването на надеждна, устойчива и сигурна система за имена на домейни (DNS) е ключов фактор за запазването на целостта на интернет и е 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 всички доставчици на DNS услуги по веригата

[17] *[да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

на преобразуване на DNS, включително операторите на базови сървъри за имена на домейни, сървъри за имена на домейни от първо ниво (TLD), сървъри за окончателно или рекурсивно преобразуване на имена на домейни.

(16) Компютърните услуги „в облак“ следва да обхващат услуги, позволяващи широк отдалечен достъп при поискване до променлив по мащаб и еластичен набор от разпределени компютърни ресурси, които могат да бъдат ползвани съвместно. Тези компютърни ресурси включват ресурси като мрежи, сървъри или друга инфраструктура, операционни системи, софтуер, средства за съхранение, приложения и услуги. Моделите на внедряване на компютърни услуги „в облак“ следва да включват частен, общностен, публичен и хибриден облак. Горепосочените модели за внедряване и предоставяне на услуги 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, 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.

(17) Предвид възникването на новаторски технологии и нови бизнес модели се очаква на пазара да се появят нови модели за внедряване и предоставяне 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“).

(18) 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 мрежите и информационните системи, настоящата директива следва 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“ не се прилага по отношение на вътрешни, корпоративни центрове за данни, притежавани и използвани за собствени цели на съответния субект.

(19) Доставчиците на пощенски услуги по смисъла на Директива 97/67/ЕО на Европейския парламент и на Съвета[18], както и доставчиците на експресни и куриерски услуги, следва да са подчинени на настоящата директива, ако предоставят поне една от операциите от веригата на пощенски доставки, и по-специално събирането, сортирането или доставката, включително услугите за вземане от адрес. Превозът, когато не е предприет във връзка с някоя от тези операции, следва да попада извън обхвата на пощенските услуги.

(20) Тази нарастваща взаимозависимост е резултат от все по-трансграничния и взаимообвързан характер на мрежата за доставка на услуги, използваща ключови инфраструктури в целия Съюз, в секторите енергетика, транспорт, цифрова инфраструктура, питейна 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 космическите му програми). 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. Пандемията от COVID-19 показа колко са уязвими нашите все по-взаимозависими общества за рискове с ниска вероятност.

(21) 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 повече от един национален компетентен орган, отговарящ за изпълнение на задачите, свързани със сигурността на мрежите и информационните системи на съществени и значими субекти съгласно настоящата директива. Държавите членки следва да могат да възлагат тези функции на съществуващ орган.

(22) 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 национално единно звено за контакт, което да отговаря за координацията на въпросите, свързани със

[18] Директива 97/67/ЕО на Европейския парламент и на Съвета от 15 декември 1997 година 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).

сигурността на мрежите и информационните системи, и за трансграничното сътрудничество на равнището на Съюза.

(23) Компетентните органи или ЕРИКС следва да получават уведомления за инциденти от субектите по ефективен и ефикасен начин. На единните звена за контакт следва да се възложи задачата да предават уведомленията за инциденти на единните звена за контакт на други засегнати държави членки. На равнището на органите на държавите членки, с цел да се осигури едно-единствено звено за контакт във всяка от държавите членки, единните звена за контакт следва да са и адресатите за относима информация за инциденти, засягащи субекти от финансовия сектор, постъпваща от компетентните органи съгласно Регламент XXXX/XXXX, която те следва при необходимост да могат да препращат на съответните национални компетентни органи или ЕРИКС съгласно настоящата директива.

(24) Държавите членки следва да разполагат с достатъчно технически и организационен капацитет, за да предотвратяват, идентифицират, реагират и ограничават инцидентите и рисковете в мрежите и информационните системи. Ето защо държавите членки следва да гарантират, че разполагат с добре функциониращи ЕРИКС, известни още като екипи за незабавно реагиране при компютърни инциденти (CERT), които да отговарят на основните изисквания, за да се гарантират ефективни и съвместими способности за справяне с инциденти и рискове и да се осигури ефективно сътрудничество на равнището на Съюза. С цел да се подобри връзката на доверие между субектите и ЕРИКС, когато ЕРИКС е част от компетентния орган, държавите членки следва 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.

(25) По отношение на личните данни ЕРИКС следва да могат да предоставят, в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[19] във връзка с личните данни, от името на субект и при поискване от негова страна съгласно настоящата директива, активно сканиране на мрежите и информационните системи, използвани за предоставянето на техните услуги. Държавите членки следва да имат за цел да гарантират еднакво равнище на технически възможности за всички секторни ЕРИКС. Държавите членки могат да поискат помощ от Агенцията на Европейския съюз за киберсигурност (ENISA) при създаването на националните ЕРИКС.

(26) 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.

(27) В съответствие с приложението към Препоръка (ЕС) 2017/1548 на Комисията относно координирана реакция на мащабни киберинциденти и кризи

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

(„концепция“)[20], мащабен инцидент следва да означава инцидент със значително въздействие върху поне две държави членки или инцидент, смущението от който надхвърля капацитета за отговор на една държава членка. В зависимост от причината и въздействието си, мащабните инциденти може да се разраснат и да се превърнат в същински кризи, непозволяващи правилното функциониране на вътрешния пазар. Предвид широкомащабния обхват и, в повечето случаи, трансграничния характер на такива инциденти, държавите членки и съответните институции, органи и служби на Съюза следва да си сътрудничат на техническо, оперативно и политическо равнище за правилно координиране на отговора в Съюза.

(28) Тъй като злонамереното използване на уязвимостите в мрежите и информационните системи може да причини значителни смущения и вреди, бързото установяване и отстраняване на тези уязвимости е важен фактор за намаляване на риска за киберсигурността. Затова субектите, които изграждат такива системи, следва да установят подходящи процедури за справяне с уязвимостите, които са открити. Тъй като уязвимостите често се откриват и докладват (оповестяват) от трети страни (докладващи субекти), производителят или доставчикът на ИКТ продукти или 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 29417 предоставят насоки съответно за справянето с уязвимости и за тяхното оповестяване. По отношение на оповестяването на уязвимости от особено значение е координацията между докладващите субекти и производителите или доставчиците на ИКТ продукти или услуги. С координираното оповестяване на уязвимостите се определя структуриран процес, чрез който те се докладват на организациите по начин, позволяващ на последните да диагностицират и отстранят уязвимостта преди разкриването на подробна информация за нея на трети страни или на обществеността. Координираното оповестяване на уязвимостите следва да включва и координиране между докладващия субект и организацията по отношение на графика за отстраняване и публикуване на уязвимостите.

(29) Ето защо държавите членки следва да предприемат мерки за улесняване на координираното оповестяване на уязвимостите, като установят съответна национална политика. В това отношение държавите членки следва да определят ЕРИКС, който да поеме ролята на „координатор“, при необходимост действащ като посредник между докладващите субекти и производителите или доставчиците на ИКТ продукти или услуги. Задачите на координиращия ЕРИКС следва по-специално да включват установяването на съответните субекти и осъществяването на контакт с тях, подпомагането на докладващите субекти, договарянето на графици за оповестяване и управлението на уязвимостите, засягащи множество организации (многостранно оповестяване на уязвимостите). Когато уязвимостите засягат множество производители или доставчици на ИКТ продукти или услуги, установени в повече от една държава членка, определените ЕРИКС от всяка от засегнатите държави членки следва да си сътрудничат в рамките на мрежата на ЕРИКС.

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

(30) Достъпът до вярна и своевременна информация относно уязвимостите, засягащи ИКТ продукти и услуги, допринася за подобрено управление на риска, свързан с киберсигурността. В това отношение източниците на публично достъпна информация относно уязвимостите са важен инструмент за субектите и техните потребители, но също и за националните компетентни органи и ЕРИКС. Поради тази причина ENISA следва да създаде регистър на уязвимостите, където съществените и значимите субекти и техните доставчици, както и субектите, които не попадат в приложното поле на настоящата директива, могат доброволно да разкриват уязвимости и да предоставят информация за тях, позволяваща на потребителите да предприемат подходящи ограничаващи мерки.

(31) При все че подобни регистри или бази данни за уязвимости съществуват, те се предоставят и поддържат от установени извън ЕС субекти. Един поддържан от ENISA Европейски регистър на уязвимостите би осигурил повишена прозрачност относно процеса на публикуване преди официалното разкриване на уязвимостта, както и устойчивост в случаи на смущения или прекъсвания при предоставянето на подобни услуги. За да се избегне дублиране на усилията и да се постигне взаимно допълване във възможно най-висока степен, ENISA следва да разгледа възможността за сключване на споразумения за структурирано сътрудничество с подобни регистри под юрисдикцията на трети страни.

(32) Групата за сътрудничество следва да съставя работна програма на всеки две години, включваща действията, които да предприема за изпълнение на своите цели и задачи. Времевата рамка на първата програма, приета съгласно настоящата директива, следва да е синхронизирана с времевата рамка на последната програма, приета съгласно Директива (ЕС) 2016/1148, за да се избегнат потенциални смущения в работата на групата.

(33) 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, които да се следват посредством по-доброто прилагане на съществуващите правила.

(34) 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 следва да организира редовни съвместни заседания с относимите частни заинтересованите страни от Съюза с цел обсъждане на дейностите, извършвани от групата, и събиране на информация относно възникващите предизвикателства пред политиките. С цел подобряване на сътрудничество на равнището на Съюза групата следва да разгледа възможността да покани работещите в областта на политиките за киберсигурност органи и служби на Съюза, като например Европейския център за борба с киберпрестъпността (ЕС3), Агенцията за авиационна безопасност на Европейския съюз (ЕААБ) и Агенцията на Европейския съюз за космическата програма (EUSPA), да участват в нейната работа.

(35) На компетентните органи и ЕРИКС следва да бъдат предоставени правомощия да участват в схеми за обмен на длъжностни лица от други държави членки с цел подобряване на сътрудничеството. 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.

(36) При необходимост Съюзът следва да сключва международни споразумения в съответствие с член 218 ДФЕС с трети държави или международни организации, които допускат и уреждат участието им в някои дейности на групата за сътрудничество и мрежата на ЕРИКС. Тези споразумения следва да гарантират адекватна защита на данните.

(37) 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, посредством съществуващите мрежи за сътрудничество, особено мрежата за връзка на организациите при кибернетични кризи (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. В процедурния правилник на EU-CyCLONe следва допълнително да бъдат посочени редът и условията, при които следва да функционира мрежата, включително (но не само) ролите, режимите 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 за реакция на политическо равнище при кризи (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 (ОПСО), следва да бъде активиран Механизмът за реакция при кризи (CRM) на Европейската служба за външна дейност (ЕСВД).

(38) За целите на настоящата директива, понятието „риск“ следва да се отнася до потенциала за възникване на загуба или смущение в резултат на инцидент с киберсигурността, и да се изразява като комбинация от мащаба на загубата или смущението и вероятността за настъпване на въпросния инцидент.

(39) За целите на настоящата директива понятието „ситуации, близки до инциденти“ следва да се отнася до събитие, което потенциално е можело да причини вреда, но неговото пълно настъпване е било успешно предотвратено.

(40) Мерките за управление на риска следва да включват мерки за идентифициране на всякакви рискове от инциденти с цел предотвратяване, откриване и справяне с инциденти, както и ограничаване на тяхното въздействие. Сигурността на мрежите и информационните системи следва да включва сигурността на данните, които се съхраняват, предават и обработват.

(41) С цел да се избегне налагането на непропорционална финансова и административна тежест върху съществените и значимите субекти, изискванията за управление на риска, свързан с киберсигурността, следва да бъдат пропорционални на риска, който съществува по отношение на съответната мрежа и информационна система, като се отчитат последните достижения в областта на тези мерки.

(42) Съществените и значимите субекти следва да гарантират сигурността на мрежите и информационните системи, които използват в своите дейности. Това са предимно частни мрежи и информационни системи, управлявани от вътрешен ИТ персонал или чиято сигурност е възложена на външни изпълнители.

Изискванията за управлението на риска, свързан с киберсигурността, и за докладване съгласно настоящата директива следва да се прилагат по отношение на съответните съществени и значими субекти без оглед на това дали те извършват вътрешно поддръжка на своите мрежи и информационни системи или я възлагат на външни изпълнители.

(43) Справянето с рискове за киберсигурността, коренящи се във веригата на доставки на даден субект и отношенията му с доставчиците, е от особено значение предвид преобладаващия брой на инцидентите, при които субекти стават жертва на кибератаки или сигурността на техните мрежи и информационни системи бива компрометирана от злонамерено действащи лица благодарение на уязвимостите, засягащи продукти и услуги на трети страни. Затова субектите следва да преценяват и вземат предвид цялостното качество на продуктите и практиките на своите доставчици на продукти и услуги в областта на киберсигурността, включително техните процедури за сигурно разработване.

(44) Сред доставчиците на услуги тези, предоставящи услуги за управление на сигурността в области като реагиране при инциденти, проверка за проникванията, одити за сигурността и консултантски услуги, играят особено важна роля в оценката на усилията на субектите за идентифициране и реагиране на инциденти. Самите тези доставчици на услуги за управление на сигурността обаче също са цел на кибератаки и посредством тяхното тясно интегриране в дейностите на операторите пораждат особен риск за киберсигурността. Ето защо субектите следва да подхождат с повишено внимание към избора на доставчик на услуги за управление на сигурността.

(45) Субектите следва да намерят решения и за рискове за киберсигурността, произтичащи от взаимодействията и отношенията им с други заинтересовани страни в рамките на една по-широка екосистема. Субектите 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 субектите, те трябва да предприемат всички необходими мерки за киберсигурност, когато ползват услуги на трети страни за преобразуването и анализа на данните.

(46) За да се отговори допълнително на рисковете по веригата на доставка и да се подпомогнат субектите, упражняващи дейност в обхванати от настоящата директива сектори, правилно да управляват веригата на доставка и свързаните с доставчика рискове за киберсигурността, групата за сътрудничество, включваща съответните национални органи, в сътрудничество с Комисията и ENISA, следва да извърши координирани секторни оценки на веригата на доставка, както това бе вече направено за 5G мрежите в съответствие с Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите[21], с цел да се установи за всеки сектор кои са критичните ИКТ услуги, системи или продукти, относимите заплахи и уязвимости.

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

(47) С оглед на характеристиките на съответния сектор, в секторните оценки на веригата на доставка следва да се вземат предвид техническите и, когато е уместно, нетехническите фактори, включително определените в Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите, в координираната в целия ЕС оценка на риска на сигурността 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, следва да бъдат взети предвид следните критерии: i) степента, в която съществените и значимите субекти използват и разчитат на конкретни критични ИКТ услуги, системи или продукти; ii) значението на конкретни критични ИКТ услуги, системи или продукти за изпълнението на критични или чувствителни функции, включително обработването на лични данни; iii) наличието на алтернативни ИКТ услуги, системи или продукти; iv) устойчивостта на цялостната верига на доставки на ИКТ услуги, системи или продукти срещу смущаващи събития и v) за възникващи ИКТ услуги, системи или продукти, тяхната потенциална бъдеща значимост за дейностите на субектите.

(48) С цел да се облекчат правните задължения, наложени на доставчиците на обществени електронни съобщителни мрежи или общественодостъпни електронни съобщителни услуги и на доставчиците на удостоверителни услуги, свързани със сигурността на техните мрежи и информационни системи, както и за да се даде възможност на тези субекти и съответните компетентни органи да се възползват от установената с настоящата директива правна рамка (включително определяне на ЕРИКС, отговарящ за управлението на рисковете и инцидентите, участие на компетентните органи и служби в работата на групата за сътрудничество и мрежата на ЕРИКС), те следва да бъдат включени в приложното поле на настоящата директива. Ето защо съответстващите разпоредби, предвидени в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[22] и Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета[23], отнасящи се до налагането на мерки за сигурност и уведомяване по отношение на тези видове субекти, следва да бъдат отменени. Правилата относно задълженията за докладване не следва да засягат Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО на Европейския парламент и на Съвета[24].

(49) Когато е целесъобразно и за да се избегнат ненужни смущения, съществуващите национални насоки и законодателство, приети за транспониране на правилата, свързани с мерките за сигурност по член 40, параграф 1 от Директива (ЕС) 2018/1972, както и на изискванията по член 40, параграф 2 от същата директива относно параметрите, свързани със значимостта на инцидент, следва да

---

22 Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година 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).

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

24 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година 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).

продължат да се използват от компетентните органи, отговарящи за надзора и правоприлагането за целите на настоящата директива.

(50) Предвид нарастващото значение на междуличностните съобщителни услуги без номерà, е необходимо да се гарантира, че и за тях се прилагат подходящи изисквания за сигурност с оглед на тяхната специфика и икономическо значение. Така доставчиците на такива услуги следва също да осигурят ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск. 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 риск за 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, при които се използват номерà и не се упражнява действителен контрол върху преноса на сигнали.

(51) Вътрешният пазар разчита на функционирането на интернет повече от всякога. Услугите на практически всички съществени и значими субекти са зависими от предоставяните по интернет услуги. За да се осигури гладкото предоставяне на услуги от страна на съществените и значимите субекти, от значение е обществените електронни съобщителни мрежи, като например опорните мрежи на интернет или подводните комуникационни кабели, да имат въведени подходящи мерки за киберсигурност и да докладват за свързаните с тях инциденти.

(52) Когато е подходящо, субектите следва да уведомяват получателите на техните услуги за конкретни и значими заплахи, както и за мерките, които тези получатели могат да предприемат за ограничаване на произтичащия за тях риск. Изискването да се уведомяват тези получатели за такива заплахи не следва да освобождава субектите от задължението да предприемат за своя сметка подходящи и незабавни мерки за предотвратяване или отстраняване на каквито и да било киберзаплахи и да възстановят нормалното ниво на сигурност на услугата. Предоставянето на получателите на такава информация относно заплахите за сигурността следва да бъде безплатно.

(53) Доставчиците на обществени електронни съобщителни мрежи или на обществено достъпни електронни съобщителни услуги следва по-специално да информират получателите на услуги за конкретни и значителни киберзаплахи и за мерките, които те могат да предприемат, за да защитят сигурността на своите съобщения, например чрез използване на специални типове софтуер или технологии за криптиране.

(54) С цел да се защити сигурността на електронните съобщителни мрежи и услуги следва да се насърчи използването на криптиране, и по-специално на криптиране от край до край, като при необходимост то следва да стане задължително за доставчиците на такива услуги и мрежи в съответствие с принципите за сигурност и поверителност по подразбиране и на етапа на проектиране на целите по член 18. 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 разследване, установяване и наказателно преследване на престъпления в съответствие с правото на Съюза. Решенията по отношение на законосъобразния достъп до информация при комуникации с криптиране от край

до край следва да запазват ефективността на криптирането при защитата на неприкосновеността и сигурността на комуникациите и същевременно да дават ефективен отговор на престъпността.

(55) С настоящата директива се определя двуетапен подход по отношение на докладването на инциденти с цел да се постигне подходящ баланс между бързото докладване, което подпомага ограничаването на потенциалното разпространение на инциденти и позволява на субектите 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 устойчивостта на киберзаплахи на отделни дружества или цели сектори, от друга. От субектите следва да се изисква да направят първоначално уведомление в рамките на 24 часа, след като са узнали за инцидент, и да изготвят окончателен доклад в срок от един месец. В първоначалното уведомление следва да се посочва само информацията, която е строго необходима на компетентните органи и позволява на субекта да потърси подкрепа, ако е необходимо. В такова уведомление, когато е приложимо, се посочва дали се предполага, че инцидентът се дължи на незаконосъобразно или злонамерено действие. Държавите членки следва да гарантират, че изискването за подаване на такова първоначално уведомление не отклонява ресурсите на докладващия субект от дейностите по справяне с инцидента, които следва да имат приоритет. За да се гарантира още по-добре, че задълженията за докладване на инциденти нито отклоняват ресурси от дейностите по справяне с инцидента, нито затормозяват по някакъв друг начин на усилията на субекта в това отношение, държавите членки следва да предвидят разпоредба, че в надлежно обосновани случаи и при споразумение с компетентните органи или ЕРИКС съответният субект може да се отклони от 24-часовия срок за първоначалното уведомление и едномесечния срок за окончателния доклад.

(56) Съществените и значимите субекти 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 допълнителни пречки и могат да доведат и до несигурност с оглед на формата и процедурите на такива уведомления. С оглед на това и с цел опростяване на докладването за инциденти със сигурността държавите членки следва да установят *единна входяща точка* за всички уведомления, изисквани съгласно настоящата директива, както и съгласно останалото право на Съюза, като например Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО. ENISA следва да разработи съвместно с групата за сътрудничество общи образци на уведомления посредством насоки, които биха опростили и оптимизирали изискваната съгласно правото на Съюза докладвана информация и биха намалили тежестите за дружествата.

(57) 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 значимите 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.

(58) 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 за защита на личните данни и надзорните органи съгласно Директива 2002/58/ЕО.

(59) Поддържането на точни и пълни бази данни с имена на домейни и данни за регистрация (т. нар. „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 свои ред допринася за по-високо ниво на киберсигурност в Съюза. Когато обработването включва лични данни, то следва да е в съответствие с правото на Съюза в областта на защитата на данните.

(60) Наличността и своевременната достъпност на тези данни за публичните органи, включително за компетентните органи съгласно правото на Съюза или националното право за предотвратяване, разследване или наказателно преследване на престъпления, CERT, ЕРИКС, и — по отношение на данните на техните клиенти — за доставчиците на електронни комуникации мрежи и услуги и на технологии и услуги в областта на киберсигурността, действащи от името на тези клиенти, са от съществено значение за предотвратяването и борбата със злоупотребите по отношение на системата за имена на домейни, по-специално за предотвратяване, разкриване и реагиране на инциденти с киберсигурността. Този достъп следва да е в съответствие с правото на Съюза за защита на личните данни, доколкото е свързан с този вид данни.

(61) 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 от първо ниво (т. нар. регистратори), следва да събират и гарантират целостта и наличността на данните за регистрация на имената на домейни. По-специално регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво, следва да установят политики и процедури за събиране и поддържане на точни и пълни данни за регистрация, както и да предотвратяват и поправят неточни такива данни в съответствие с правилата на Съюза за защита на данните.

(62) Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да правят публично достъпни данните за този вид регистрация, попадащи извън обхвата на правилата на Съюза за защита на данните, като например отнасящите се до юридическите лица[25]. Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях 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

[25] РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА, съображение (14), съгласно което „[н]астоящият регламент не обхваща обработването на лични данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка на юридическото лице“.

търсещите достъп, в съответствие с правото на Съюза за защита на данните. Държавите членки следва да гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да отговарят незабавно на искания от законно търсещи достъп за разкриване на данни за регистрация на имена на домейни. Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях 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. Процедурите за достъп може 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 приеме насоки относно такива процедури, без да се засягат правомощията на Европейския комитет по защита на данните.

(63) Всички съществени и значими субекти съгласно настоящата директива следва да попадат под юрисдикцията на държавата членка, в която предоставят своите услуги. Ако предоставя услуги 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 действия по надзор.

(64) За да се вземат предвид трансграничният характер на услугите и операциите на доставчиците на DNS услуги, регистрите на имената на домейни от първо ниво, доставчиците на мрежи за предоставяне на съдържание, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни и доставчици на цифрово съдържание, само една държава членка следва да има юрисдикция по отношение на тези субекти. Юрисдикцията следва да се предоставя на държавата членка, в която съответният 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 мрежи 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 бъде мястото, където в Съюза се вземат решенията във връзка с мерките по управлението на риска за киберсигурността. То обикновено съответства на мястото на централното управление на дружествата в Съюза. Ако такива решения не се вземат в Съюза, за основно място на установяване следва се считат държавите членки, в които 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.

(65) В случаи, при които доставчик на DNS услуги, регистър на имена на домейни от първо ниво, доставчик на мрежи за предоставяне на съдържание, доставчик на

компютърни услуги „в облак“, доставчик на услуги на център за данни и цифров доставчик, които не са установени в Съюза, предлагат услуги на негова територия, те следва да определят представител. За да се установи дали този субект предлага услуги в Съюза, следва да се установи дали е видно, че 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 и други данни за контакт, или използването на език, който широко се използва в третата държава, в която е установен субектът, не е достатъчна, 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 друг език, или посочването на потребители или ползватели на територията на Съюза, може 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 свържат с представителя. Представителят следва да е определен изрично чрез упълномощаване в писмена форма от доставчика да действа от негово име във връзка със задълженията му съгласно настоящата директива, включително за докладването на инциденти.

(66) Когато информация, считана за класифицирана съгласно правото на Съюза, се обменя, докладва или споделя по друг начин съгласно разпоредбите на настоящата директива, следва да се прилагат съответните конкретни правила относно предприемането на действия по нея.

(67) Предвид нарастването на сложността и професионализма на киберзаплахите качеството на мерките за разкриване и 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 заплахи в действителни 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 редица фактори изглежда са възпрепятствали такъв обмен на информация, по-специално несигурността относно съвместимостта с правилата за конкуренцията и отговорността.

(68) Субектите следва да бъдат насърчавани колективно да вложат своите лични познания и практически опит на стратегическо, тактическо и оперативно равнище с цел подобряване на способностите си за адекватен достъп, наблюдение, защита срещу и отговор на киберзаплахи. Затова е необходимо на равнището на Съюза да се даде възможност за възникването на механизми за договорености за доброволен обмен на информация. За тази цел държавите членки следва активно да подкрепят и насърчават и съответните субекти, които не попадат в обхвата на настоящата директива, да участват в тези механизми за споделяне на информация. Въпросните механизми следва да бъдат използвани в пълно съответствие с правилата за конкуренцията на Съюза, както и с правилата на Съюза за защита на данните.

(69) Обработването на личните данни, в степента, строго необходима и пропорционална за гарантиране на сигурността на мрежите и информацията от субектите, публичните органи, CERT, ЕРИКС и доставчиците на технологии и услуги в областта на сигурността, следва да представлява законен интерес на

съответния администратор на данни, съгласно посоченото в Регламент (ЕС) 2016/679. Това следва да включва мерки, свързани с предотвратяването, разкриването, 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, както и доброволния обмен на информация за тези инциденти, за киберзаплахи и уязвимости, показатели за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране. Тези мерки може да изискват обработването на следните видове лични данни: IP адреси, унифицирани указатели на ресурс (URL), имена на домейни и адреси на електронна поща.

(70) За да се засилят правомощията и действията по надзор, подпомагащи осигуряването на ефективно изпълнение, настоящата директива следва да предостави минимален списък с действия и средства по надзор, чрез които компетентните органи може да осъществяват надзор върху съществените и значимите субекти. Освен това с настоящата директива следва да се разграничат режимите на надзор за съществените и за значимите субекти, за да гарантира справедлив баланс на задълженията както за субектите, така и за компетентните органи. Така съществените субекти следва да са подчинени на напълно изразен режим на надзор (предхождащ и последващ), докато значимите субекти следва да са подчинени на по-лек режим, включващ само последващ надзор. Това означава, че във втория случай значимите субекти не следва да документират систематично изпълнението на изискванията за управлението на риска, свързан с киберсигурността, а компетентните органи следва да прилагат подход с *последващ* надзор, поради което няма да имат общо задължение за осъществяване на надзор върху тези субекти.

(71) За да се осъществи ефективното правоприлагане, следва да бъде създаден минимален списък с административни санкции за нарушение на управлението на риска, свързан с киберсигурността, и задълженията за докладване, предвидени от настоящата директива, като се установи ясна и последователна рамка за такива санкции в Съюза. Дължимо внимание следва да се обърне на естеството, тежестта и продължителността на нарушението, действително причинените вреди или понесените загуби, потенциалните вреди или загуби, преднамерения или неумишлен характер на нарушението, действията, предприети за предотвратяване или намаляване на претърпените вреди и/или загуби, степента на отговорност или евентуални относими предходни нарушения, степента на сътрудничество с компетентния орган и всякакъв друг утежняващ или смекчаващ фактор. Налагането на санкции, включително административни глоби, следва да подлежи на подходящи процедурни гаранции в съответствие с общите принципи на правото на Съюза и Хартата на основните права на Европейския съюз, включително ефективна съдебна защита и справедлив съдебен процес.

(72) 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.

(73) Когато административната глоба се налага на предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с членове 101 и 102 от ДФЕС за тези цели. При налагане на административни глоби на лица, които не са предприятие, надзорният орган следва да има предвид

общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, за да определи 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.

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

(75) Когато административните наказания не са хармонизирани в настоящата директива или при необходимост в други случаи, например при сериозни нарушения на задълженията по настоящата директива, държавите членки следва да прилагат система, която предвижда ефективни, пропорционални и възпиращи санкции. Естеството на тези санкции, наказателни или административни, следва да бъде определено съгласно правото на държавата членка.

(76) За допълнително засилване на ефективността и убедителността на санкциите, приложими за нарушенията на задълженията съгласно настоящата директива, компетентните органи следва да разполагат с правомощия да прилагат санкции, състоящи се в прекратяване на удостоверение или разрешение за всички или част от услугите, предоставяни от съществен субект, и налагането на временна забрана за упражняване на управленски функции от физическо лице. Предвид тежестта и въздействието върху дейностите на субектите и в крайна сметка върху техните потребители, тези санкции следва да се прилагат само пропорционално на тежестта на нарушението и да отчитат конкретните за всеки случай обстоятелства, включително предумишлен или непредумишлен характер на нарушението, действията, предприети за предотвратяване или ограничаване на претърпените щети и/или загуби. Тези санкции следва да се прилагат единствено като ultima ratio, т.е. само след като останалите относими действия по правоприлагане, предвидени от настоящата директива, са били изчерпани, и само докато субектите, към които те се прилагат, предприемат необходимото действие за отстраняване на недостатъците или изпълнение на изискванията на компетентния орган, за които се отнасят тези санкции. Налагането на такива санкции подлежи на подходящи процедурни гаранции в съответствие с общите принципи на правото на Съюза и Хартата на основните права на Европейския съюз, включително ефективна съдебна защита, справедлив процес, презумпция за невиновност и право на защита.

(77) Настоящата директива следва да установи правила за сътрудничество между компетентните органи и надзорните органи в съответствие с Регламент (ЕС) 2016/679 с цел справяне със свързаните с личните данни нарушения.

(78) Настоящата директива следва да има за цел да гарантира високо равнище на отговорност при мерките за управление на риска, свързан с киберсигурността, и задълженията за докладване на равнището на организациите. Поради тези съображения управителните органи на субектите, попадащи в обхвата на

настоящата директива, следва да одобряват мерките за управление на рисковете за киберсигурността и да осъществяват надзор върху тяхното изпълнение.

(79) Следва да бъде въведен механизъм за партньорска проверка, позволяващ прилагането на политиките в областта на киберсигурността, включително равнището на способностите и наличните ресурси на държавите членки, да се оценява от експерти, определени от държавите членки.

(80) За да се вземат предвид новите киберзаплахи, технологическото развитие или секторните особености, правомощието за приемане на актове в съответствие с член 290 ДФЕС следва да бъде делегирано на Комисията при спазване на елементите във връзка с мерките за управление на риска, изисквани от настоящата директива. Комисията следва да разполага и с правомощия да приема делегирани актове, определящи от кои категории съществени субекти се изисква да получават удостоверение, както и съгласно кои конкретни европейски схеми за удостоверяване на киберсигурността. От особена важност е по време на подготвителната работа Комисията да проведе подходящи консултации, включително на експертно равнище, и те да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество[26]. 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.

(81) За да се осигурят еднакви условия за прилагането на относимите разпоредби на настоящата директива във връзка с процедурните правила, необходими за функционирането на групата за сътрудничество, техническите елементи, свързани с мерките за управление на риска или вида на информацията, формата и процедурата за уведомяване за инциденти, на Комисията следва да бъдат предоставени изпълнителни правомощия. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета[27].

(82) Комисията следва периодично да извършва преглед на настоящата директива, като се консултира със заинтересованите страни, по-специално с цел установяване на необходимостта от изменения предвид промените в обществените, политически, технологични или пазарни условия.

(83) Тъй като 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

[26] ОВ L 123, 12.5.2016 г., стр. 1.

[27] Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 година 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).

същия член, настоящата директива не надхвърля необходимото за постигане на тази цел.

(84) Настоящата директива зачита основните права и спазва принципите, признати в Хартата на основните права на Европейския съюз, и по-специално правото на зачитане на личния живот и тайната на съобщенията, защитата на личните данни, свободата на стопанската инициатива, правото на собственост, правото на ефективни правни средства за защита и правото на изслушване. Настоящата директива следва да бъде прилагана в съответствие с посочените права и принципи,

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

ГЛАВА I

Общи разпоредби

Член 1

Предмет

1. С настоящата директива се установяват мерки с цел осигуряване на високо общо ниво на киберсигурност в Съюза.

2. За тази цел с настоящата директива:

а) се установяват задължения за държавите членки да приемат национални стратегии за киберсигурност, да определят компетентни национални органи, единни звена за контакт и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС);

б) се установяват задължения за управление на риска, свързан с киберсигурността, и за докладване за субекти от видове, определени като съществени в приложение I и като значими в приложение II;

в) се установяват задължения относно обмена на информация за киберсигурността.

Член 2

Обхват

1. Настоящата директива се прилага за публичноправните и частноправните субекти от видове, определени като съществени в приложение I и като значими в приложение II. Настоящата директива не се прилага за субектите, квалифицирани като микропредприятия и малки предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията[28].

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

2. Настоящата директива обаче се прилага за субекти, посочени в приложения I и II, също и независимо от техния размер, когато:

а) услугите са предоставяни от някой от следните субекти:

i) обществени електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги, посочени в точка 8 от приложение I;

ii) доставчици на удостоверителни услуги, посочени в точка 8 от приложение I;

iii) регистри на имена на домейни от първо ниво и доставчици на DNS услуги, посочени в точка 8 от приложение I.

б) субектът е орган на публичната администрация съгласно определението в член 4, точка 23;

в) субектът е единствен доставчик на дадена услуга в държава членка;

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

д) потенциално смущение на предоставяната от субекта услуга би могло да предизвика системни рискове, по-специално за секторите, в които такова нарушаване би могло да има трансгранично въздействие;

е) субектът е с критичен характер поради своята специфична значимост на регионално или национално равнище за конкретния сектор или вид услуга или за други взаимозависими сектори в държавата членка;

ж) субектът е определен като критичен съгласно Директива (ЕС) XXXX/XXXX на Европейския парламент и на Съвета[29] [Директива относно устойчивостта на критичните субекти] или като равностоен на критичен съгласно член 7 от същата директива.

Държавите членки съставят списък със субектите, определени съгласно букви б)—е), и го представят на Комисията до [6 месеца след срока за транспониране]. Държавите членки извършват редовен преглед на списъка и поне на всеки две години след това и го актуализират, когато е подходящо.

3. Настоящата директива не засяга правомощията на държавите членки по отношение на поддържането на обществената сигурност, отбраната и националната сигурност в изпълнение на правото на Съюза.

4. Настоящата директива се прилага, без да се засягат Директива 2008/114/ЕО на Съвета[30] и Директиви 2011/93/ЕС[31] и 2013/40/ЕС[32] на Европейския парламент и на Съвета.

---

29 *[да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

30 Директива 2008/114/ЕО на Съвета от 8 декември 2008 година относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (ОВ L 345, 23.12.2008 г., стр. 75).

31 Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 година относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с

5. Без да се засяга член 346 от ДФЕС, информация, която е поверителна съгласно правилата на Съюза и националните правила, например правилата за търговската тайна, се обменя с Комисията и други съответни органи 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. При обмена на информация се запазва поверителността на информацията, както и сигурността и търговските интереси на съществените и значимите субекти.

6. Когато разпоредбите на специфичните за сектора актове на правото на Съюза изискват съществените или значимите субекти да приемат мерки за управление на риска, свързан с киберсигурността, или да уведомяват за инциденти или значителни киберзаплахи и тези изисквания имат поне равностоен ефект на предвидените в настоящата директива задължения, съответните разпоредби на настоящата директива, включително разпоредбата относно надзора и правоприлагането, предвидени в глава VI, не се прилагат.

Член 3

Минимална хармонизация

Без да се засягат техните други задължения съгласно правото на Съюза, държавите членки могат, в съответствие с настоящата директива, да приемат или поддържат разпоредби, осигуряващи по-високо ниво на киберсигурност.

Член 4

Определения

За целите на настоящата директива се прилагат следните определения:

1) „мрежа и информационна система“ означава:

   а) електронна съобщителна мрежа по смисъла на член 2, параграф 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 обработват автоматично цифрови данни;

   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 мрежите и информационните системи“ означава способността на мрежите и информационните системи да издържат — при дадено равнище на увереност — на действия, засягащи отрицателно наличието, истинността,

---

детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 17.12.2011 г., стр. 1).

[32] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година 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).

целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях;

3) „киберсигурност“ означава киберсигурност по смисъла на член 2, параграф 1 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[33]

4) „национална стратегия относно киберсигурността“ означава съгласувана рамка на държава членка, съдържаща стратегически цели и приоритети относно сигурността на мрежите и информационните системи в тази държава членка;

5) „инцидент“ означава всяко събитие, компрометиращо наличието, автентичността, целостта или поверителността на съхранявани, предавани или обработвани данни или на свързаните с тях услуги, предлагани или направени достъпни чрез мрежи и информационни системи;

6) „действия при инцидент“ означава всички действия и процедури, имащи за цел установяването, анализа, ограничаването и реагирането на инцидент;

7) „киберзаплаха“ означава киберзаплаха по смисъла на член 2, параграф 8 от Регламент (ЕС) 2019/881;

8) „уязвимост“ означава слабост, предразположеност или недостатък на актив, система, процес или контролен механизъм, които могат да бъдат използвани при киберзаплаха;

9) „представител“ означава всяко установено в Съюза физическо или юридическо лице, изрично определено да действа от името на i) доставчик на система за имена на домейни (DNS), регистър на имената на домейни от първо ниво (TLD), доставчик на компютърни услуги „в облак“, доставчик на услуги на център за данни, доставчик на мрежи за предоставяне на съдържание съгласно посоченото в точка 8 от приложение I или ii) субекти, неустановени в Съюза, които са посочени в точка 6 от приложение II и към които, по отношение на задълженията на даден субект съгласно настоящата директива, национален компетентен орган или ЕРИКС може да се обръща вместо към самия субект;

10) „стандарт“ означава стандарт по смисъла на член 2, параграф 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета[34];

11) „техническа спецификация“ означава техническа спецификация по смисъла на член 2, параграф 4 от Регламент (ЕС) № 1025/2012;

12) „точка за обмен в интернет (ТОИ)“ означава мрежово съоръжение, което дава възможност за свързване на повече от две независими мрежи (автономни системи), преди всичко с цел улесняване на обмена на интернет трафик; чрез ТОИ се осъществява свързване само на автономни системи; свързването чрез

---

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

[34] Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 година 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).

ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин;

13) „система за имена на домейни (DNS)“ означава йерархична разпределена система за именуване на домейни, позволяваща на крайните потребители да достигат до услугите и ресурсите в интернет;

14) „доставчик на DNS услуги“ означава субект, предоставящ рекурсивни или окончателни услуги по преобразуване на имена на домейни на крайни потребители в интернет и други доставчици на DNS услуги;

15) „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;

16) „цифрова услуга“ означава услуга по смисъла на член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета[35];

17) „онлайн място за търговия“ означава цифрова услуга по смисъла на член 2 буква н) от Директива 2005/29/ЕО на Европейския парламент и на Съвета[36];

18) „онлайн търсачка“ означава цифрова услуга по смисъла на член 2, параграф 5 от Регламент (ЕС) 2019/1150 на Европейския парламент и на Съвета[37]

19) „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 разпределени компютърни ресурси, които могат да бъдат ползвани съвместно;

20) „услуга на център за данни“ означава услуга, включваща 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 инфраструктури за електроразпределение и контрол на околната среда;

21) „мрежа за доставяне на съдържание“ означава мрежа от географски разпределени сървъри, с цел да се осигури висока степен на наличност,

---

35 Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 година, 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).

36 Директива 2005/29/ЕО на Европейския парламент и на Съвета от 11 май 2005 година 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).

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

достъпност или бързо доставяне на цифрово съдържание и услуги на интернет потребителите от страна на доставчиците на съдържание и услуги;

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

23) „орган на публичната администрация“ означава орган в държава членка, 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;

в) финансира се основно от държавата, регионален орган или други публичноправни организации; или е обект на управленски надзор от страна на тези органи или организации; или има административен, управителен или надзорен съвет, повечето от половината от членовете на който са назначени от държавните, 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.

Изключват се органите на публичната администрация, извършващи дейности в областите на обществената сигурност, правоприлагането, отбраната или националната сигурност.

24) „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;

25) „съществен субект“ означава всеки субект от вид, посочен като съществен в приложение I;

26) „значим субект“ означава всеки субект от вид, посочен като значим в приложение II.

ГЛАВА II

Координирани регулаторни рамки в областта на киберсигурността

Член 5

Национална стратегия за киберсигурност

1. Всяка държава членка приема национална стратегия за киберсигурност, в която са определени стратегическите 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 по-специално следното:

а) определяне на целите и приоритетите на стратегията на държавата членка относно киберсигурността;

б) управленска рамка за постигане на тези цели и приоритети, включително посочените в параграф 2 политики и ролите и отговорностите на публичните служби и органи, както и на останалите относими действащи лица;

в) оценка за установяване на относимите активи и рискове за киберсигурността в съответната държава членка;

г) набелязване на мерките, гарантиращи подготвеността, реагирането и възстановяването при инциденти, включително сътрудничеството между публичния и частния сектор;

д) списък с различните органи и действащи лица, които участват в прилагането на националната стратегия за киберсигурност;

е) рамка на политиките за подобрена координация между компетентните органи съгласно настоящата директива и Директива (ЕС) XXXX/XXXX на Европейския парламент и на Съвета[38] [Директива относно устойчивостта на критичните субекти] с цел обмен на информация относно инциденти и киберзаплахи и упражняването на задачи по надзор.

2. Като част от националната стратегия за киберсигурност държавите членки по-специално приемат следните политики:

а) политика за разрешаване на въпросите с киберсигурността по веригата за доставки на ИКТ продукти и услуги, използвана от съществените и значимите субекти за предоставянето на техните услуги;

б) насоки относно включването и посочването на свързани с киберсигурността изисквания за ИКТ продуктите и услугите при възлагането на обществени поръчки;

в) политика за насърчаване и улесняване на координираното оповестяване на уязвимости по смисъла на член 6;

г) политика, свързана с поддържането на общата наличност и цялост на обществото ядро на отворения интернет;

д) политика за насърчаване и развитие на умения в областта на киберсигурността, повишаване на осведомеността и инициативи за научноизследователска и развойна дейност;

е) политика за подпомагане на академичните и научноизследователските институции за разработване на инструменти за киберсигурност и сигурна мрежова инфраструктура;

ж) политика, съответни процедури и подходящи инструменти за обмен на информация, подпомагащи доброволния обмен на информация за киберсигурността между дружествата в изпълнение на правото на Съюза;

з) политика, намираща решения за специфичните нужди на малките и средните предприятия, по-специално на изключените от обхвата на

[38] *[да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

настоящата директива, във връзка с насоки и подкрепа за подобряване на тяхната устойчивост на заплахи за киберсигурността.

3. Държавите членки уведомяват Комисията за своите национални стратегии за киберсигурност в рамките на три месеца от приемането им. Държавите членки могат да изключват конкретна информация от уведомлението, когато и доколкото е строго необходимо да се запази националната сигурност.

4. Държавите членки извършват оценка на своите национални стратегии за киберсигурност поне на всеки четири години въз основа на ключови показатели за ефективност и, при необходимост, внасят изменения в тях. По искане на държавите членки Агенцията на Европейския съюз за киберсигурност (ENISA) ги подпомага при разработването на национална стратегия и на ключови показатели за ефективност за оценката на стратегията.

Член 6

Координирано оповестяване на уязвимости и а Европейски регистър на уязвимостите

1. Всяка държава членка определя един от своите екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) съгласно посоченото в член 9 като координатор за целите на координираното оповестяване на уязвимости. Определеният ЕРИКС действа като доверен посредник, улесняващ при необходимост взаимодействието между докладващия субект и производителя или доставчика на ИКТ продукти или услуги. Когато докладваната уязвимост засяга няколко производители или доставчици на ИКТ продукти или услуги в Съюза, определеният ЕРИКС на всяка засегната държава членка си сътрудничи с мрежата на ЕРИКС.

2. ENISA разработва и поддържа Европейски регистър на уязвимостите. За тази цел ENISA създава и поддържа подходящите информационни системи, политики и процедури, по-специално за да даде възможност на значимите и съществените субекти и техните доставчици на мрежи и информационни системи да оповестяват и регистрират уязвимостите, налични в ИКТ продукти или услуги, както и да предоставят достъп до съдържащата се в регистъра информация на всички заинтересовани страни. Регистърът по-специално включва описваща уязвимостта информация, засегнатите ИКТ продукти или услуги и тежестта на уязвимостта с оглед на обстоятелствата, при които тя може да бъде използвана злонамерено, наличието на съответни корекции и, ако такива липсват – насоки за потребителите на уязвимите продукти и услуги как да бъде ограничен рискът, произтичащ от оповестените уязвимости.

Член 7

Национални рамки за управление на кризи в областта на киберсигурността

1. Всяка държава членка определя един или повече компетентни органи, отговарящи за управлението на мащабните инциденти и кризи. Държавите членки гарантират, че компетентните органи разполагат с адекватни ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин.

2. Всяка държава членка набелязва способности, активи и процедури, които могат да бъдат разгърнати в случай на криза за целите на настоящата директива.

3. Всяка държава членка приема национален план за реакция при инциденти и кризи в областта на киберсигурността, в който се предвиждат целите и условията и редът за управлението на мащабни инциденти и кризи, свързани с киберсигурността. Планът обхваща по-специално следното:

   а) цели на националните мерки и дейности за подготвеност;

   б) задачи и отговорности на националните компетентни органи;

   в) процедури за управление на кризи и канали за обмен на информация;

   г) мерки за подготвеност, включително дейности по учения и обучения;

   д) съответните публичноправни и частноправни заинтересовани страни и засегнатата 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 инциденти и кризи, свързани с киберсигурността, на равнището на Съюза.

4. Държавите членки съобщават на Комисията определянето на своите компетентни органи, посочени в параграф 1, и представят своите национални планове за реакция при инциденти и кризи в областта на киберсигурността съгласно посоченото в параграф 3 в рамките на три месеца от определянето и приемането на тези планове. Държавите членки може да изключат конкретна информация от плана, когато и доколкото това е строго необходимо за тяхната национална сигурност.

Член 8

Национални компетентни органи и единни звена за контакт

1. Всяка държава членка определя един или повече компетентни органи, отговарящи за киберсигурността и за задачите по надзор, посочени в глава VI от настоящата директива. Държавите членки могат да определят за тази цел вече съществуващ орган или органи.

2. Компетентните органи, посочени в параграф 1, наблюдават прилагането на настоящата директива на национално равнище.

3. Всяка държава членка определя едно национално единно звено за контакт в областта на киберсигурността („единно звено за контакт“). Когато държава членка определи само един компетентен орган, 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 в други държави членки, както и за да осигури междусекторно сътрудничество с други национални компетентни органи в рамките на своята държава членка.

5. Държавите членки гарантират, че компетентните органи, посочени в параграф 1, и единните 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. Държавите членки осигуряват ефективно, ефикасно и сигурно сътрудничество на определените представители в групата за сътрудничество, посочена в член 12.

6. Всяка държава членка уведомява Комисията без излишно забавяне за определянето на компетентния орган по параграф 1 и на единното звено за контакт по параграф 3, за техните задачи и за евентуални последващи промени в тях. Всяка държава членка оповестява публично своето определяне. Комисията публикува списъка на определените единни звена за контакт.

Член 9

Екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС)

1. Всяка държава членка определя един или повече ЕРИКС, отговарящи на изискванията, посочени в член 10, параграф 1, които обхващат най-малко секторите, подсекторите или субектите, посочени в приложения I и II, които отговарят за предприемането на действия при инциденти в съответствие с подробно определена процедура. ЕРИКС може да бъде създаден в рамките на компетентен орган, посочен в член 8.

2. Държавите членки гарантират, че всеки ЕРИКС разполага с достатъчни ресурси, за да изпълнява ефективно задачите си, установени в член 10, параграф 2.

3. Държавите членки гарантират, че всеки ЕРИКС разполага с подходяща, сигурна и устойчива комуникационна и информационна инфраструктура за обмен на информация със съществените и значимите субекти, както и с други относими заинтересовани страни. За тази цел държавите членки гарантират, че ЕРИКС допринасят за внедряването на сигурни инструменти за обмен на информация.

4. ЕРИКС си сътрудничат и, когато е подходящо, обменят относима информация в съответствие с член 26 с доверени секторни и междусекторни общности на съществените и значимите субекти.

5. ЕРИКС участват в партньорски проверки, организирани в съответствие с член 16.

6. Държавите членки гарантират, че чрез мрежата на ЕРИКС, посочена в член 13, техните ЕРИКС си сътрудничат ефективно, ефикасно и сигурно.

7. Държавите членки съобщават на Комисията без излишно забавяне определените съгласно параграф 1 ЕРИКС, координатора на ЕРИКС, определен съгласно член 6, параграф 1, и техните съответни задачи, предвидени във връзка със субектите, посочени в приложения I и II.

8. Държавите членки може да поискат помощ от Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) при създаването на националните ЕРИКС.

Член 10

Изисквания към ЕРИКС и задачи на ЕРИКС

1. ЕРИКС отговарят на следните изисквания:

   а) ЕРИКС гарантират високо ниво на достъпност на своите комуникационни услуги, 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. ЕРИКС 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 разполагат с достатъчно персонал, за да гарантират разполагаемост по всяко време;

   д) ЕРИКС разполагат с резервни системи и резервно работно пространство, за да гарантират непрекъснатост своите услуги;

   е) ЕРИКС имат възможността да участват в мрежи за международно сътрудничество.

2. ЕРИКС имат следните задачи:

   а) наблюдение на киберзаплахи, уязвимости и инциденти на национално равнище;

   б) подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за киберзаплахи, уязвимости и инциденти до съществените и значимите субекти, както и до други относими заинтересовани страни;

   в) реагиране на инциденти;

   г) осигуряване на динамичен анализ на рисковете и инцидентите и ситуационна осведоменост за киберсигурността;

   д) осигуряване, при заявка от субект, на активно сканиране на мрежите и информационните системи, използвани за предоставянето на неговите услуги;

   е) участие в мрежата на ЕРИКС и предоставяне на взаимопомощ на останалите членове на мрежата при заявка от тяхна страна.

3. ЕРИКС изграждат отношения на сътрудничество с относими действащи лица в частния сектор, с цел по-добро постигане на целите на директивата.

4. За да улеснят сътрудничеството, ЕРИКС насърчават приемането и използването на общи или стандартизирани практики, схеми за класификация и таксономии във връзка със следното:

   а) процедури за предприемане на действия при инциденти;

   б) управление на кризи в областта на киберсигурността;

в) координирано оповестяване на уязвимости.

Член 11

Сътрудничество на национално равнище

1. Ако са отделени, компетентните органи по член 8, 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 компетентни органи или ЕРИКС получават уведомления за инциденти, и съществени киберзаплахи и ситуации, близки до инциденти, подадени съгласно настоящата директива. Когато държава членка реши, че нейните ЕРИКС няма да получават тези уведомления, на ЕРИКС — до степента, необходима за изпълнението на техните задачи, се предоставя достъп до данните за инциденти, за които са постъпили уведомления от съществените или значимите субекти съгласно член 20.

3. Всяка държава членка гарантира, че нейните компетентни органи или ЕРИКС информират нейното единно звено за контакт за уведомления за инциденти, съществени киберзаплахи и ситуации, близки до инциденти, подадени съгласно настоящата директива.

4. В степента, необходима за ефективното изпълнение на задачите и задълженията, предвидени в настоящата директива, държавите членки гарантират подходящо сътрудничество между компетентните органи и единни звена за контакт и правоприлагащите органи, органите за защита на личните данни и органите, отговарящи за критичната инфраструктура съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти] и националните финансови органи, определени в съответствие с Регламент (ЕС) XXXX/XXXX на Европейския парламент и на Съвета[39] [Регламент за ОУЦТ] в рамките на тази държава членка.

5. Държавите членки гарантират, че техните компетентни органи редовно предоставят информация на компетентните органи, определени съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], за рискове за киберсигурността, киберзаплахи и инциденти, засягащи съществените субекти, определени като критични или като субекти, равностойни на критични субекти, съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], както и за мерките, предприети от компетентните органи в отговор на тези рискове и инциденти.

ГЛАВА III

[39] *[да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

Сътрудничество

Член 12
Група за сътрудничество

1. С цел подкрепа и улесняване на стратегическото сътрудничество и обмен на информация между държавите членки в областта на прилагане на директивата се създава група за сътрудничество.

2. Групата за сътрудничество изпълнява задачите си въз основа на двугодишните работни програми, посочени в параграф 6.

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) в съответствие с член 17, параграф 5, буква в) от Регламент (ЕС) XXXX/XXXX [Регламент за ОУЦТ] могат да участват в дейностите на групата за сътрудничество.

   Групата за сътрудничество може да кани 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) 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, обучения, учения и умения, изграждане на капацитет, както и стандарти и технически спецификации;

   в) взаимни консултации и сътрудничество с Комисията по възникващи инициативи за политики в областта на киберсигурността;

   г) взаимни консултации и сътрудничество с Комисията по нейни проекти за актове за изпълнение или делегирани актове, приети съгласно настоящата директива;

   д) обмен на най-добри практики и информация с относимите институции, органи, служби и агенции на Съюза;

   е) обсъждане на доклади от партньорски проверки съгласно посоченото в член 16, параграф 7;

   ж) обсъждане на резултатите от съвместни дейности по надзор при трансгранични случаи съгласно посоченото в член 34;

   з) предоставяне на стратегически насоки на мрежата на ЕРИКС по конкретни възникващи въпроси;

   и) 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 на държавите членки;

й) организиране на редовни съвместни заседания с относими частни заинтересовани страни от Съюза за обсъждане на дейностите, извършвани от групата, и събиране на приноса във връзка с възникващите предизвикателства пред политиките;

к) обсъждане на работата, предприета във връзка с ученията в областта на киберсигурността, включително извършената от ENISA работа.

5. Групата за сътрудничество може да изисква от мрежата на ЕРИКС технически доклади по избрани теми.

6. До … [24 месеца след датата на влизане в сила на настоящата директива] 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. Времевата рамка на първата програма, приета съгласно настоящата директива, се синхронизира с времевата рамка на последната програма, приета съгласно Директива (ЕС) 2016/1148.

7. 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 37, параграф 2.

8. Групата за сътрудничество провежда заседания редовно и поне веднъж годишно с групата за устойчивост на критичните субекти, създадена съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], за да се насърчават стратегическото сътрудничество и обменът на информация.

Член 13
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 на държавите членки и екипите за незабавно реагиране при компютърни инциденти (CERT) на ЕС. Комисията участва в мрежата на ЕРИКС като наблюдател. ENISA осигурява административното обслужване и активно подкрепя сътрудничеството между ЕРИКС.

3. Мрежата на ЕРИКС изпълнява следните задачи:

а) обмен на информация относно способностите на ЕРИКС;

б) обмен на относима информация за инциденти, ситуации, близки до инциденти, киберзаплахи, рискове и уязвимости;

в) по искане на потенциално засегнат от инцидент представител на мрежата на ЕРИКС — обмен и обсъждане на информация във връзка с този инцидент и свързаните киберзаплахи, рискове и уязвимости;

г) по искане на представител на мрежата на ЕРИКС — обсъждане и, при възможност, осъществяване на координирана реакция на инцидент, констатиран в рамките на юрисдикцията на тази държава членка;

д) предоставяне на държавите членки на подкрепа за справянето с трансгранични инциденти съгласно настоящата директива;

е) сътрудничество или предоставяне на помощ на определените ЕРИКС по член 6 с оглед на управлението на многостранно координирано оповестяване на уязвимости, засягащи няколко производители или доставчици на ИКТ продукти, услуги и процедури, установени в различни държави членки;

ж) 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, условия и ред за координация при реакция на трансгранични рискове и инциденти;

v) допринасяне за националния план за реакция при инциденти и кризи в областта на киберсигурността, посочен в член 7, параграф 3;

з) информиране на групата за сътрудничество относно дейностите на мрежата на ЕРИКС и допълнителните форми на оперативно сътрудничество, обсъдени в съответствие с буква ж), и при необходимост искане на насоки във връзка с това;

и) извършване на равносметка от ученията в областта на киберсигурността, включително от организираните от ENISA;

й) по искане на отделен ЕРИКС — обсъждане на способностите и подготвеността на същия този ЕРИКС;

к) 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 заплахи в ЕС;

л) обсъждане на доклади от партньорски проверки съгласно посоченото в член 16, параграф 7;

м) издаване 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. За целите на посочения в член 35 преглед и до [24 месеца след датата на влизане в сила на настоящата директива], както и на всеки две години след това, мрежата на ЕРИКС извършва оценка на напредъка, постигнат при оперативното сътрудничество, и представя доклад. В доклада по-специално се правят заключения за резултатите от партньорските проверки по член 16, извършени във връзка с националните ЕРИКС, в това число заключения и препоръки съгласно настоящия член. Този доклад се представя и на групата за сътрудничество.

5. Мрежата на ЕРИКС приема свой процедурен правилник.

Член 14

Европейска мрежа за връзка на организациите при кибернетични кризи (EU — CyCLONe)

1. С цел подпомагане на координираното управление на мащабни инциденти и кризи, свързани с киберсигурността, на оперативно равнище и осигуряване на редовния обмен на информация сред държавите членки и институциите, службите и агенциите на Съюза, се създава Европейската мрежа за връзка на организациите при кибернетични кризи (EU — CyCLONe).

2. EU-CyCLONe се състои от представителите на органите за управление на кризи на държавите членки, определени в съответствие с член 7, както и от Комисията и ENISA. ENISA осигурява административното обслужване на мрежата и оказва подкрепа за сигурния обмен на информация.

3. EU-CyCLONe има следните задачи:

   а) повишаване на степента на подготвеност при управлението на мащабни инциденти и кризи;

   б) развиване на споделена ситуационна осведоменост за относими събития в областта на киберсигурността;

   в) координиране на управлението на мащабни инциденти и кризи и подпомагане на процеса на вземане на решения на политическо равнище във връзка с такива инциденти и кризи;

   г) обсъждане на националните планове за реакция при инциденти в областта на киберсигурността, посочени в член 7, параграф 2.

4. EU-CyCLONe приема свой процедурен правилник.

5. EU-CyCLONe докладва редовно на групата за сътрудничество относно киберзаплахи, инциденти и тенденции, като се фокусира по-специално върху тяхното въздействие върху съществените и значимите субекти.

6. EU-CyCLONe си сътрудничи с мрежата на ЕРИКС въз основа на договорени процедурни правила.

Член 15

Доклад за състоянието на киберсигурността в Съюза

1. В сътрудничество с Комисията ENISA издава двугодишен доклад за състоянието на киберсигурността в Съюза. Докладът по-специално включва оценка на следното:

   а) развитието на способностите в областта на киберсигурността в Съюза;

   б) техническите, финансовите и човешките ресурси, налични за компетентните органи и политиките в областта на киберсигурността, както и прилагането на мерки за надзор и действия по правоприлагане с оглед на резултатите от партньорските проверки по член 16;

в) индекс за киберсигурност, предоставящ обобщена оценка на степента на зрялост на способностите в областта на киберсигурността.

2. В доклада се включват конкретни препоръки за политиките във връзка с повишаването на степента на киберсигурността в Съюза, както и резюме на констатациите за конкретния период от докладите на Агенцията за техническото състояние на киберсигурността на ЕС, издавани от ENISA в съответствие с член 7, параграф 6 от Регламент (ЕС) 2019/881.

Член 16

Партньорски проверки

1. След консултиране с групата за сътрудничество и ENISA и най-късно до 18 месеца след влизането в сила на настоящата директива Комисията съставя методологията и съдържанието на система за партньорска проверка за оценяване на ефективността на политиките на държавите членки в областта на киберсигурността. Проверките се провеждат от технически експерти по киберсигурност, подбрани от държави членки, различни от тази, която е обект на проверка, и обхващат най-малко следното:

   i) ефективността от прилагането на изискванията за управлението на риска, свързан с киберсигурността, и задълженията за докладване по членове 18 и 20;

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

   iii) оперативните способности и ефективност на ЕРИКС;

   iv) ефективността от взаимопомощта по член 34;

   v) ефективността на рамката за обмен на информация по член 26 от настоящата директива.

2. Методологията включва обективни, недискриминационни, справедливи и прозрачни критерии, въз основа на които държавите членки определят експерти, отговарящи на условията за провеждане на партньорските проверки. ENISA и Комисията определят експерти, които да участват като наблюдатели в партньорските проверки. Комисията, подпомагана от ENISA, установява в методологията по параграф 1 обективна, недискриминационна, справедлива и прозрачна система за подбора и разпределението на случаен принцип на експерти за всяка партньорска проверка.

3. Организационните аспекти на партньорските проверки се решават от Комисията, подпомагана от ENISA, и след консултация с групата за сътрудничество се основават на критерии, определени в методологията по параграф 1. В партньорските проверки се прави оценка на аспектите по параграф 1 за всички държави членки и сектори, включително за целеви въпроси, специфични за една или няколко държави членки или един или няколко сектора.

4. Партньорските проверки включват действителни или виртуални посещения на място, както и дистанционен обмен. С оглед на принципа на доброто

сътрудничество държавите членки, които са обект на проверка, предоставят на определените експерти поисканата информация, необходима за оценката на проверяваните аспекти. Всяка информация, получена в процеса на партньорска проверка, се използва единствено за тази цел. Участващите в партньорската проверка експерти не оповестяват никаква чувствителна или поверителна информация, получена в хода на тази проверка, на които и да е трети страни.

5. Веднъж проверени в държава членка, същите аспекти не подлежат на последваща партньорска проверка в тази държава членка в рамките на две години след приключването на партньорска проверка, освен ако Комисията не реши друго след консултация с ENISA и групата за сътрудничество.

6. Държавата членка гарантира, че всеки риск от конфликт на интереси, засягащ определените експерти, се разкрива на останалите държави членки, Комисията и ENISA без излишно забавяне.

7. Участващите в партньорските проверки експерти изготвят доклади за констатациите и заключения от проверката. Докладите се представят на Комисията, групата за сътрудничество, мрежата на ЕРИКС и ENISA. Докладите се обсъждат в групата за сътрудничество и мрежата на ЕРИКС. Докладите може да бъдат публикувани на специално предназначения уебсайт на групата за сътрудничество.

ГЛАВА IV

Управление на риска, свързан с киберсигурността, и задължения за докладване

РАЗДЕЛ I

Управление на риска, свързан с киберсигурността, и докладване

Член 17

Управление

1. Държавите членки гарантират, че управителните органи на съществените и значимите субекти одобряват мерките за управление на риска, свързан с киберсигурността, предприети от тези субекти с цел спазване на член 18, осъществяват надзор върху прилагането му и отговарят за неизпълнението от субектите на задълженията съгласно този член.

2. Държавите членки гарантират, че членовете на управителния орган редовно преминават през конкретни обучения за придобиване на достатъчно познания и умения, с цел да могат да разбират и оценяват рисковете за киберсигурността и управленските практики и тяхното въздействие върху операциите на субекта.

Член 18

Мерки за управление на риска, свързан киберсигурността

1. Държавите членки гарантират, че съществените и значимите субекти предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, които тези субекти използват при предоставяне на своите услуги. Тези мерки осигуряват ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск, съобразно последните постижения в тази област.

2. Мерките, посочени в параграф 1, включват най-малко следното:

   а) анализ на риска и политики на сигурност в областта на информационните системи;

   б) действия при инциденти (предотвратяване, установяване и реакция на инциденти);

   в) непрекъснатост на стопанската дейност и управление на кризи;

   г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите снабдители или доставчици на услуги, като например доставчиците на услуги за съхранение и обработване на данни или услуги за управление на сигурността;

   д) сигурност при придобиването на мрежи и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им;

   е) политики и процедури (проверки и одити) за оценяване на ефективността на мерките за управление на риска, свързан с киберсигурността;

   ж) използването на криптография и криптиране.

3. Държавите членки гарантират, че когато разглеждат подходящи мерки по параграф 2, буква г), субектите вземат предвид уязвимостите, специфични за всеки снабдител или доставчик на услуги, както и цялостното качество на продуктите и практиките в областта на киберсигурността на своите снабдители или доставчици на услуги, включително техните процедури за сигурно разработване.

4. Държавите членки гарантират, че когато един субект установи, че неговите услуги или задачи не са в съответствие с изискванията по параграф 2, той без излишно забавяне предприема всички необходими коригиращи мерки за привеждането на въпросната услуга в съответствие.

5. Комисията може да приема актове за изпълнение, с цел да определи техническите и методологическите спецификации на елементите по параграф 2. При изготвянето на тези актове Комисията действа в съответствие с процедурата за разглеждане по член 37, параграф 2 и във възможно най-голяма степен следва международните и европейските стандарти, както и съответните технически спецификации.

6. Комисията е оправомощена да приема делегирани актове в съответствие с член 36 за допълване на елементите по параграф 2 с цел отчитане на нови киберзаплахи, технологично развитие или секторни специфики.

Член 19

Координирана на равнището на ЕС оценка на критични вериги за доставка

1. Групата за сътрудничество, в сътрудничество с Комисията и ENISA, може да извършва координирани оценки на риска на конкретни критични вериги за доставка на ИКТ услуги, системи или продукти, при които се вземат предвид техническите и, когато е уместно, нетехническите рискови фактори.

2. След консултиране с групата за сътрудничество и ENISA Комисията установява конкретните критични ИКТ услуги, системи или продукти, които може да бъдат предмет на координирана оценка на риска по параграф 1.

Член 20

Задължения за докладване

1. Държавите членки гарантират, че съществените и значимите субекти уведомяват без излишно забавяне компетентните органи или ЕРИКС в съответствие с параграфи 3 и 4 за всякакви инциденти, имащи значително въздействие върху предоставянето на техните услуги. Когато е подходящо, тези субекти уведомяват без излишно забавяне получателите на техните услуги за инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги. Държавите членки гарантират, че тези субекти докладват, наред с друго, всяка информация, позволяваща на компетентните органи или на ЕРИКС да определи всякакво трансгранично въздействие на инцидентите.

2. Държавите членки гарантират, че съществените и значимите субекти уведомяват без излишно забавяне компетентните органи или ЕРИКС за всяка значима киберзаплаха, която тези субекти установят, че може потенциално да доведе до значим инцидент.

   Когато е приложимо, тези субекти уведомяват без излишно забавяне получателите на своите услуги, които са потенциално засегнати от значителна киберзаплаха, за всички мерки или средства за защита, които тези получатели могат да предприемат като реакция на тази заплаха. Когато е подходящо, субектите следва да уведомят тези получатели за самата заплаха. Уведомлението не води до повишена отговорност за уведомяващия субект.

3. Даден инцидент се счита за значителен, ако:

   а) е причинил или има потенциала да причини съществено оперативно смущение или финансови загуби за съответния субект;

   б) е засегнал или има потенциала да засегне други физически или юридически лица, причинявайки значителни материални или нематериални загуби.

4. Държавите членки гарантират, че за целите на уведомяването по параграф 1 съответните субекти представят на компетентните органи или ЕРИКС:

   а) без излишно забавяне и при всички случаи в рамките на 24 часа след узнаването за даден инцидент — първоначално уведомление, в което, когато е приложимо, се посочва дали се предполага, че

инцидентът се дължи на незаконосъобразно или злонамерено действие;

б) по искане на компетентен орган или на ЕРИКС — междинен доклад за съответните новости на състоянието;

в) окончателен доклад, не по-късно от един месец след представянето на доклада по буква а), включващ най-малко следното:

i) подробно описание на инцидента, неговата тежест и въздействие;

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

iii) приложените и текущите мерки за ограничаване.

Държавите членки гарантират, че в надлежно обосновани случаи и при споразумение с компетентните органи или ЕРИКС съответният субект може да се отклони от сроковете по букви а) и в).

5. Компетентните национални органи или ЕРИКС предоставят, в рамките на 24 часа след получаването на първоначалното уведомление по параграф 4, буква а), отговор на уведомяващия субект, включително първоначална обратна информация за инцидента и, при искане от субекта, насоки за прилагането на възможни мерки за ограничение. Когато ЕРИКС не е получил уведомлението, посочено в параграф 1, насоките се предоставят от компетентния орган в сътрудничество с ЕРИКС. ЕРИКС предоставя допълнителна техническа подкрепа, ако съответният субект изиска това. Когато има подозрения, че инцидентът е с престъпно естество, компетентните национални органи или ЕРИКС предоставят насоки относно докладването на инцидента на правоприлагащите органи.

6. Когато е целесъобразно и особено когато инцидентът по параграф 1 засяга две или повече държави членки, компетентният орган или ЕРИКС информира другите засегнати държави членки и ENISA за инцидента. При това компетентните органи, ЕРИКС и единните звена 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, което е в съответствие с правото на Съюза.

7. При необходимост от обществено уведомяване с цел предотвратяване на инцидент или справяне с текущ инцидент или когато оповестяването на инцидента е в обществен интерес по друга причина, компетентният орган или ЕРИКС, и когато е уместно, органите или ЕРИКС на други засегнати държави членки могат, след като се консултират със засегнатия субект, да уведомят обществеността за инцидента или да изискат от него на направи това.

8. По искане на компетентния орган или ЕРИКС единното звено за контакт предава уведомленията, получени съгласно параграфи 1 и 2, на единните звена за контакт на други засегнати държави членки.

9. Единното звено за контакт представя месечно на ENISA обобщителен доклад, включващ анонимизирани и обобщени данни за инцидентите, значителните киберзаплахи и ситуации, близки до инциденти, за които е изпратено уведомление в съответствие с параграфи 1 и 2 и с член 27. За да допринесе за

предоставянето на сравнима информация, ENISA може да издава технически насоки за параметрите на включената в обобщителния доклад информация.

10. Компетентните органи предоставят на компетентните органи, определени съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти], информация относно инцидентите и киберзаплахите, за които е изпратено уведомление в съответствие с параграфи 1 и 2 от съществените субекти, определени като критични или като субекти, равностойни на критични субекти, съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти].

11. Комисията може да приема актове за изпълнение, в които допълнително се уточняват видът на информацията, форматът и процедурата на изпратено по параграфи 1 и 2 уведомление. Комисията може да приема актове за изпълнение, в които допълнително се уточняват случаите, при които даден инцидент се счита за значителен съгласно посоченото в параграф 3. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 37, параграф 2.

Член 21

Използване на европейски схеми за сертифициране на киберсигурността

1. За да се докаже съответствие с някои изисквания по член 18, държавите членки могат да изискат от съществените и значимите субекти да сертифицират някои ИКТ продукти, услуги и процедури съгласно конкретни европейски схеми за сертифициране на киберсигурността, приети съгласно член 49 от Регламент (ЕС) 2019/881. Подлежащите на сертифициране продукти, услуги и процедури може да бъдат разработени от съществен или значим субект или да бъдат предоставени от трети страни.

2. Комисията е оправомощена да приема делегирани актове, определящи за кои категории съществени субекти се изисква да получат сертификат и съгласно кои конкретни европейски схеми за сертифициране на киберсигурността в съответствие с параграф 1. Делегираните актове се приемат в съответствие с член 36.

3. Комисията може да изиска от ENISA да изготви схема за сертифициране съгласно член 48, параграф 2 от Регламент (ЕС) 2019/881 в случаите, при които не е налична подходяща европейска схема за сертифициране на киберсигурността за целите на параграф 2.

Член 22

Стандартизация

1. С цел насърчаване на еднообразното прилагане на член 18, параграфи 1 и 2 държавите членки, без да налагат употребата на определен тип технология или да упражняват дискриминация в нейна полза, насърчават използването на европейско или международно приетите стандарти и спецификации от значение за сигурността на мрежите и информационните системи.

2. В сътрудничество с държавите членки 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 на държавите членки, което да позволи обхващането на тези области.

Член 23

Бази данни с имена на домейни и регистрационни данни

1. С цел допринасяне за сигурността, стабилността и устойчивостта на системата за имена на домейни държавите членки гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на такива имена на домейни, надлежно събират и поддържат точни и пълни данни за регистрация на имената на домейни в специално предназначено съоръжение за база данни съгласно правото на Съюза за защита на данните по отношение на личните данни.

2. Държавите членки гарантират, че базите данни за съхранение на данните за регистрация на имена на домейни по параграф 1, съдържат относима 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.

3. Държавите членки гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, имат установени политики и процедури, за да осигурят, че базите данни включват точна и пълна информация. Държавите членки гарантират, че тези политики и процедури са направени публично достъпни.

4. Държавите членки гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, публикуват, без излишно забавяне след регистрацията на име на домейн, данните за нея, които не са лични.

5. Държавите членки гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, предоставят достъп до конкретни данни за регистрация на имена на домейни при законосъобразни и надлежни искания от законно търсещите достъп, в изпълнение на правото на Съюза за защита на данните. Държавите членки гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, отговарят без излишно забавяне на всички искания за достъп. Държавите членки гарантират, че политиките и процедурите за оповестяване на такива данни са направени публично достъпни.

Раздел II

Юрисдикция и регистрация

Член 24

Юрисдикция и териториалност

1. 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 и доставчиците на мрежи за предоставяне на съдържание, посочени в точка 8 от приложение I, както и доставчиците на цифрово съдържание, посочени в точка 6 от приложение II, се считат за попадащи под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Съюза.

2. За целите на настоящата директива се счита, че основното място на установяване в Съюза на субектите, посочени в параграф 1, е в държавата членка, в която се вземат решенията относно мерките за управление на риска, свързан с киберсигурността. Ако такива решения не се вземат в никое от местата на установяване в Съюза, за основното място на установяване се счита държавата членка, в която е мястото на установяване на субектите с най-големия брой служители в Съюза.

3. Ако субект по параграф 1 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. Приема се, че този субект е под юрисдикцията на държавата членка, в която е установен представителят. При липсата на определен представител в Съюза съгласно настоящия член всяка държава членка, в която субектът предоставя услуги, може да предприеме правни действия срещу него за неизпълнение на задълженията съгласно настоящата директива.

4. Определянето на представител от страна на субект по параграф 1 не засяга правните действия, които биха могли да се предприемат срещу самия субект.

Член 25

Регистър за съществените и значимите субекти

1. ENISA създава и поддържа регистър за съществените и значимите субекти по член 24, параграф 1. Субектите изпращат на ENISA следната информация [най-късно 12 месеца след влизането в сила на директивата]:

   а) наименованието на субекта;

   б) адреса на основното място на установяване и на останалите законови места на установяване в Съюза или, при липсата на място на установяване в Съюза, на неговия представител, определен съгласно параграф 3 от член 24;

   в) актуални данни за контакт, включително адрес на електронна поща и телефонни номера на субектите.

2. Субектите по параграф 1 уведомяват ENISA без забавяне за всякакви промени в изпратените от тях данни съгласно параграф 1, и при всички положения, в рамките на три месеца от датата, на която е влязла в сила промяната.

3. При получаване на информацията по параграф 1 ENISA я препраща на единните звена за контакт в зависимост от указаното местоположение на

основното място на установяване на всеки субект или, ако не е установен в Съюза, на неговия определен представител. Когато субект по параграф 1 има освен своето основно място на установяване в Съюза и допълнителни места на установяване в други държави членки, ENISA уведомява и единните звена за контакт на тези държави членки.

4. Когато субект не успее да регистрира своята дейност или да предостави относимата информация в срока, определен по параграф 1, всяка държава членка, в която субектът предоставя услуги, е компетентна да гарантира, че този субект изпълнява задълженията, определени в настоящата директива.

ГЛАВА V

Обмен на информация

Член 26

Споразумения за обмен на информация в областта на киберсигурността

1. Без да се засягат разпоредбите на Регламент (ЕС) 2016/679, държавите членки гарантират, че съществените и значимите субекти могат да обменят помежду си информация за киберсигурността, включително такава относно киберзаплахи, уязвимости, признаци за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността, както и инструменти за конфигуриране, когато този обмен на информация:

   а) има за цел предотвратяване, откриване, реакция или ограничаване на инциденти с киберсигурността;

   б) подобрява нивото на киберсигурност, по-специално посредством повишаване на осведомеността във връзка с киберзаплахи, ограничаване или възпрепятстване на такива заплахи, способност за разпространение, поддържане на набор от отбранителни способности, отстраняване и оповестяване на уязвимости, техники за откриване на заплахи, стратегии за ограничаване или етапи за реакция или възстановяване.

2. Държавите членки гарантират, че обменът на информация се осъществява в рамките на доверени общности на съществените и значимите субекти. Този обмен се осъществява чрез споразумения за обмен на информация с оглед на потенциално чувствителния характер на споделяната информация и в изпълнение на правилата от правото на Съюза по параграф 1.

3. Държавите членки посочват правилата, определящи процедурата, оперативните елементи (включително използването на специално предназначени ИКТ платформи), съдържанието и условията по споразуменията за обмен на информация по параграф 2. В тези правила се определят и подробностите за участието на публичните органи в такива споразумения, както и оперативните елементи, включително използването на специално предназначени ИТ платформи. Държавите членки предлагат подкрепа за прилагането на такива споразумения в съответствие със своите политики, посочени в член 5, параграф 2, буква ж).

4. Съществените и значимите субекти уведомяват компетентните органи за своето участие в споразуменията за обмен на информация 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. В изпълнение на правото на Съюза ENISA осигурява подкрепа за установяването на споразуменията за обмен на информация в областта на киберсигурността по параграф 2, като предоставя най-добри практики и насоки.

Член 27

Доброволно уведомяване за относима информация

Държавите членки гарантират, че без да се засягат разпоредбите на член 3, субектите извън обхвата на настоящата директива могат доброволно да изпращат уведомления за значителни инциденти, киберзаплахи или ситуации, близки до инциденти. При обработването на уведомленията държавите членки действат в съответствие с процедурата по член 20. Държавите членки могат да обработват задължителните уведомления с предимство пред доброволните уведомления. Доброволното докладване не води до налагането на никакви допълнителни задължения за докладващия субект, на които той не би бил предмет, ако не подаде уведомлението.

ГЛАВА VI

Надзор и правоприлагане

Член 28

Основни аспекти относно надзора и правоприлагането

1. Държавите членки гарантират, че компетентните органи ефективно следят и предприемат мерки, необходими за осигуряване на съвместимостта с настоящата директива, по-специално задълженията по членове 18 и 20.

2. Компетентните органи работят в тясно сътрудничество с органите за защита на данните при работа по инцидентите, които водят до нарушаване на сигурността на лични данни.

Член 29

Надзор и правоприлагане за съществените субекти

1. Държавите членки гарантират, че мерките за надзор или правоприлагане, 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 когато изпълняват своите задачи по надзор във връзка със съществените субекти, компетентните органи са оправомощени да подлагат тези субекти на:

а) проверки на място или дистанционни проверки, включително случайни;

б) редовно одитиране;

в) целеви одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;

г) сканирания за сигурност въз основа на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска;

д) искания за информация, необходима за оценка на мерките за киберсигурност, приети от субекта, включително документирани политики за киберсигурност, както и съответствие със задълженията за уведомяване на ENISA съгласно член 25, параграфи 1 и 2;

е) искания за достъп до данни, документи или всякаква информация, необходими за изпълнението на техните задачи по надзор;

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.

3. При упражняване на своите правомощия по параграф 2, букви д)—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 компетентните органи са оправомощени:

а) да издават предупреждения при неизпълнение на задълженията по настоящата директива от субектите;

б) да изискват посредством обвързващи указания или разпореждане от тези субекти да поправят установените пропуски или нарушения на задълженията по настоящата директива;

в) да разпореждат на тези субекти да преустановяват поведение, което не е в съответствие със задълженията по настоящата директива и да се въздържат от повтарянето на такова поведение;

г) да разпореждат на тези субекти да привеждат своите мерки за управление на риска и/или задължения за докладване в съответствие със задълженията по членове 18 и 20 по конкретизиран начин и в рамките на посочен период;

д) да разпореждат на тези субекти да уведомяват физическото или юридическото лице или лица, на които предоставят услуги или дейности, потенциално засегнати от значителна киберзаплаха, за възможните защитни или коригиращи мерки, които могат да бъдат предприети от това физическо или юридическо лице или лица в отговор на тази заплаха;

е) да разпореждат на тези 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 изпълнението на задълженията им по членове 18 и 20;

з) да разпореждат на тези субекти да обявяват публично аспектите на неизпълнение на задълженията, предвидени в настоящата директива, по конкретен начин;

и) да правят публично изявление, в което се посочват юридическото или физическото лице или лица, отговорни за нарушението на задължение, предвидено в настоящата директива, както и характера на това нарушение;

й) да налагат или изискват налагането от съответните органи или съдилища съгласно националното право на административна глоба по член 31 в допълнение към или вместо мерките по букви а)—и) от настоящия параграф, в зависимост от обстоятелствата по всеки отделен случай.

5. Когато действията по правоприлагане, приети съгласно параграф 4, букви а)—г) и е), се окажат неефективни, държавите членки гарантират, че компетентните органи разполагат с правомощие да определят срок, в 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 органи разполагат с правомощия:

а) да прекратят или да изискат от сертифициращ или разрешаващ орган да прекрати сертификат или разрешение относно всички или част от услугите или дейностите, предоставяни от съществен субект;

б) да наложат или изискат от съответните органи или съдилища налагането съгласно националното право на временна забрана спрямо всяко лице, изпълняващо ръководни функции на равнището на главно изпълнително длъжностно лице или законен представител в този съществен субект, както и спрямо всяко друго физическо лице, отговарящо за нарушението, да упражнява управленски функции в този субект.

Тези санкции се прилагат само докато субектът предприеме необходимото действие за отстраняване на недостатъците или за изпълнение на изискванията на компетентния орган, за които са приложени такива санкции.

6. Държавите членки гарантират, че всяко физическо лице, отговорно за съществен субект или действащо като негов 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 задълженията, предвидени в настоящата директива, от страна на този субект. Държавите членки гарантират, че тези физически лица могат да бъдат подвеждани под отговорност за неизпълнението на своите задължения да осигурят спазването на задълженията, предвидени в настоящата директива.

7. При предприемане на действията по правоприлагане или прилагане на санкции съгласно параграфи 4 и 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. Сред считаните за сериозни нарушения са: повторни нарушения, неуведомяване или несправяне с инциденти със значително смущаващо въздействие, неотстраняване на недостатъци съгласно обвързващи

указания от компетентните органи, възпрепятстване на одити или дейности по мониторинг от компетентния орган след констатация на нарушение, предоставяне на невярна или грубо неточна информация във връзка с изискванията за управление на риска или задълженията за докладване по членове 18 и 20.

б) продължителността на нарушението, включително елемента на повторни нарушения;

в) причинената действителна вреда, или възникналите загуби, или потенциалната вреда, която е можело да възникне, доколкото могат да бъдат определени. При оценката на този аспект се вземат предвид, наред с друго, действителните или потенциалните икономически загуби, въздействия върху други услуги, броят на засегнатите или потенциалните потребители;

г) дали нарушението е извършено умишлено или по небрежност;

д) предприетите от субекта мерки за предотвратяване или ограничаване на вредите и/или загубите;

е) придържането към одобрени кодекси на поведение или одобрени механизми за сертифициране;

ж) равнището на съдействие, което носещото отговорност физическо или юридическо лице или лица оказват на компетентните органи.

8. Компетентните органи излагат подробни мотиви за своите решения по правоприлагането. Преди вземането на такива решения компетентните органи уведомяват засегнатите субекти за своите предварителни констатации и предоставят разумен срок на тези субекти да представят становище.

9. Държавите членки гарантират, че техните компетентни органи уведомяват съответните компетентни органи на засегнатата държава членка, определени съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти], когато упражняват своите правомощия по надзор и правоприлагане, имащи за цел да гарантират изпълнението на задълженията съгласно настоящата директива от съществен субект, определен като критичен или като субект, равностоен на критичен субект, съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти]. При поискване от компетентните органи съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти] компетентните органи може да упражняват своите правомощия по надзор и правоприлагане върху съществен субект, определен като критичен или равностоен на такъв.

Член 30

Надзор и правоприлагане за значимите субекти

1. Когато разполагат с доказателства или индикации, че значим субект не изпълнява задълженията по настоящата директива, и по-специално по членове 18 и 20, държавите членки гарантират, че компетентните органи предприемат действия, при необходимост, посредством *последващи* мерки за надзор.

2. Държавите членки гарантират, че при упражняването на своите задачи по надзор във връзка със значимите субекти компетентните органи имат правомощия да подлагат тези субекти на:

а) проверки на място и *последващ* дистанционен надзор;

б) целеви одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;

в) сканирания за сигурност въз основа на обективни, справедливи и прозрачни критерии за оценка на риска;

г) искания за информация, необходима за последваща оценка на мерките за киберсигурност, включително документирани политики за киберсигурност, както и съответствие със задълженията за уведомяване на ENISA съгласно член 25, параграфи 1 и 2;

д) искания за достъп до данни, документи и/или всякаква информация, необходими за изпълнението на задачите по надзор.

3. При упражняване на своите правомощия по параграф 2, букви г) или д) компетентните органи заявяват целта на своето искане и поясняват исканата информация.

4. Държавите членки гарантират, че при упражняване на своите правомощия по правоприлагане във връзка със значимите субекти компетентните органи са оправомощени:

а) да издават предупреждения при неизпълнение на задълженията по настоящата директива от субектите;

б) да изискват посредством обвързващи указания или разпореждане от тези субекти да поправят установените пропуски или нарушението на задълженията по настоящата директива;

в) да разпореждат на тези субекти да преустановяват поведение, което не е в съответствие със задълженията по настоящата директива и да се въздържат от повтарянето на такова поведение;

г) да разпореждат на тези субекти да привеждат своите мерки за управление на риска или задължения за докладване в съответствие със задълженията по членове 18 и 20 по конкретизиран начин и в рамките на посочен период;

д) да разпореждат на тези субекти да уведомяват физическото или юридическото лице или лица, на които предоставят услуги или дейности, потенциално засегнати от значителна киберзаплаха, за възможните защитни или коригиращи мерки, които могат да бъдат предприети от това физическо или юридическо лице или лица в отговор на тази заплаха;

е) да разпореждат на тези субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността в рамките на разумен срок;

ж) да разпореждат на тези субекти да обявяват публично аспектите на неизпълнение на своите задължения, предвидени в настоящата директива, по конкретизиран начин;

з) да правят публично изявление, в което се посочват юридическото или физическото лице или лица, отговорни за нарушението на задължение,

предвидено в настоящата директива, както и характера на това нарушение;

и) да налагат или изискват налагането от съответните органи или съдилища съгласно националното право на административна глоба по член 31 в допълнение към или вместо мерките по букви а)—з) от настоящия параграф, в зависимост от обстоятелствата по всеки отделен случай.

5. Член 29, параграфи 6—8 се прилагат и за мерките по надзор и правоприлагане, предвидени в настоящия член за значимите субекти, изброени в приложение II.

Член 31

Общи условия за налагане на административни глоби на съществените и значимите субекти

1. Държавите членки гарантират, че налагането на административни глоби на съществените и значимите субекти съгласно настоящия член по отношение на нарушения на задълженията, предвидени в настоящата директива, за всеки отделен случай е ефективно, пропорционално и възпиращо.

2. В зависимост от обстоятелствата във всеки конкретен случай административните глоби се налагат в допълнение към или вместо мерките, посочени в член 29, параграф 4, букви а)—и), член 29, параграф 5, и член 30, параграф 4, букви а)—з).

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 29, параграф 7.

4. Държавите членки гарантират, че нарушенията на задълженията по член 18 или член 20, в съответствие с параграфи 2 и 3 от настоящия член, подлежат на административни глоби от поне 10 000 000 EUR или до 2 % — която от сумите е по-голяма — от общия световен годишен оборот на предприятието, към което принадлежи съществения или значимият субект, за предходната финансова година.

5. Държавите членки може да предвидят правомощие за налагане на периодични наказателни плащания с цел принуждаване на съществен или значим субект да преустанови нарушение в съответствие с предходно решение на компетентния орган.

6. Без да се засягат правомощията на компетентните органи по членове 29 и 30, 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 по член 4, параграф 23, които са обект на задълженията, предвидени в настоящата директива.

Член 32

Нарушения, водещи до нарушаване на сигурността на лични данни

1. Когато компетентните органи имат индикации, че нарушението на задълженията по членове 18 и 20 от страна на съществен или значим субект води 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 уведомяват надзорните органи, компетентни съгласно членове 55 и 56 от същия регламент, в рамките на разумен срок.

2. Когато надзорните орани, компетентни съгласно членове 55 и 56 от Регламент (ЕС) 2016/679, решат да упражнят правомощията си по член 58, буква и) от същия регламент и да наложат административна глоба, компетентните органи не налагат административна глоба за същото нарушение съгласно член 31 от настоящата директива. Компетентните органи могат обаче да предприемат правоприлагащи действия или да упражнят правомощията по санкциониране, предвидени в член 29, параграф 4, букви а)—и), член 29, параграф 5, и член 30, параграф 4, букви а)—з) 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 може да уведоми надзорния орган, установен в същата държава членка.

Член 33

Санкции

1. Държавите членки установяват правилата за налагане на санкции, приложими при нарушение на националните разпоредби, приети съгласно настоящата директива, и вземат всички необходими мерки за осигуряване на тяхното прилагане. Предвидените санкции са ефективни, пропорционални и възпиращи.

2. Най-късно до [две] години от влизането в сила на настоящата директива държавите членки съобщават на Комисията тези правила и мерки и ѝ съобщават незабавно всички последващи техни изменения.

Член 34

Взаимопомощ

1. Когато съществен или значим субект предоставя услуги в повече от една държава членка или има основно място на установяване или представител в държава членка, но неговите мрежи и информационни системи са разположени в една или повече други държави членки, компетентният орган на държавата членка на основното място на установяване, или на друго място на установяване, или на представителя и компетентните органи на тези други държави членки си сътрудничат и се подпомагат взаимно, ако е необходимо. Това сътрудничество включва най-малко следното:

   а) компетентните органи, прилагащи мерки по надзор или правоприлагане в държава членка, посредством единното звено за контакт, уведомяват и се консултират с компетентните органи в останалите засегнати държави

членки относно предприетите мерки по надзор и правоприлагане и тяхното проследяване, в съответствие с членове 29 и 30;

б) компетентен орган може да поиска от друг компетентен орган да предприеме мерки по надзор или правоприлагане, посочени в членове 29 и 30;

в) когато компетентен орган получи обосновано искане от друг компетентен орган, той оказва помощ на искащия орган, така че действията по надзор или правоприлагане по членове 29 и 30 да могат да бъдат приложени по ефективен, ефикасен и последователен начин. Тази взаимопомощ може да обхваща искания за информация и мерки по надзор, включително искания за провеждане на проверки на място или дистанционен надзор, или целеви одити на сигурността. Компетентен орган, към който е отправено искане за помощ, не може да откаже това искане, освен ако след обмен на информация с останалите засегнати органи, ENISA и Комисията не бъде установено, че или органът не е компетентен да предостави исканата помощ, или тази помощ не е пропорционална на задачите по надзор на компетентния орган, изпълнявани в съответствие с член 29 или член 30.

2. Когато е подходящо и при общо съгласие компетентните органи от различни държави членки може да извършват общите действия по надзор, посочени в членове 29 и 30.

ГЛАВА VII

Преходни и заключителни разпоредби

Член 35

Преглед

Комисията периодично 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 секторите, подсекторите, размера и вида на субектите, посочени 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. Първият доклад се представя до … [54 месеца след датата на влизане в сила на настоящата директива].

Член 36

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 18, параграф 6 и член 21, параграф 2, се предоставя на Комисията за срок от пет години, считано от [...] г.

3. Делегирането на правомощия, посочено в член 18, параграф 6 и член 21, 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. То поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна, посочена в решението дата. 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 18, параграф 6 и член 21, параграф 2, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на акта 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. Този срок се удължава с два месеца по инициатива на Европейския парламент или на Съвета.

Член 37

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.

Член 38

Транспониране

1. Държавите членки приемат и публикуват до [18 месеца след влизане в сила на настоящата директива] законовите, подзаконовите и административните разпоредби, необходими за да се съобразят с настоящата директива. Те незабавно информират Комисията за това. Те прилагат тези мерки, считано от … [един ден след датата, посочена в първа алинея].

2. Когато държавите членки приемат тези мерки, 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 39

Изменение на Регламент (ЕС) № 910/2014

Член 19 от Регламент (ЕС) № 910/2014 се заличава.

Член 40

Изменения на Директива (ЕС) 2018/1972

Членове 40 и 41 от Директива (ЕС) 2018/1972 се заличават.

Член 41

Отмяна

Директива (ЕС) 2016/1148 се отменя, считано от ... [датата на крайния срок за транспониране на директивата].

Позоваванията на Директива (ЕС) 2016/1148 се считат за позовавания на настоящата директива и се четат в съответствие с таблицата на съответствието в приложение III.

Член 42

Влизане в сила

Настоящата директива влиза в сила на двадесетия ден след публикуването ѝ в *Официален вестник на Европейския съюз*.

Член 43

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

Съдържание

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за Директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

1.2. Съответни области на политиката *(програмен клъстер)*

Съобщителни мрежи, съдържание и технологии

1.3. Предложението/инициативата е във връзка с:

☐ **ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[40]

☒ **продължаване на съществуващо действие**

☐ **сливане или пренасочване на едно или няколко действия към друго/ново действие**

1.4. Мотиви за предложението/инициативата

1.4.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

Целта на преработването е да се повиши нивото на киберустойчивост на широкообхватен набор от предприятия, извършващи дейност в Европейския съюз във всички относими сектори, да се намалят разликите в равнищата на устойчивост в рамките на вътрешния пазар във вече обхванатите от директивата сектори и да се подобрят равнището на съвместна ситуационна осведоменост и колективната способност за подготовка и реакция.

1.4.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки.

Устойчивостта на киберсигурността в Съюза не може да бъде ефективна, ако подходът към нея е различен при отделните национално или регионално обособени системи. С Директивата за МИС тази слабост се преодолява, като се установява рамка за сигурността на мрежите и информационните системи на национално равнище и на равнището на Съюза. В първия периодичен преглед на Директивата за МИС обаче се посочват редица присъщи недостатъци, довели в крайна сметка до значителни различия сред държавите членки от гледна точка на способностите, планирането и степента на защита и засягащи същевременно условията на равнопоставеност за сходни дружества на вътрешния пазар. Намесата на ЕС отвъд настоящите мерки по Директивата за МИС е обоснована главно от: i) трансграничния характер на проблема; ii) потенциала на

[40] Съгласно посоченото в член 58, параграф 2, буква а) или б) от Финансовия регламент.

действията на ЕС за подобряване и улесняване на ефективните национални политики; iii) значението на съгласувани и съвместни действия на политиките в областта на МИС за ефективната защита на данните и поверителността.

Обявените цели могат следователно да бъдат постигнати по-успешно на равнище ЕС, отколкото от държавите членки самостоятелно.

1.4.3. Изводи от подобен опит в миналото

Директивата за МИС е първият хоризонтален инструмент за вътрешния пазар, имащ за цел да подобри устойчивостта на мрежите и системите в Съюза срещу рискове за киберсигурността. Тя вече допринесе значително за повишаване на общото ниво на киберсигурност сред държавите членки. При прегледа на функционирането и прилагането на директивата обаче се очертаха редица слабости, за които, в допълнение към нарастващата цифровизация и нуждата от по-актуална реакция, трябва да бъде намерено решение в преработения правен акт.

1.4.4. Съгласуваност и евентуални полезни взаимодействия с други подходящи инструменти

Новото предложение е изцяло съгласувано и в съответствие с други свързани инициативи, като например предложението за регламент относно оперативната устойчивост на цифровите технологии за финансовия сектор („ОУЦТ“) и предложението за директива относно устойчивостта на критичните оператори на основни услуги. То е в съответствие и с Европейския кодекс за електронни съобщения, Общия регламент относно защитата на данните и Регламента относно електронната идентификация и удостоверителните услуги.

Предложението е съществена част от стратегията на ЕС за Съюза на сигурност.

1.5. Срок на действие и финансово отражение

☐ **ограничен срок на действие**

– ☐ в сила от [ДД/ММ]ГГГГ до [ДД/ММ]ГГГГ

– ☐ Финансово отражение от ГГГГ до ГГГГ за бюджетни кредити за поети задължения и от ГГГГ до ГГГГ за бюджетни кредити за плащания.

☒ **неограничен срок на действие**

– Изпълнение с период на започване на дейност от 2022 г. до 2025 г.

– последван от функциониране с пълен капацитет.

1.6. Планирани методи на управление[41]

Пряко управление от Комисията

– ☒ от нейните служби, включително от нейния персонал в делегациите на Съюза;

– ☐от изпълнителните агенции

☐ **Споделено управление** с държавите членки

☐ **Непряко управление** чрез възлагане на задачи по изпълнението на бюджета на:

– ☐ трети държави или на органите, определени от тях;

– ☐ международни организации и техните агенции (да се уточни);

– ☐ ЕИБ и Европейския инвестиционен фонд;

– Х☐ органите, посочени в членове 70 и 71 от Финансовия регламент;

– ☐ публичноправни органи;

– ☐ частноправни органи със задължение за обществена услуга, доколкото предоставят подходящи финансови гаранции;

– ☐ органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и които предоставят подходящи финансови гаранции;

– ☐ лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.

– *Ако е посочен повече от един метод на управление, пояснете в частта „Забележки“.*

Забележки

Агенцията на Европейския съюз за киберсигурност, ENISA, на която е възложен нов постоянен мандат посредством Акта за киберсигурността, ще подпомага държавите членки и Комисията при прилагането на преработената Директива за МИС.

В резултат на преработената Директива за МИС, считано от 2022/2023 г., ENISA ще има допълнителни области на дейност. Независимо че тези области на дейност биха

[41] Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

били обхванати от основните задачи на ENISA съгласно нейния мандат, те ще доведат до допълнително натоварване за агенцията. По-специално, в допълнение към настоящите ѝ области на дейност, съгласно предложението на Комисията за преработена Директива за МИС от ENISA ще се изисква по-конкретно да включи в работната си програма, наред с друго, следните действия: i) разработване и поддържане на Европейски регистър на уязвимостите (член 6, параграф 2 от предложението), ii) осигуряване на секретариата на Европейската мрежа за връзка на организациите при кибернетични кризи (CyCLONe), (член 14 от предложението) и публикуване на годишен доклад за състоянието на киберсигурността в ЕС (член 15 от предложението), iii) подпомагане на организацията на партньорски проверки между държавите членки (член 16 от предложението), iv) събиране на обобщени данни за инциденти от държавите членки и издаване на технически насоки (член 20, параграф 9 от предложението), v) създаване и поддържане на регистър за субектите, предоставящи трансгранични услуги (член 25 от предложението).

Затова ще бъде отправено искане за 5 допълнителни ЕПРВ от 2022 г. със съответния бюджет около 0,61 млн. евро годишно за обезпечаване на тези нови длъжности (вж. отделната Финансова обосновка за агенциите).

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Комисията периодично ще преразглежда функционирането на директивата и ще докладва на Европейския парламент и на Съвета, за първи път три години след влизането ѝ в сила.

Комисията ще направи също така оценка на правилното транспониране на директивата от държавите членки.

2.2. Системи за управление и контрол

2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол

Отделът в ГД „Съобщителни мрежи, съдържание и технологии“, отговарящ за областта на политиката, ще ръководи прилагането на директивата.

2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им

Много нисък риск, тъй като екосистемата на Директивата за МИС вече е въведена.

2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

Не се прилага. Използва се само административен бюджет („Общ финансов пакет“).

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита, например от стратегията за борба с измамите.

Не се прилага. Използва се само административен бюджет („Общ финансов пакет“).

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Функция от многогодишната финансова рамка и предложени нови разходни бюджетни редове

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансов принос			
	Номер [Функция…7……..……]	Многогод./ едногод.[42]	от държави от ЕАСТ[43]	от държави кандидатки [44]	от трети държави	по смисъла на член [21, параграф 2, буква б)] от Финансовия регламент
	20 02 06 разходи за управление 20 02 06	Едногод.	НЕ	НЕ	НЕ	НЕ

[42] Многогод. = многогодишни бюджетни кредити / Едногод. = едногодишни бюджетни кредити.

[43] ЕАСТ: Европейска асоциация за свободна търговия.

[44] Държави кандидатки и, ако е приложимо, потенциални кандидатки от Западните Балкани.

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

млн. евро (до 3-тия знак след десетичната запетая)

Функция от многогодишната финансова рамка	**<…>**	[Функция……...……]

			2021 г.	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	***След 2027 г.***	**ОБЩО**
Бюджетни кредити за оперативни разходи (разбити по бюджетните редове, изброени в точка 3.1)	Поети задължения	(1)									
	Плащания	(2)									
Бюджетни кредити за административни разходи, финансирани от пакета за програмата[45]	Поети задължения = Плащания	(3)									
ОБЩО бюджетни кредити за финансовия пакет на програмата	Поети задължения	=1+3									
	Плащания	=2+3									

Функция от многогодишната финансова рамка	7	„Административни разходи“ Заседания: Пленарните заседания на групата за сътрудничество за МИС обикновено се провеждат четири пъти годишно. Комисията покрива разходите за храна и пътуване на представителите на 27 държави членки (по един представител от държава членка). Разходите за едно заседание биха могли да достигнат до 15 000 EUR.

[45] Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

		Командировки: Командировките са свързани с наблюдение на прилагането на Директивата за МИС. Пример: За една година (май 2019 г. — юли 2020 г.) се очакваше да бъдат организирани т. нар. „посещения в страните за МИС“ и да се посетят всички 27 държави членки, за да се обсъди прилагането на Директивата за МИС в ЕС.

Тази част следва да бъде попълнена, като се използва таблицата за бюджетни данни от административно естество, която най-напред се въвежда в приложението към финансовата обосновка, което се качва в DECIDE за провеждането на вътрешни консултации между службите.

млн. евро (до 3-тия знак след десетичната запетая)

		2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	*След 2027 г.*	ОБЩО
Човешки ресурси		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Други административни разходи		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
ОБЩО бюджетни кредити за ФУНКЦИЯ 7 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

млн. евро (до 3-тия знак след десетичната запетая)

		2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	*След 2027 г.*	ОБЩО
ОБЩО бюджетни кредити за всички ФУНКЦИИ от многогодишната финансова рамка	Поети задължения									
	Плащания									

3.2.2. Резюме на очаквано отражение върху бюджетните кредити за административни разходи

– ☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

– ☒ Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

години	**2021 г.**	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	**ОБЩО**
ФУНКЦИЯ 7 от многогодишната финансова рамка								
Човешки ресурси	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Други административни разходи	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Извън ФУНКЦИЯ 7[46] от многогодишната финансова рамка								
Човешки ресурси								
Други разходи с административен характер								
Междинен сбор извън ФУНКЦИЯ 7 от многогодишната финансова рамка								

ОБЩО	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Бюджетните кредити, необходими за човешки ресурси и други разходи с административен характер, ще бъдат покрити от бюджетни кредити на ГД, които вече са определени за управлението на действието и/или които са преразпределени в рамките на ГД, при необходимост заедно с допълнително отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

[46] Техническа и/или административна помощ и разходи в подкрепа на изпълнението на програми и/или дейности на ЕС (предишни редове ВА), непреки научни изследвания, преки научни изследвания.

3.2.2.1. Очаквани нужди от човешки ресурси

– ☐ Предложението/инициативата не налага използване на човешки ресурси

– X☐ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в еквиваленти на пълно работно време

години		**2021 г.**	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**
•Длъжности в щатното разписание (длъжностни лица и срочно наети служители)								
Централа и представителства на Комисията		6	6	6	6	6	6	6
Делегации								
Научни изследвания								
• Външен персонал (в еквивалент на пълно работно време — ЕПРВ) — ДНП, МП, КНЕ, ПНА и МЕД [47] Функция 7								
Финансирани от ФУНКЦИЯ 7 от многогодишната финансова рамка	- в централата	3	3	3	3	3	3	3
	- в делегациите							
Финансирани от финансовия пакет на програмата [48]	- в централата							
	- в делегациите							
Научни изследвания								
Други бюджетни редове (да се посочат)								
ОБЩО		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители	• Подготовка на делегирани актове съгласно член 18, параграф 6, член 21, параграф 2, член 36; • Подготовка на актове за изпълнение съгласно член 12, параграф 8, член 18, параграф 5, член 20, параграф 11; • Осигуряване на секретариат за групата за сътрудничество за МИС; • Организиране на пленарните заседания и заседанията на работния процес на групата за сътрудничество за МИС; • Координиране на работата на държавите членки по различни документи (насоки, инструментариуми и пр.); • Осъществяване на връзка с други служби на Комисията, ENISA и национални органи с оглед на прилагането на Директивата за МИС; • Анализиране на националните методи и най-добри практики, свързани с прилагането на Директивата за МИС.
Външен персонал	Подкрепа според необходимостта за осъществяването на горните задачи

[47] ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

[48] Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

3.2.3. Финансов принос от трети страни

Предложението/инициативата:

– X☐ не предвижда съфинансиране от трети страни

– ☐ предвижда следното съфинансиране от трети страни, като оценките са дадени по-долу:

Бюджетни кредити в млн. евро (до 3-тия знак след десетичната запетая)

години	**2021 г.**	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	**ОБЩО**
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

3.3. Очаквано отражение върху приходите

– ☐X Предложението/инициативата няма финансово отражение върху приходите.

– ☐ Предложението/инициативата има следното финансово отражение:

☐ върху собствените ресурси

☐ върху разните приходи

моля, посочете дали приходите са записани по разходни бюджетни редове ☐

млн. евро (до 3-тия знак след десетичната запетая)

Приходен бюджетен ред:	Отражение на предложението/инициативата[49]						
	2021 г.	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**
Статия ……							

За целевите приходи да се посочат съответните разходни бюджетни редове.

Други забележки (например метод/формула за изчисляване на отражението върху приходите или друга информация).

[49] Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднати 20 % за разходи по събирането.

ПРИЛОЖЕНИЕ
към ЗАКОНОДАТЕЛНАТА ФИНАНСОВА ОБОСНОВКА

Наименование на предложението/инициативата:

Предложение за директива за преработване на Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

……
……

1. **БРОЙ И РАЗХОДИ ЗА СЧИТАНИТЕ ЗА НЕОБХОДИМИ ЧОВЕШКИ РЕСУРСИ**
2. **ДРУГИ АДМИНИСТРАТИВНИ РАЗХОДИ**
3. **МЕТОДИ ЗА ИЗЧИСЛЯВАНЕ, ИЗПОЛЗВАНИ ЗА ОЦЕНКА НА РАЗХОДИТЕ**
   - **3.1 Човешки ресурси**
   - **3.2 Други административни разходи**

*Настоящото приложение, **което се попълва от всяка генерална дирекция/служба, участваща в предложението/инициативата**, трябва да придружава законодателната финансова обосновка, когато се провежда междуведомствената консултация.*

Данните от таблиците са включени в таблиците в законодателната финансова обосновка. Те са само за вътрешна употреба в рамките на Комисията.

1. Разходи за считаните за необходими човешки ресурси

☐ Предложението/инициативата не налага използване на човешки ресурси

X☐ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

ФУНКЦИЯ 7 от многогодишната финансова рамка		**2021 г.**		**2022 г.**		**2023 г.**		**2024 г.**		**2025 г.**		**2026 г.**		**2027 г.**		**ОБЩО**	
		ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити
• Длъжности в щатното разписание (длъжностни лица и срочно наети служители)																	
Централа и представителства на Комисията	AD	6	0,90	6	0,90	6	0,90	6	0,90	6	0,90	6	0,90	6	0,90	42	6,3
	AST																
в делегациите на Съюза	AD																
	AST																
• Външен персонал [50] 0,24																	
Общ финансов пакет	ДНП	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	КНЕ																
	ПНА																
в делегациите на Съюза	ДНП																
	МП																

[50] ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

	КНЕ																
	ПНА																
	МЕД																
Други бюджетни редове (*да се посочат*)																	
Междинен сбор — ФУНКЦИЯ 7 от многогодишната финансова рамка		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Извън ФУНКЦИЯ 7 от многогодишната финансова рамка			2021 г.		2022 г.		2023 г.		2024 г.		2025 г.		2025 г.		2025 г.		ОБЩО	
			ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити	ЕПРВ	Бюджетни кредити
• Длъжности в щатното разписание (длъжностни лица и срочно наети служители)																		
Научни изследвания		AD																
		AST																
• Външен персонал [51]																		
Външен персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове „ВА“).	- в централата	ДНП																
		КНЕ																
		ПНА																
	- в делегациите на Съюза	ДНП																
		МП																
		КНЕ																
		ПНА																
		МЕД																
Научни изследвания		ДНП																
		КНЕ																
		ПНА																

[51] ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

Други бюджетни редове (*да се посочат*)																	
Междинен сбор — извън ФУНКЦИЯ 7 от многогодишната финансова рамка																	

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Очаквано отражение върху човешките ресурси на ENISA

Агенцията на Европейския съюз за киберсигурност, ENISA, на която е възложен нов постоянен мандат посредством Акта за киберсигурността, ще подпомага държавите членки и Комисията при прилагането на преработената Директива за МИС. В резултат на преработената Директива за МИС, считано от 2022/2023 г., ENISA ще има допълнителни области на дейност. Независимо че тези области на дейност биха били обхванати от основните задачи на ENISA съгласно нейния мандат, те ще доведат до допълнително натоварване за агенцията. По-специално, в допълнение към настоящите ѝ области на дейност, съгласно предложението на Комисията за преработена Директива за МИС от ENISA ще се изисква по-конкретно да включи в работната си програма, наред с друго, следните действия: i) разработване и поддържане на Европейски регистър на уязвимостите (член 6, параграф 2 от предложението), ii) осигуряване на секретариата на Европейската мрежа за връзка на организациите при кибернетични кризи (CyCLONe), (член 14 от предложението) и публикуване на годишен доклад за състоянието на киберсигурността в ЕС (член 15 от предложението), iii) подпомагане на организацията на партньорски проверки между държавите членки (член 16 от предложението), iv) събиране на обобщени данни за инциденти от държавите членки и издаване на технически насоки (член 20, параграф 9 от предложението), v) създаване и поддържане на регистър за субектите, предоставящи трансгранични услуги (член 25 от предложението). Затова ще бъде отправено искане за 5 допълнителни ЕПРВ от 2022 г. със съответния бюджет около 0,61 млн. евро годишно за обезпечаване на тези нови длъжности (вж. отделната Финансова обосновка за агенциите).

Затова ще бъде отправено искане за 5 допълнителни ЕПРВ от 2022 г. със съответния бюджет за обезпечаване на тези нови длъжности.

☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

☐X Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

	Година **N** [52] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на	**ОБЩО**

[52] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

					отражението (вж. точка 1.6)			

Срочно наети служители (степени AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Срочно наети служители (степени AST)								
Договорно нает персонал	0,160	0,160	0,160	0,160	0,160	0,160		
Командировани национални експерти								**0,96**

ОБЩО	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Изисквания по отношение на персонала (ЕПРВ):

	Година **N** [53] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)	**ОБЩО**

[53] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

Срочно наети служители (степени AD)	3	3	3	3	3	3		**18**
Срочно наети служители (степени AST)								
Договорно нает персонал	2	2	2	2	2	2		**12**
Командировани национални експерти								

ОБЩО	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Други административни разходи

☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

X☐ Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

ФУНКЦИЯ 7 от многогодишната финансова рамка	**2021 г.**	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	**Общо**
В централата:								
Разходи за мисии и представителни разходи	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**

Разходи за конференции и срещи	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Комитети[54]								
Проучвания и консултации								
Информационни системи и системи за управление								
ИКТ оборудване и услуги[55]								
Други бюджетни редове (*да се посочи, където е необходимо*)								
В делегациите на Съюза								
Разходи за командировки, конференции и представителни цели								
Допълнително обучение на персонала								
Придобиване, наемане и свързани с това разходи								
Оборудване, обзавеждане, доставки и услуги								
Междинен сбор за ФУНКЦИЯ 7 от многогодишната финансова рамка	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[54] Посочва се видът на комитета и групата, към която той принадлежи.

[55] ИКТ: Информационни и комуникационни технологии: необходими са консултации с ГД „Информатика“.

млн. евро (до 3-тия знак след десетичната запетая)

Извън ФУНКЦИЯ 7 от многогодишната финансова рамка	**2021 г.**	**2022 г.**	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	**Общо**
Разходи за техническа и административна помощ (невключващи външен персонал) от бюджетни кредити за оперативни разходи (предишни редове „ВА“)								
- в централата								
- в делегациите на Съюза								
Други разходи за управление за изследователски дейности								
Други бюджетни редове (*да се посочи, където е необходимо*)								
Междинен сбор — извън ФУНКЦИЯ 7 от многогодишната финансова рамка								

ОБЩО **ФУНКЦИЯ 7 и извън ФУНКЦИЯ 7** от многогодишната финансова рамка	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Необходимите бюджетни кредити за административни разходи ще бъдат покрити от бюджетните кредити, които вече са разпределени за управлението на действието и/или които са преразпределени, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства, и като се имат предвид съществуващите бюджетни ограничения.

3. Методи за изчисляване, използвани за оценка на разходите

3.1 Човешки ресурси

В тази част се определя методът за изчисляване на считаните за необходими човешки ресурси (предположения за работно натоварване, включително специфични длъжностни характеристики (работни профили в Sysper 2), категории служители и съответните средни разходи)

ФУНКЦИЯ 7 от многогодишната финансова рамка
NB: Средните разходи за всяка категория служители в централата са достъпни на уебсайта BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Длъжностни лица и срочно наети служители 6 длъжностни лица в ЕПРВ (среден разход 0,150) = 0,9 годишно - Подготовка на делегирани актове съгласно член 18, параграф 6, член 21, параграф 2, член 36; - Подготовка на актове за изпълнение съгласно член 12, параграф 8, член 18, параграф 5, член 20, параграф 11; - Осигуряване на секретариат за групата за сътрудничество за МИС; - Организиране на пленарните заседания и заседанията на работния процес на групата за сътрудничество за МИС; - Координиране на работата на държавите членки по различни документи (насоки, инструментариуми и пр.); - Осъществяване на връзка с други служби на Комисията, ENISA и национални органи с оглед на прилагането на Директивата за МИС; - Анализиране на националните методи и най-добри практики, свързани с прилагането на Директивата за МИС.
• Външен персонал 3 ДНП (среден разход 0,08) = 0,24 годишно - Подкрепа според необходимостта за осъществяването на горните задачи

Извън ФУНКЦИЯ 7 от многогодишната финансова рамка
• Само длъжностите, финансирани от бюджета за научни изследвания
• Външен персонал

3.2 Други административни разходи

Опишете подробно метода за изчисляване, използван за всеки бюджетен ред,

и по-специално заложените предположения (например брой заседания на година, средни разходи и др.)

ФУНКЦИЯ 7 от многогодишната финансова рамка
Заседания: Пленарните заседания на групата за сътрудничество за МИС обикновено се провеждат четири пъти годишно. Комисията покрива разходите за храна и пътуване на представителите на 27 държави членки (по един представител от държава членка). Разходите за едно заседание биха могли да достигнат до 15 000 EUR, което прави 60 000 EUR годишно. Командировки: Командировките са свързани с наблюдение на прилагането на Директивата за МИС. Пример: За една година (май 2019 г. — юли 2020 г.) се очакваше да бъдат организирани т. нар. „посещения в страните за МИС“ и да се посетят всички 27 държави членки, за да се обсъди прилагането на Директивата за МИС в ЕС.

Извън ФУНКЦИЯ 7 от многогодишната финансова рамка

ПРИЛОЖЕНИЕ 7

към
РЕШЕНИЕ НА КОМИСИЯТА

относно вътрешните правила за изпълнение на общия бюджет на Европейския съюз (раздел „Европейска комисия“) на вниманието на службите на Комисията

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА — „АГЕНЦИИ“

Настоящата законодателна финансова обосновка обхваща искането за увеличаване на персонала на ENISA с 5 ЕПРВ от 2022 г. за изпълнение на допълнителни дейности, свързани с прилагането на Директивата за МИС. Тези дейности вече са обхванати от правомощията на ENISA.

СЪДЪРЖАНИЕ

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за Директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148

1.2. Съответни области на политиката

Съобщителни мрежи, съдържание и технологии

1.3. Предложението е във връзка с:

☐ **ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[56]

☒ **продължаване на съществуващо действие**

☐ **сливане на едно или няколко действия в друго/ново действие**

1.4. Цел(и)

1.4.1. Общи цели

Целта на преработването е да се повиши нивото на киберустойчивост на широкообхватен набор от предприятия, извършващи дейност в Европейския съюз във всички относими сектори, да се намалят разликите в равнищата на устойчивост в рамките на вътрешния пазар във вече обхванатите от директивата сектори и да се подобрят равнището на съвместна ситуационна осведоменост и колективната способност за подготовка и реакция.

1.4.2. Конкретни цели

За решаването на проблема с ниското ниво на киберустойчивостта на предприятията, осъществяващи дейност в Европейския съюз, конкретно трябва да се гарантира, че субектите във всички сектори, зависими от мрежите и информационните системи и предоставящи ключови услуги за икономиката и обществото като цяло, са задължени да предприемат мерки за киберсигурност и да докладват за инциденти с оглед на повишаване на цялостното равнище на киберустойчивостта в рамките на вътрешния пазар.

За решаването на проблема с нееднаквите равнища на устойчивост в отделните държави членки и сектори конкретно трябва да се гарантира, че всички субекти, които са активни в обхванатите от правната рамка за МИС сектори и които са сходни по размер и имат сравнима роля, са подчинени на един и същ регулаторен режим (т.е. или попадат, или не попадат в обхвата), без значение под чия юрисдикция в ЕС се намират.

За да се гарантира, че всички субекти, които са активни в обхванатите от правната рамка за МИС сектори, са задължени да спазват едни и същи задължения въз основа на концепцията за управление на риска, когато става въпрос за мерки за сигурност, и че те трябва да докладват за всички инциденти по уеднаквен набор от критерии, конкретно

[56] Съгласно посоченото в член 58, параграф 2, буква а) или б) от Финансовия регламент.

трябва да се гарантира, че компетентните органи прилагат предвидените в правните инструменти правила по-ефективно посредством съгласувани мерки за надзор и правоприлагане, както и да се осигури сравнимо ниво на ресурсите, разпределени на компетентните органи в различните държави членки, което би им позволило да изпълняват основните предвидени в рамката за МИС задачи.

За решаването на проблема със съвместна ситуационна осведоменост и липсата на съвместна реакция при кризи, конкретно трябва да се гарантира, че между държавите членки се обменя съществена информация посредством въвеждането на ясни задължения за компетентните органи да споделят информация и да си сътрудничат, когато става въпрос за киберзаплахи и инциденти, като се развие съвместен оперативен капацитет на Съюза за реакция при кризи.

1.4.3. Очаквани резултати и отражение

Да се посочи въздействието, което предложението/инициативата следва да окаже по отношение на бенефициерите/ целевите групи.

Очаква се предложението да донесе значителни ползи: съгласно указаното в прогнозите то може да доведе до намаляване на разходите за инциденти в областта на киберсигурността с 11,3 милиарда евро. Секторният обхват би се разширил значително съгласно рамката за МИС, но наред с горепосочените предимства, тежестта, която може да породят изискванията за МИС, особено от гледна точка на надзора, също би се уравновесила както за новите субекти, които ще бъдат обхванати, така и за компетентните органи. Причината за това е, че с новата рамка за МИС би се установил подход на две нива, с фокус върху големите и ключовите субекти, и разграничаване на режимите за надзор, което позволява за голям брой от тях, по-специално за тези, които се считат за „значими“, но не и за „съществени“, да се прилага само последващ надзор.

Като цяло предложението би довело и до ефикасни съгласувания и полезни взаимодействия и разполага с най-добрия потенциал от всички анализирани варианти на политиката за осигуряване на повишено и съгласувано равнище на киберустойчивостта на ключови субекти в Съюза, което в крайна сметка би довело до икономия на разходи както за предприятията, така и за обществото.

Предложението би довело и до някои разходи за изпълнение и правоприлагане за съответните органи на държавите членки (прогнозирано е общо увеличение с около 20—30 % от ресурсите). Новата рамка обаче би донесла и съществени ползи чрез подобряването на обзора върху ключовите предприятия и на взаимодействието с тях, подобряването на трансграничното оперативно сътрудничество, както и чрез механизми за взаимопомощ и партньорска проверка. Това би довело до цялостно повишаване на способностите в областта на киберсигурността сред държавите членки.

За дружествата, които биха попаднали в обхвата на рамката за МИС, се прогнозира, че би било необходимо увеличение от най-много 22 % от техните разходи за сигурността на ИКТ за първите години след въвеждането на новата рамка за МИС (то би било 12 % за дружествата, които вече попадат в обхвата на настоящата Директива за МИС). Това средно увеличение на разходите за сигурност на ИКТ обаче би довело до пропорционални ползи от тези инвестиции, особено поради значително намаляване на разходите за инциденти с киберсигурността (прогнозирани в размер на 118 милиарда евро за десет години).

Малките предприятия и микропредприятията биха били изключени от обхвата на рамката за МИС. За средните предприятия може да се очаква увеличение в нивото на разходите за сигурността на ИКТ през първите години след въвеждането на новата рамка за МИС. Същевременно, повишаването на равнището на изискванията за сигурност по отношение на тези субекти би стимулирало и техните способности в областта на киберсигурността и би спомогнало за подобряване на управлението на риска при ИКТ.

Предложението би оказало въздействие върху националните бюджети и администрации: би се очаквало прогнозирано увеличение с приблизително 20—30 % от ресурсите в краткосрочен и средносрочен план.

Не се очакват други съществени неблагоприятни въздействия. Предложението се очаква да доведе до по-солидни способности в областта на киберсигурността и следователно

би имало по-значително ограничаващо въздействие върху броя и тежестта на инцидентите, включително нарушенията на сигурността на данните. Вероятно е то да има положително въздействие и върху гарантирането на условията на равнопоставеност в държавите членки на всички субекти, попадащи в обхвата на МИС, и да намали информационната асиметрия в областта на киберсигурността.

1.4.4. Показатели за изпълнението

Да се посочат показателите за проследяване на напредъка и постиженията.

Оценката на показателите се извършва от Комисията, с подкрепата на ENISA и групата за сътрудничество, като се започне три години след влизането в сила на новия правен акт за МИС. Някои от показателите за мониторинг, въз основа на които ще се оценява успехът на прегледа на МИС, са следните:

• Подобрени действия при инциденти: С предприемането на мерки за киберсигурност дружествата не само подобряват способността си за избягване на някои инциденти изцяло, но и своя капацитет за реагиране при инциденти. Ето защо критериите за успех са i) намаляване на средното време, необходимо за установяването на инцидент, ii) времето, което средно е необходимо на организациите да се възстановят от инцидент и iii) средните разходи за причинена от инцидент вреда.

• Повишена осведоменост на висшето ръководство на дружествата за рисковете за киберсигурността: Като изисква от дружествата да предприемат мерки, преработената Директива за МИС би допринесла за повишаване на осведомеността за свързаните с киберсигурността рискове сред висшето ръководство. Това може да се измери, като се проучи в каква степен дружествата в обхвата на МИС отдават приоритет на киберсигурността във вътрешните си политики и процедури, въз основата на вътрешна документация, относими програми за обучение и дейности, свързани с осведомеността на служителите, както и приоритизирането на свързаните със сигурността на ИКТ инвестиции. Ръководството на всички съществени и значими субекти също следва да е запознато с предвидените от Директивата за МИС правила.

• Изравняване на специфичните за секторите разходи: Разходите за сигурност на ИКТ се различават значително в отделните сектори в ЕС. Задължаването на дружествата в повече сектори да предприемат мерки следва да доведе до намаляване на разликите между секторите и между държавите членки по отношение на средния процентен дял на разходите за сигурност на ИКТ от общите разходи за ИКТ, специфичен за отделните сектори.

• По-силни компетентни органи и повишено сътрудничество: С преработената Директива за МИС компетентните органи потенциално биха получили допълнителни задачи. Това би имало измеримо въздействие върху финансовите и човешките ресурси, предназначени за службите за киберсигурност на национално равнище и би оказало и положително въздействие върху капацитета на компетентните органи да си сътрудничат активно, поради което би се увеличил броят на случите, при които компетентните органи действат съвместно за справяне с трансгранични инциденти или провеждане на съвместни дейности по надзор.

• Повишен обмен на информация: Преработването на правилата за МИС би подобрило и обмена на информация между дружествата и с компетентните органи. Една от целите на прегледа би била да се увеличи броят на субектите, участващи в различните форми на обмен на информация.

1.5. Мотиви за предложението/инициативата

1.5.1. Изисквания, които трябва да бъдат изпълнени в краткосрочна или дългосрочна перспектива, включително подробен график за изпълнението на инициативата

Предложението има за цел да се повиши нивото на киберустойчивост на широкообхватен набор от предприятия, извършващи дейност в Европейския съюз във всички относими сектори, да се намалят разликите в равнищата на устойчивост в рамките на вътрешния пазар във вече обхванатите от директивата сектори и да се подобрят равнището на съвместна ситуационна осведоменост и колективната способност за подготовка и реакция. То ще надгради вече постигнатото с прилагането на Директива (ЕС) 2016/1148 през последните четири години.

1.5.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори, например ползи по отношение на координацията, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която е резултат от намесата на ЕС и е допълнителна спрямо стойността, която би била създадена само от отделните държави членки.

Устойчивостта на киберсигурността в Съюза не може да бъде ефективна, ако подходът към нея е различен при отделните национално или регионално обособени системи. С Директивата за МИС тази слабост се преодолява, като се установява рамка за сигурността на мрежите и информационните системи на национално равнище и на равнището на Съюза. В първия периодичен преглед на Директивата за МИС обаче се посочват редица присъщи недостатъци, довели в крайна сметка до значителни различия сред държавите членки от гледна точка на способностите, планирането и степента на защита и засягащи същевременно условията на равнопоставеност за сходни дружества на вътрешния пазар.

Намесата на ЕС отвъд настоящите мерки по Директивата за МИС е обоснована главно от: i) трансграничния характер на проблема; ii) потенциала на действията на ЕС за подобряване и улесняване на ефективните национални политики; iii) значението на съгласувани и съвместни действия на политиките в областта на МИС за ефективната защита на данните и поверителността.

Обявените цели могат следователно да бъдат постигнати по-успешно на равнище ЕС, отколкото от държавите членки самостоятелно.

1.5.3. Изводи от подобен опит в миналото

Директивата за МИС е първият хоризонтален инструмент за вътрешния пазар, имащ за цел да подобри устойчивостта на мрежите и системите в Съюза срещу рискове за киберсигурността. След влизането си в сила през 2016 г. тя вече допринесе значително за повишаване на общото ниво на киберсигурност сред държавите членки. При прегледа на функционирането и прилагането на директивата обаче се очертаха редица слабости, за които, в допълнение към нарастващата цифровизация и нуждата от по-актуална реакция, трябва да бъде намерено решение в преработения правен акт.

1.5.4. Съгласуваност с многогодишната финансова рамка и евентуални полезни взаимодействия с други подходящи инструменти

Новото предложение е изцяло съгласувано и в съответствие с други свързани инициативи, като например предложението за регламент относно оперативната устойчивост на цифровите технологии за финансовия сектор („ОУЦТ“) и предложението за директива относно устойчивостта на критичните оператори на основни услуги. То е в съответствие и с Европейския кодекс за електронни съобщения, Общия регламент относно защитата на данните и Регламента относно електронната идентификация и удостоверителните услуги.

Предложението е съществена част от стратегията на ЕС за Съюза на сигурност.

1.5.5. Оценка на различните налични варианти за финансиране, включително възможностите за преразпределяне на средства

Управлението на тези задачи от ENISA изисква конкретни профили и допълнително работно натоварване, което не може да бъде поето без увеличение на човешките ресурси.

1.6. Срок на действие и финансово отражение на предложението/инициативата

☐ **ограничен срок на действие**

– ☐ Предложение/инициатива в сила от [ДД/ММ]ГГГГ до [ДД/ММ]ГГГГ

– ☐ Финансово отражение от ГГГГ до ГГГГ

☒ **неограничен срок на действие**

– Изпълнение с период на започване на дейност от 2022 г. до 2025 г.,

– последван от функциониране с пълен капацитет.

1.7. Планирани методи на управление[57]

☒ **Пряко управление** от Комисията

чрез

– ☐ изпълнителните агенции

☐ **Споделено управление** с държавите членки

☐Х **Непряко управление** чрез възлагане на задачи по изпълнението на бюджета на:

☐ международни организации и техните агенции (да се уточни);

☐ ЕИБ и Европейския инвестиционен фонд;

☒ органи, посочени в членове 70 и 71;

☐ публичноправни органи;

☐ частноправни органи със задължение за обществена услуга, доколкото предоставят подходящи финансови гаранции;

☐ органи, уредени в частното право на държава членка, на които е възложено осъществяването на публично-частно партньорство и които предоставят подходящи финансови гаранции;

☐ лица, на които е възложено изпълнението на специфични дейности в областта на ОВППС съгласно дял V от ДЕС и които са посочени в съответния основен акт.

Забележки

Агенцията на Европейския съюз за киберсигурност, ENISA, на която е възложен нов постоянен мандат посредством Акта за киберсигурността, ще подпомага държавите членки и Комисията при прилагането на преработената Директива за МИС.

В резултат на преработената Директива за МИС, считано от 2022/2023 г., ENISA ще има допълнителни области на дейност. Независимо че тези области на дейност биха били обхванати от основните задачи на ENISA съгласно нейния мандат, те ще доведат до допълнително натоварване за агенцията. По-специално, в допълнение към настоящите ѝ области на дейност, съгласно предложението на Комисията за преработена Директива за МИС от ENISA ще се изисква по-конкретно да включи в работната си програма, наред с друго, следните действия: i)

[57] Подробности във връзка с методите на управление и позоваванията на Финансовия регламент могат да бъдат намерени на уебсайта BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

разработване и поддържане на Европейски регистър на уязвимостите (член 6, параграф 2 от предложението), ii) осигуряване на секретариата на Европейската мрежа за връзка на организациите при кибернетични кризи (CyCLONe), (член 14 от предложението) и публикуване на годишен доклад за състоянието на киберсигурността в ЕС (член 15 от предложението), iii) подпомагане на организацията на партньорски проверки между държавите членки (член 16 от предложението), iv) събиране на обобщени данни за инциденти от държавите членки и издаване на технически насоки (член 20, параграф 9 от предложението), v) създаване и поддържане на регистър за субектите, предоставящи трансгранични услуги (член 25 от предложението).

Затова ще бъде отправено искане за 5 допълнителни ЕПРВ от 2022 г. със съответния бюджет около 0,61 млн. евро годишно за обезпечаване на тези нови длъжности.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

Комисията периодично ще преразглежда функционирането на директивата и ще докладва на Европейския парламент и на Съвета, за първи път три години след влизането ѝ в сила.

Комисията ще направи също така оценка на правилното транспониране на директивата от държавите членки.

Мониторингът и докладването съгласно предложението ще следват принципите, изложени в постоянния мандат на ENISA съгласно РЕГЛАМЕНТ (ЕС) 2019/881 (Акт за киберсигурността).

Източниците на данни, използвани за планирания мониторинг, биха били предимно от ENISA, групата за сътрудничество, мрежата на ЕРИКС и органите на държавите членки. Освен данните, събрани от докладите (включително годишните доклади за дейността) на ENISA, групата за сътрудничество и мрежата на ЕРИКС, при необходимост биха могли да се използват специфични инструменти за събиране на данни (например проучвания на националните органи, Евробарометър и доклади от кампанията „Месец на киберсигурността“ и общоевропейските учения).

2.2. Системи за управление и контрол

2.2.1. Обосновка на предложените начини за управление, механизми за финансиране на изпълнението, начини за плащане и стратегия за контрол

Отделът в ГД „Съобщителни мрежи, съдържание и технологии“, отговарящ за областта на политиката, ще ръководи прилагането на директивата.

По отношение на ръководството на ENISA член 15 от Акта за киберсигурността предвижда подробен списък на контролните функции на управителния съвет на ENISA.

Съгласно член 31 от Акта за киберсигурността изпълнителният директор на ENISA отговаря за изпълнението на бюджета на ENISA, а вътрешният одитен орган на Комисията се ползва със същите правомощия спрямо ENISA като тези спрямо службите на Комисията. Управителният съвет на ENISA дава становище относно окончателния счетоводен отчет на ENISA.

2.2.2. Информация относно установените рискове и системите за вътрешен контрол, създадени с цел намаляването им

Много нисък риск, тъй като екосистемата на Директивата за МИС вече е установена и обхваща ENISA, която има постоянен мандат след влизането в сила на Акта за киберсигурността през 2019 г.

2.2.3. Оценка и обосновка на разходната ефективност на проверките (съотношение „разходи за контрол ÷ стойност на съответните управлявани фондове“) и оценка на очакваната степен на риска от грешки (при плащане и при приключване)

Исканото увеличение на бюджета се отнася за дял 1 и е предназначено за финансиране на възнагражденията. Това означава много нисък риск от грешка на равнището на изплащане.

2.3. Мерки за предотвратяване на измами и нередности

Да се посочат съществуващите или планираните мерки за превенция и защита, например от стратегията за борба с измамите.

Ще се прилагат мерките на ENISA за предотвратяване и защита, по-специално:

- Плащания за всякакви услуги или поискани проучвания се проверяват от персонала на агенцията преди те да бъдат извършени, като се взимат под внимание договорните задължения, икономическите принципи и добрите финансови и управленски практики. Разпоредби за борба с измамите (наблюдение, изисквания за докладване и т.н.) ще бъдат включени във всички договори и споразумения, сключени между агенцията и получателите на плащанията.

- С оглед на борбата с измамите, корупцията и други незаконни дейности, разпоредбите на Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 25 май 1999 година относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), се прилагат без ограничения.

- Съгласно член 33 от Акта за киберсигурността, към 28 декември 2019 г. ENISA се присъединява към Междуинституционалното споразумение от 25 май 1999 г. между Европейския парламент, Съвета на Европейския съюз и Комисията на Европейските общности относно вътрешните разследвания, провеждани от Европейската служба за борба с измамите (OLAF). ENISA издава незабавно подходящите разпоредби, приложими за всички служители на агенцията.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

3.1. Съответни функции от многогодишната финансова рамка и разходни бюджетни редове

- Съществуващи бюджетни редове

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансов принос			
	Номер	Многогод./ едногод.[58]	от държави от ЕАСТ[59]	от държави кандидатки[60]	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
2	02 10 04	./Едногод.	ДА	НЕ	НЕ	/НЕ

- Поискани нови бюджетни редове

[58] Многогод. = многогодишни бюджетни кредити / Едногод. = едногодишни бюджетни кредити.

[59] ЕАСТ: Европейска асоциация за свободна търговия.

[60] Държави кандидатки и, ако е приложимо, потенциални кандидатки от Западните Балкани.

По реда на функциите от многогодишната финансова рамка и на бюджетните редове.

Функция от многогодишната финансова рамка	Бюджетен ред	Вид на разхода	Финансов принос			
	Номер	Многогод./ едногод.	от държави от ЕАСТ	от държави кандидатки	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент
	[XX.YY.YY.YY]		ДА/НЕ	ДА/НЕ	ДА/НЕ	ДА/НЕ

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

млн. евро (до 3-тия знак след десетичната запетая)

Функция от многогодишната финансова рамка	Номер	[Функция…2 Единен пазар, иновации и цифровизация……..……]

[Орган]: <…ENISA….>			Година **N**[61] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6) **2026 г.**	**2027 г.**		**ОБЩО**
Дял 1:	Поети задължения	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Плащания	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Дял 2:	Поети задължения	(1a)								
	Плащания	(2a)								
Дял 3:	Поети задължения	(3a)								
	Плащания	(3б)								
ОБЩО бюджетни кредити за [орган] <ENISA…….>	Поети задължения	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Плащания	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

Функция от многогодишната финансова рамка	**5**	„Административни разходи“

млн. евро (до 3-тия знак след десетичната запетая)

		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			**ОБЩО**
ГД: <…….>									
• Човешки ресурси									
• Други административни разходи									
ОБЩО ГД <…….>	Бюджетни кредити								

ОБЩО бюджетни кредити съгласно ФУНКЦИЯ 5 от многогодишната финансова рамка	(Общо поети задължения = Общо плащания)								

млн. евро (до 3-тия знак след десетичната запетая)

		Година **N**[62] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6) **2026 г.**	**2027 г.**		**ОБЩО**
ОБЩО бюджетни кредити съгласно ФУНКЦИИ 1—5 от многогодишната финансова рамка	Поети задължения	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Плащания	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

3.2.2. Очаквано отражение върху бюджетните кредити [за органа]

– ☐x Предложението/инициативата не налага използване на бюджетни кредити за оперативни разходи

– ☐ Предложението/инициативата налага използване на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

Бюджетни кредити за поети задължения, в млн. евро (до 3-тия знак след десетичната запетая)

Да се посочат целите и резултатите ⇩			Година **N**		Година **N+1**		Година **N+2**		Година **N+3**		Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)						**ОБЩО**	
	КРАЙНИ ПРОДУКТИ																	
	Вид[63]	Средни разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Бр.	Разходи	Общо брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[64]…																		
- Краен продукт																		
- Краен продукт																		
- Краен продукт																		
Междинен сбор за конкретна цел № 1																		
КОНКРЕТНА ЦЕЛ № 2…																		
- Краен продукт																		

63 Крайните продукти са продукти и услуги, които следва да бъдат доставени (напр.: брой финансирани обмени на обучаващи се, брой километри на изградени пътища и пр.).

64 Съгласно описанието в точка 1.4.2. „Конкретни цели...“

Междинен сбор за конкретна цел № 2																
ОБЩО РАЗХОДИ																

3.2.3. Очаквано отражение върху човешките ресурси на ENISA

3.2.3.1. Резюме

В резултат на преработената Директива за МИС, считано от 2022/2023 г., ENISA ще има допълнителни задачи. При все че тези задачи биха били обхванати от мандата на ENISA, те ще доведат до допълнително натоварване за агенцията. По-специално, в допълнение към настоящите ѝ задачи и съгласно предложението на Комисията за преработена Директива за МИС, на ENISA ще бъдат възложени, наред с другото, следните задачи: i) да разработи и поддържа Европейски регистър на уязвимостите (член 6, параграф 2), ii) да осигурява секретариата на Европейската мрежа за връзка на организациите при кибернетични кризи (CyCLONe), (член 14) и да издава годишен доклад за състоянието на киберсигурността в ЕС (член 15), iii) да подпомага организирането на партньорски проверки между държавите членки (член 16), iv) да събира обобщени данни за инциденти от държавите членки и да издава технически насоки (член 20, параграф 9), v) да създаде и поддържа регистър за субектите, предоставящи трансгранични услуги (член 25).

Затова ще бъде отправено искане за 5 допълнителни ЕПРВ от 2022 г. със съответния бюджет за обезпечаване на тези нови длъжности.

– ☐ Предложението/инициативата не налага използване на бюджетни кредити за административни разходи

– ☐X Предложението/инициативата налага използване на бюджетни кредити за административни разходи съгласно обяснението по-долу:

млн. евро (до 3-тия знак след десетичната запетая)

	Година **N** [65] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6) **2026 г. 2027 г.**			**ОБЩО**
Срочно наети служители (степени AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Срочно наети служители (степени AST)								
Договорно нает персонал	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Командировани национални експерти								

[65] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

ОБЩО	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Изисквания по отношение на персонала (ЕПРВ):

	Година **N** [66] **2022 г.**	Година **N+1** **2023 г.**	Година **N+2** **2024 г.**	Година **N+3** **2025 г.**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6) **2026 г. 2027 г.**			**ОБЩО**
Срочно наети служители (степени AD)	3	3	3	3	3	3		**18**
Срочно наети служители (степени AST)								
Договорно нает персонал	2	2	2	2	2	2		**12**
Командировани национални експерти								
ОБЩО	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Очаквани нужди от човешки ресурси за отговарящата ГД

– ☐ Предложението/инициативата не налага използване на човешки ресурси

– ☐ Предложението/инициативата налага използване на човешки ресурси съгласно обяснението по-долу:

Оценката се посочва в цели стойности (или най-много до един знак след десетичната запетая)

	Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
• **Длъжности в щатното разписание (длъжностни лица и срочно наети служители)**							

[66] Година N е годината, през която започва да се изпълнява предложението/инициативата. Буквата N да се замени с очакваната първа година от изпълнението (например: 2021 г.). Същото за следващите години.

XX 01 01 01 (Централа и представителства на Комисията)								
XX 01 01 02 (Делегации)								
XX 01 05 01 (Непреки научни изследвания)								
10 01 05 01 (Преки научни изследвания)								
• Външен персонал (в еквивалент на пълно работно време: ЕПРВ)[67]								
XX 01 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)								
XX 01 02 02 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)								
XX 01 04 *гг*[68]	- в централата[69]							
	- в делегациите							
XX 01 05 02 (ДНП, КНЕ, ПНА — непреки научни изследвания)								
10 01 05 02 (ДНП, КНЕ и ПНА — преки научни изследвания)								
Други бюджетни редове (да се посочат)								
ОБЩО								

XX е съответната област на политиката или съответният бюджетен дял.

Нуждите от човешки ресурси ще бъдат покрити от персонала на ГД, на който вече е възложено управлението на дейността и/или който е преразпределен в рамките на ГД, при необходимост заедно с всички допълнителни отпуснати ресурси, които могат да бъдат предоставени на управляващата ГД в рамките на годишната процедура за отпускане на средства и като се имат предвид бюджетните ограничения.

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители	
Външен персонал	

[67] ДНП = договорно нает персонал; МП = местен персонал; КНЕ = командирован национален експерт; ПНА = персонал, нает чрез агенции за временна заетост; МЕД = младши експерт в делегация.

[68] Подтаван за външния персонал, покрит с бюджетните кредити за оперативни разходи (предишни редове ВА).

[69] Основно за структурните фондове, Европейския земеделски фонд за развитие на селските райони (ЕЗФРСР) и Европейския фонд за рибарство (ЕФР).

Описание на изчисляването на разходите за еквивалента на пълно работно време (ЕПРВ) следва да бъде включено в приложение V, раздел 3.

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

– ☒ Предложението/инициативата е съгласувано с текущата многогодишна финансова рамка.

– ☐ Предложението/инициативата налага препрограмиране на съответната функция от многогодишната финансова рамка.

Обяснете какво препрограмиране е необходимо, като посочите съответните бюджетни редове и суми. Предложението е съвместимо с МФР за 21/27 г. Прихващането на бюджетните средства, поискани за увеличението на човешките ресурси в ENISA, ще бъде извършено чрез намаляване със същата сума на бюджета на програма „Цифрова Европа“ (ПЦЕ) в същата функция.

– ☐ Предложението/инициативата налага да се използва Инструментът за гъвкавост или да се преразгледа многогодишната финансова рамка[70].

Обяснете какво е необходимо, като посочите съответните функции, бюджетни редове и суми.

3.2.5. Финансов принос от трети страни

– Предложението/инициативата не предвижда съфинансиране от трети страни.

– Предложението/инициативата предвижда съфинансиране съгласно следните прогнози:

млн. евро (до 3-тия знак след десетичната запетая)

	Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)			Общо
Да се посочи съфинансиращият орган								
ОБЩО съфинансирани бюджетни кредити								

[70] Вж. членове 11 и 17 от Регламент (ЕС, Евратом) № 1311/2013 на Съвета за определяне на многогодишната финансова рамка за годините 2014—2020.

3.3. Очаквано отражение върху приходите

– ☐ Предложението/инициативата няма финансово отражение върху приходите.

– ☐ Предложението/инициативата има следното финансово отражение:

☐ върху собствените ресурси

☐ върху разните приходи

☐ моля, посочете дали приходите са записани по разходни бюджетни редове

млн. евро (до 3-тия знак след десетичната запетая)

Приходен бюджетен ред:	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата[71]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
Статия ……								

За разните целеви приходи да се посочат съответните разходни бюджетни редове.

Да се посочи методът за изчисляване на отражението върху приходите.

[71] Що се отнася до традиционните собствени ресурси (мита, налози върху захарта), посочените суми трябва да бъдат нетни, т.е. брутни суми, от които са приспаднати 20 % за разходи по събирането.