ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 4.10.2017 г.
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

ПРИЛОЖЕНИЕ

към

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И ДО СЪВЕТА

Извличане на максимална полза от МИС — по пътя към ефективното прилагане на Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

СЪДЪРЖАНИЕ

ПРИЛОЖЕНИЕ

1. Въведение.

Настоящото приложение има за цел да допринесе за ефективно прилагане, въвеждане и изпълнение на Директивата за мрежовата и информационната сигурност (МИС) (ЕС) 2016/1148 относно сигурността на мрежите и информационните системи в Съюза[1] (наричана по-нататък „директивата за МИС“ или „директивата“) и да подпомогне държавите членки да гарантират ефективното прилагане на правото на ЕС. По-специално неговите специфични цели са три: а) да осигури по-голяма яснота за националните органи относно съдържащите се в директивата задължения, приложими към тези органи, б) да гарантира ефективното изпълнение на задълженията съгласно директивата, приложими към субектите, имащи задължения, свързани с изискванията за сигурност и уведомленията за инциденти, и в) като цяло да допринесе за създаването на правна сигурност за всички съответни участници.

За тази цел с настоящото приложение се предоставят насоки по следните аспекти, които са ключови за постигане на целта на директивата за МИС, т.е. да се гарантира високо общо ниво на сигурност на мрежите и информационните системи в ЕС, което е от основно значение за функционирането на нашето общество и икономика:

- задължението на държавите членки да приемат национална стратегия за сигурност на мрежите и информационните системи (раздел 2);
- създаването на национални компетентни органи, единни звена за контакт и Екипи за реагиране при инциденти с компютърната сигурност (раздел 3);
- изискванията за сигурност и уведомления за инциденти, приложими към операторите на основни услуги и доставчиците на цифрови услуги (раздел 4); и
- връзката между директивата за МИС и друго законодателство (раздел 5)

За да подготви настоящите насоки, Комисията използва информацията и анализа, събрани при изготвяне на директивата, информация от Агенцията на Европейския съюз за мрежова и информационна сигурност („ENISA“) и групата за сътрудничество. Тя използва и опита на определени държави членки. Когато е уместно, Комисията е взела предвид ръководните принципи за тълкуване на правото на ЕС: формулировката, контекста и целите на директивата за МИС. Като се има предвид, че директивата не е транспонирана, все още няма взето решение от Съда на Европейския съюз (Съда на ЕС) или националните съдилища. Следователно е невъзможно да се използва съдебната практика като насоки.

[1] Директива (ЕС) № 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза. Директивата влезе в сила на 8 август 2016 г.

Събрана в един документ, тази информация може да даде на държавите членки добър поглед върху директивата, така че те да вземат информацията под внимание при изготвяне на националното си законодателство. В същото време Комисията подчертава, че настоящото приложение има обвързващ характер и няма за цел създаването на нови правила. Върховна компетентност да тълкува правото на ЕС има Съдът на ЕС.

2. Национална стратегия относно сигурността на мрежите и информационните системи.

Съгласно член 7 от директивата за МИС държавите членки са задължени да приемат национална стратегия относно сигурността на мрежите и информационните системи, която може да се счита за еквивалентна на националната стратегия за киберсигурност („NCSS“). Функцията на националната стратегия е определяне на стратегическите цели и подходящите действия на политиката и регулаторни действия във връзка с киберсигурността. Концепцията за NCSS е широко използвана в международен мащаб и в Европа, по-специално в контекста на работата на ENISA с държавите членки по национални стратегии, в резултат на които наскоро беше изготвен Наръчник за добри практики за NCSS[2].

В този раздел Комисията посочва по какъв начин изискването за наличие на строги национални стратегии относно сигурността на мрежите и информационните системи (член 7) в директивата за МИС засилва подготвеността на държавите членки. В настоящия раздел са разгледани следните аспекти: а) обхватът на стратегията и б) съдържанието и процедурата за приемане.

Както е описано по-долу, правилното транспониране на член 7 от директивата за МИС е от основно значение за постигане на целите на директивата и налага разпределянето на достатъчно финансови и човешки ресурси за тази цел.

2.1. Обхватът на националната стратегия.

Съгласно формулировката на член 7 задължението за приемане на NCSS е приложимо единствено към „секторите, посочени в приложение II, (т.е. енергетика, транспорт, банково дело, финансови пазари, здравеопазване, доставка и снабдяване с питейна вода и цифрова инфраструктура) и към услугите, посочени в приложение III“ (онлайн място за търговия, онлайн търсачка и компютърни услуги „в облак“).

В член 3 от директивата специално е посочен принципът за минимална хармонизация, съгласно който държавите членки може да приемат или запазват разпоредба с оглед постигането на по-високо ниво на сигурност на мрежите и информационните системи. Прилагането на този принцип към задължението за приемане на „NCSS“ дава

[2] ENISA, *National Cyber-Security Strategy Good Practice (Добри практики в областта на националната стратегия за киберсигурност)* 2016 г.). Достъпни на адрес https://www.enisa.europa.eu/publications/ncss-good-practice-guide

възможност на държавите членки да включват повече сектори и услуги от обхванатите в приложение II и приложение III към директивата.

По мнение на Комисията и в светлината на целта на директивата за МИС, т.е. постигане на по-високо ниво на сигурност на мрежите и информационните системи в рамките на Съюза[3], би било препоръчително да се изготви национална стратегия, която обхваща всички съответни измерения на обществото и икономиката, а не само секторите и цифровите услуги, обхванати съответно в приложение II и приложение III към директивата за МИС. Това е в съответствие с международните добри практики (вж. посочените по-нататък Насоки на Международния съюз по далекосъобщения (МСД) и анализа на Организацията за икономическо сътрудничество и развитие (ОИСР) и директивата за МИС.

Както е обяснено допълнително по-долу, това важи в особено голяма степен за публичните администрации, отговарящи за сектори и услуги, различни от изброените в приложение II и приложение III към директивата. Публичните администрации може да обработват чувствителна информация, което обуславя необходимостта да бъдат обхванати от NCSS и планове за управление, с които се предотвратява изтичане на информация и се гарантира надеждна защита на тази информация.

2.2. Съдържание и процедура за приемане на националните стратегии.

Съгласно член 7 от директивата за МИС, NCSS трябва да включва най-малко следното:

i) целите и приоритетите на националната стратегия относно сигурността на мрежите и информационните системи;
ii) управленска рамка за постигане на целта и приоритетите на националната стратегия;
iii) набелязване на мерки във връзка с подготвеността, реагирането и възстановяването, включително сътрудничеството между публичния и частния сектор;
iv) основна информация за съответните образователни и обучителни програми и за програмите за повишаване на осведомеността;
v) основна информация за плановете за научноизследователска и развойна дейност;
vi) план за оценка на риска с цел набелязване на рисковете; и
vii) списък с участниците в изпълнението на стратегията.

Нито член 7, нито съответното съображение 29 съдържат изискванията за приемане на NCSS или повече подробности относно съдържанието на NCSS. Що се отнася до процеса и допълнителните елементи, свързани със съдържанието на NCSS, Комисията счита изложения по-долу подход за подходящ начин за приемане на NCSS. Това се основава на анализа на опита на държавите членки и трети държави, свързан с разработването на собствените стратегии на държавите членки. Друг източник на

[3] Вж. член 1, параграф 1

информация е инструментът за обучение относно NCSS на ENISA, достъпен под формата на видеоклипове и материали за изтегляне от нейния уебсайт[4].

2.3. Процес и въпроси за разрешаване.

Процесът на изготвяне и последващото приемане на национална стратегия е сложен и многостранен, и за да бъде ефективен и успешен, се налага траен ангажимент с експерти в областта на киберсигурността, гражданското общество и националния политически процес. Абсолютно необходимо условие се явява подпомагането на висше административно ниво, най-малко на равнището на държавен секретар или еквивалентно равнище във водещото министерство, както и политическото спонсорство. За успешното приемане на NCSS може да се вземе предвид следният процес в пет стъпки (вж. фигура 1):

Първа стъпка — **Определяне на ръководните принципи и стратегическите цели, произлизащи от стратегията.**

Преди всичко националните компетентни органи следва да определят някои ключови елементи, които NCSS да включва, а именно желаните резултати, на езика на директивата (член 7, параграф 1, буква а) „*цели и приоритети*“ това означава по какъв начин тези резултати допълват националните социални и икономически политики и дали те са съвместими с привилегиите и задълженията, произхождащи от качеството на държава — членка на Европейския съюз. Целите следва да бъдат конкретни, измерими, осъществими, реалистични и да бъдат съпътствани от обвързващи крайни срокове (SMART). Илюстративен пример за това е следното: „*Ще гарантираме, че тази [съпътствана от обвързващи крайни срокове] стратегия се основава на строг и изчерпателен набор от показатели, спрямо които измерваме напредъка към постигане на необходимите резултати.*“[5]

Горепосоченото обхваща също и политическа преценка дали може да бъде получен значителен бюджет, предназначен за изпълнението на стратегията. То предполага и описание на планирания обхват на стратегията, и на различните категории заинтересовани страни от публичния и частния сектор, които следва да участват в изготвянето на различни цели и мерки.

Първата стъпка би могла да се постигне чрез специализирани семинари със старши министерски служители и политици под ръководството на киберспециалисти с професионални комуникационни умения, които могат да подчертаят последиците от липсата на киберсигурност или слабата киберсигурност за съвременната цифрова икономика и обществото.

Втора стъпка — **Разработване на съдържанието на стратегията.**

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool

[5] Откъс от Националната стратегия за киберсигурност на Обединеното кралство за 2016—2021 г., стр. 67.

Стратегията следва да съдържа спомагателни мерки, действия с определен срок на изпълнение и ключови показатели за изпълнението, свързани с оценката, усъвършенстването и подобряването, които ще се извършат след определен период на изпълнение. Тези мерки следва да подпомагат целта, приоритетите и резултатите, изложени като ръководни принципи. Необходимостта от включване на спомагателни мерки е предвидена в член 7, параграф 1, буква в) от директивата за МИС.

Препоръчително е да се сформира ръководна група, председателствана от водещото министерство, която да управлява процеса на изготвяне и да улеснява предоставянето на информация. Това би могло да се постигне чрез редица редакционни групи от съответни служители и експерти по общи теми, например, оценка на риска, изготвяне на планове за действие при извънредни ситуации, управление на инциденти, развитие на уменията, повишаване на осведомеността и научноизследователска и промишлена развойна дейност, и др. Отделно, всеки сектор (например енергетика, транспорт и др.) също би бил приканен да оцени последиците от своето включване, включително набавянето на ресурси, и да ангажира избрани оператори на основни услуги и ключови доставчици на цифрови услуги в определянето на приоритети и даването на предложения в процеса на изготвяне. Участието на заинтересовани страни е от основно значение като се има предвид и нуждата от гарантиране на хармонизирано прилагане на директивата в различните сектори при същевременно отчитане на тяхната специфичност.

Трета стъпка — **Разработване на управленска рамка.**

За да бъде ефикасна и ефективна, управленската рамка следва да се основава на ключови заинтересовани страни, определени приоритети в процеса на изготвяне и на ограниченията и контекста на националните административни и политически структури. Би било желателно отчитането да бъде пряко на политическо равнище, като рамката дава възможност за вземане на решения и разпределяне на ресурси, както и да има принос от експерти в областта на киберсигурността и заинтересовани страни от сектора. Член 7, параграф 1, буква б) от директивата за МИС се отнася до управленската рамка и по-специално предвижда „*ролите и отговорностите на държавните органи и на съответните други участници*“.

Четвърта стъпка — **Съставяне и преглед на проекта за стратегията.**

На този етап проектът за стратегията следва да бъде съставен и прегледан посредством анализ на силните и слабите страни, възможностите и заплахите (SWOT), с който би могло да се определи дали би било необходимо да се преразглежда съдържанието. След първоначалния преглед следва да се проведе консултация със заинтересованите страни. Също от съществено значение би било да се проведе обществена консултация, за да се подчертае пред обществеността значението на предложената стратегия, да се получи информация от всички възможни източници и да се потърси подкрепа за набавянето на ресурсите, необходими за последващото изпълнение на стратегията.

Пета стъпка – **Официално приемане.**

Тази последна стъпка включва официалното приемане на политическо равнище с подходящ бюджет, отразяващ сериозността, с която въпросната държава членка се отнася към киберсигурността. За да се постигнат целите на директивата за МИС и при съобщаване на националния стратегически документ на Комисията съгласно член 7, параграф 3, Комисията насърчава държавите членки да предоставят информация за бюджета. Ангажиментите по отношение на бюджета и необходимите човешки ресурси са абсолютно критични за ефективното изпълнение на стратегията и прилагането на директивата. Тъй като киберсигурността все още е доста нова и бързоразвиваща се област на обществения ред, в повечето случаи са необходими нови инвестиции дори и цялостното положение на публичните финанси да налага ограничения и икономии.

Съвети относно процеса и съдържанието на националните стратегии са налични от различни публични и академични източници, например ENISA[6], МСД[7], ОИСР[8], Световния форум за експертни знания в областта на кибернетиката и Оксфордския университет[9].

2.4. Конкретни стъпки, които държавите членки трябва да предприемат преди срока на транспониране.

Преди приемането на директивата в почти всички държави членки[10] вече бяха публикувани документи, посочени като NCSS. В раздел 6 от настоящото приложение са изброени въведените понастоящем стратегии във всяка държава членка[11]. Обикновено те включват стратегически принципи, насоки, цели, а в някои случаи и специфични мерки за смекчаване на рисковете, свързани с киберсигурността.

---

[6] ENISA, *National Cyber-Security Strategy Good Practice (Добри практики в областта на националната стратегия за киберсигурност)* 2016 г.). Достъпни на адрес https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[7] МСД, *National Cybersecurity Strategy Guide* (Наръчник за националната стратегия за киберсигурност) (2011 г.). Достъпно на адрес http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

През 2017 г. МСД ще издаде също National Cyber Security Strategy Toolkit (Набор от инструменти за националната стратегия за киберсигурност) (вж. презентацията на адрес http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf)

[8] ОИСР, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (Повратен момент в политиката в областта на киберсигурността: анализиране на ново поколение национални стратегии за киберсигурност) (2012 г.). Достъпно на адрес: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

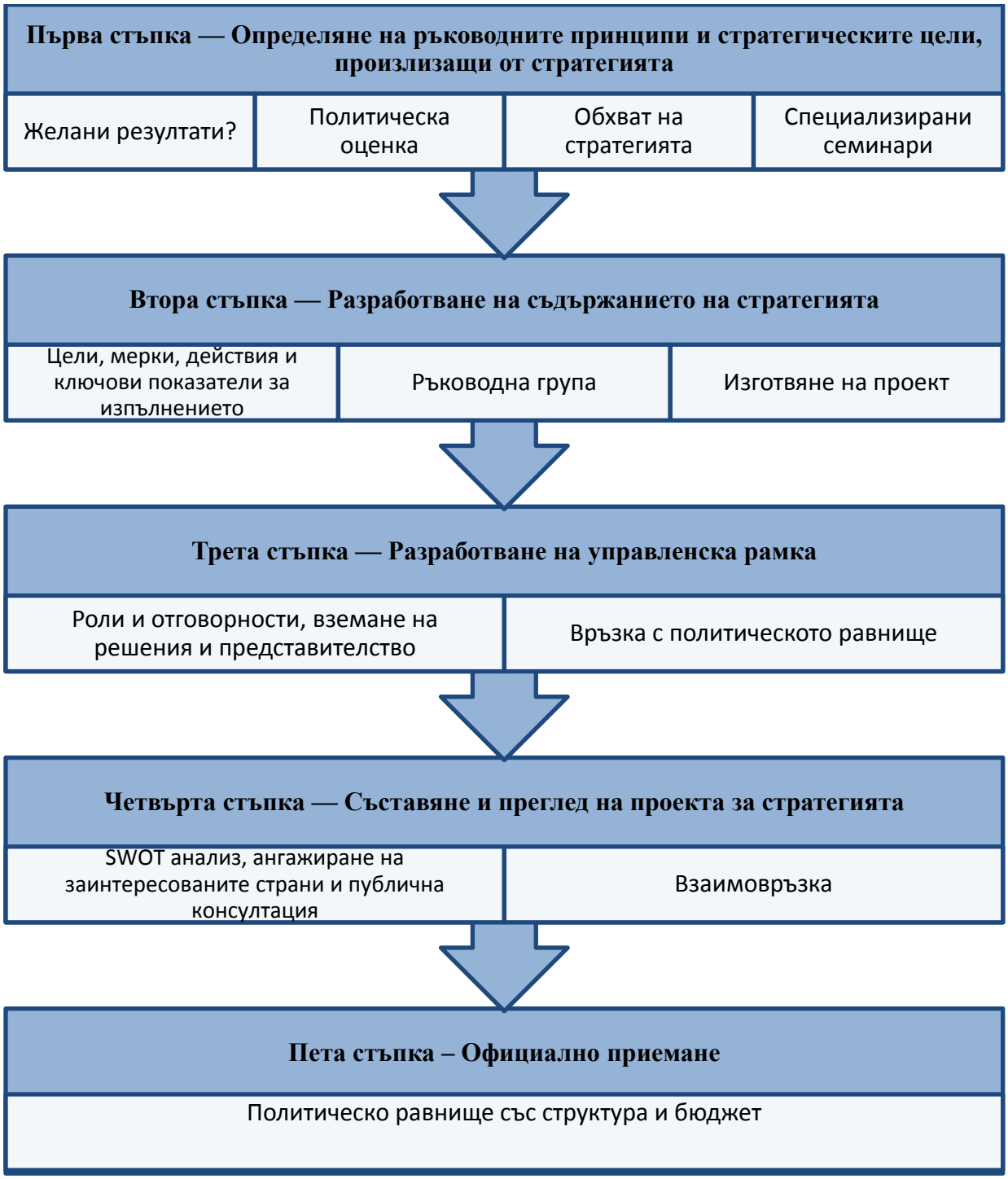
[9] Световен център за капацитет в областта на киберсигурността и Оксфордски университет, Global Cyber *Cybersecurity Capacity Maturity Model for Nations (CMM) (Световен модел на развит капацитет за киберсигурност за нациите) — Преработено издание* (2016 г.). Достъпно на адрес: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

[10] Освен Гърция, където националната стратегия за киберсигурност е в процес на изготвяне от 2014 г. насам (вж. на https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view)

[11] Тази информация е основана на прегледа на NCSS, предоставен от ENISA на https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Като се има предвид, че някои от тези стратегии са приети преди приемане на директивата за МИС, не е задължително те да съдържат всички елементи на член 7. За да се гарантира правилното транспониране, държавите членки ще трябва да извършат анализ на пропуските, като установят съответствието на съдържанието на своите NCSS със седемте отделни изисквания, посочени в член 7 за секторите, посочени в приложение II, и услугите, посочени в приложение III към директивата. След това установените пропуски могат да бъдат отстранени чрез преразглеждане на съществуващите NCSS или чрез вземане на решение за цялостно преразглеждане на принципите на тяхната национална стратегия за МИС, започвайки отначало. Горепосочените насоки относно процедурата за приемане на NCSS са от значение и за преразглеждането и актуализирането на съществуващата NCSS.

Фигура 1: Процес в 5 стъпки за приемане на NCSS



3. Директива за МИС: Национални компетентни органи, единни звена за контакт и екипи за реагиране при инциденти с компютърната сигурност (CSIRT).

Съгласно член 8, параграф 1 държавите членки са задължени да определят един или повече национални компетентни органи, които обхващат най-малко секторите, посочени в приложение II, и услугите, посочени в приложение III, и имат задачата да

наблюдават прилагането на директивата. Държавите членки могат да възложат тези функции на съществуващ орган или органи.

Разделът акцентира върху начина, по който директивата за МИС засилва подготвеността на държавите членки с изискването за наличие на ефективни национални компетентни органи и екипи за реагиране при инциденти с компютърната сигурност (CSIRT). По-конкретно разделът обхваща задължението за определяне на национални компетентни органи, включително ролята на единното звено за контакт. Разгледани са три теми: а) възможни национални структури за управление (напр. централизирани модели, децентрализирани модели и т.н.) и други изисквания; б) ролята на единното звено за контакт и в) екипи за реагиране при инциденти с компютърната сигурност.

3.1. Видове органи.

Съгласно член 8 от директивата за МИС държавите членки са длъжни да определят национални компетентни органи по сигурността на мрежите и информационните системи като изрично се признава възможността да се определят „*един или повече национални компетентни органи*“. Съображение 30 от директивата съдържа обяснение за този политически избор: *„С оглед на различията в националните структури на управление и с цел да се защитят вече съществуващи секторни правила или надзорните и регулаторни органи на Съюза, както и да се избегне дублирането, 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 операторите на основни услуги и доставчиците на цифрови услуги съгласно настоящата директива“*.

Съответно, държавите членки имат свободата да определят един централен орган, отговарящ за всички сектори и услуги, обхванати от директивата, или няколко органа в зависимост например от вида сектор.

Когато вземат решение относно подхода, държавите членки могат да се позоват на опита от националните подходи, използвани в контекста на съществуващото законодателство относно защитата на критичната инфраструктура (CIIP). Както е посочено в таблица 1, в случая на защита на критична информационна инфраструктура (CIIP) държавите членки са решили да предприемат или централизиран, или децентрализиран подход при възлагане на компетентности на национално равнище. Националните примери в настоящия документ са използвани само за илюстративни цели и с оглед на насочване на вниманието на държавите членки към съществуващите организационни рамки. Следователно Комисията не предполага, че използваният от съответните държави модел за CIIP следва задължително да се използва за целите на транспонирането на директивата за МИС.

Държавите членки може да изберат също и различни хибридни мерки, включващи елементи както от централизиран, така и от децентрализиран подход. Избраните мерки може също да бъдат в резултат на съгласуване с предишни национални правила за

управление за различните сектори и услуги, обхванати от директивата, или да са изцяло нововъведени от въпросните органи и съответните заинтересовани страни, определени като оператори на основни услуги и доставчици на цифрови услуги. Наличието на експертни мнения на специалисти по киберсигурност, съображенията от гледна точка на набавянето на ресурси, отношенията между заинтересованите страни и националните интереси (например икономическо развитие, обществена сигурност и др.) също могат да бъдат важни фактори, обуславящи избора на държавите членки.

3.2 Публичност и допълнителни свързани аспекти.

Съгласно член 8, параграф 7, държавите членки трябва да уведомят Комисията относно определянето на национални компетентни органи и техните задачи. Това трябва да се извърши в рамките на срока за транспониране.

Съгласно член 15 и член 17 от директивата за МИС държавите членки са задължени да гарантират, че компетентните органи имат специфични правомощия и средства за изпълнение на задачите, предвидени в тези членове.

Освен това определянето на конкретни субекти за национални компетентни органи трябва да бъде публично. В директивата не се посочва начинът, по който трябва да се постигне тази публичност. Като се има предвид, че целта на това изискване е да се постигне високо ниво на осведоменост на участниците, обхванати от МИС, и на широката общественост, и въз основа на опита от други сектори (телекомуникации, банково дело, лекарства), Комисията счита, че тя би могла да бъде спазена, например посредством добре популяризиран портал.

Съгласно член 8, параграф 5 от директивата за МИС тези органи трябва да разполагат с „достатъчно ресурси“, за да изпълняват възложените им задачи по линия на директивата.

Таблица 1: Национални подходи към защитата на критичната информационна структура (CIIP).

През 2016 г. ENISA публикува изследване[12] на различните подходи, следвани от държавите членки, за защита на техните критични информационни инфраструктури. В него са описани два профила спрямо управлението на CIIP в държавите членки, които могат да се използват в контекста на транспонирането на директивата за МИС.

Профил 1: Децентрализиран подход — с множество секторни органи, компетентни за специфични сектори и услуги, посочени в приложения II и III към директивата.

Децентрализираният подход се характеризира с:

(i) Принцип на субсидиарност
(ii) Силно сътрудничество между публичните органи
(iii)Секторно законодателство

Принцип на субсидиарност.

Вместо създаване или определяне на една агенция с цялостна отговорност, децентрализираният подход следва принципа на субсидиарност. Това означава, че отговорността за изпълнението носи специфичният за сектора орган, който най-добре разбира местния сектор и има съществуващи установени отношения със заинтересованите страни. Според този принцип решенията се вземат от най-близките до засегнатите страни.

Силно сътрудничество между публичните органи.

Поради многообразието от публични органи, извършващи CIIP, много държави членки са разработили схеми за сътрудничество, за да координират работата и усилията на различните органи. Тези схеми за сътрудничество могат да бъдат под формата на неформални мрежи или по-институционализирани форуми или договорености. Тези схеми за сътрудничество обаче имат за цел единствено обмен на информация и сътрудничество между различните публични органи, но нямат правомощия над тях.

Секторно законодателство.

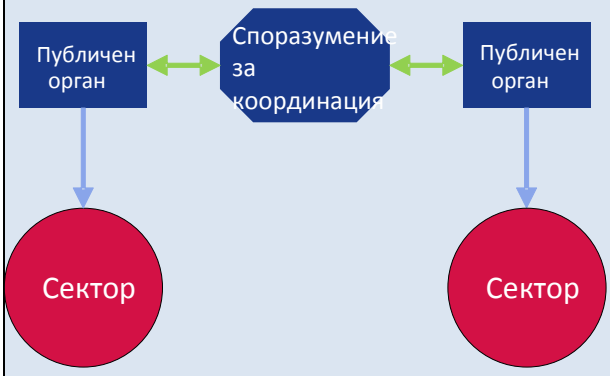
Държавите, които следват децентрализирания подход между критичните сектори често се въздържат от изготвяне на законодателство за целите на CIIP. Вместо това приемането на закони и регламенти е оставено на секторно равнище и следователно може значително да варира между секторите. Предимството на този подход би било привеждането на свързаните с МИС мерки в съответствие със съществуващите секторни регламенти с цел подобряване както на възприемането от сектора, така и на ефективността на прилагането от съответния орган.

Изцяло децентрализираният подход крие значителен риск от понижаване на последователността при прилагането на директивата в множество сектори и услуги. В

[12] https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

този случай директивата предвижда единно национално звено за контакт с цел връзка по трансгранични въпроси като на този субект въпросните държави членки биха могли да възложат също и вътрешната координация и сътрудничеството между множество национални компетентни органи в съответствие с член 10 от директивата.

Фигура 2 — децентрализиран подход.



Примери за децентрализиран подход.

Швеция е добър пример за държава, която следва децентрализиран подход при CIIP. Държавата използва „гледна точка на цялата система“, което означава, че основните задачи на CIIP, като например определянето на съществени услуги и критични инфраструктури, координацията и подкрепата на операторите, регулаторни задачи, както и мерки за подготвеност за реагиране в непредвидени ситуации са задължение на различни агенции и общини. Сред тези агенции са Шведската агенция за непредвидени ситуации на гражданско равнище (MSB), Шведската пощенска и телекомуникационна агенция (PTS) и няколко шведски агенции в областта на отбраната, военното дело и правоприлагането.

За координиране на действията между различните агенции и публичните органи, шведското правителство е разработило мрежа за сътрудничество, включваща органи „със специфични отговорности за сигурността на информираността на обществото“. Тази група за сътрудничество за информационна сигурност (SAMFI) се състои от представители на различните органи и няколко пъти в годината провежда заседания за обсъждане на въпросите, свързани с националната информационна сигурност. Тематичните области на SAMFI са главно стратегическо-политически и обхващат теми като технически въпроси и стандартизация, национално и международно развитие в областта на информационната сигурност или управление и предотвратяване на инциденти в областта на ИКТ. (Шведската агенция за непредвидени ситуации на гражданско равнище (MSB) 2015 г.).

Швеция не е публикувала централен закон за CIIP, приложим към операторите на

критична информационна инфраструктура (CII) в различните сектори. Вместо това изготвянето на законодателство, създаващо задължения за предприятията в определени сектори, е отговорност на съответните публични органи. Например MSB има правото да изготвя регламенти за правителствените органи в областта на информационната сигурност, докато PTS може да задължава операторите да прилагат определени технически или организационни мерки за сигурност въз основа на вторично законодателство.

Друг пример за държава, която има характеристиките на този профил, е Ирландия. Ирландия следва „доктрина на субсидиарност“, според която всяко министерство има задължението да определя критична информационна инфраструктура и да извършва оценка на риска в рамките на своя сектор. Освен това не са приети специфични регламенти за CIIP на национално равнище. Законодателството остава секторно и съществува главно за сектора на енергетиката и сектора на телекомуникациите (2015 г.). Други примери са Австрия, Кипър и Финландия.

Профил 2: Централизиран подход — с един централен орган, компетентен във всички сектори и услуги, посочени в приложения II и III към директивата.

Централизираният подход се характеризира с:

i) Централен орган за всички сектори
ii) Всеобхватно законодателство

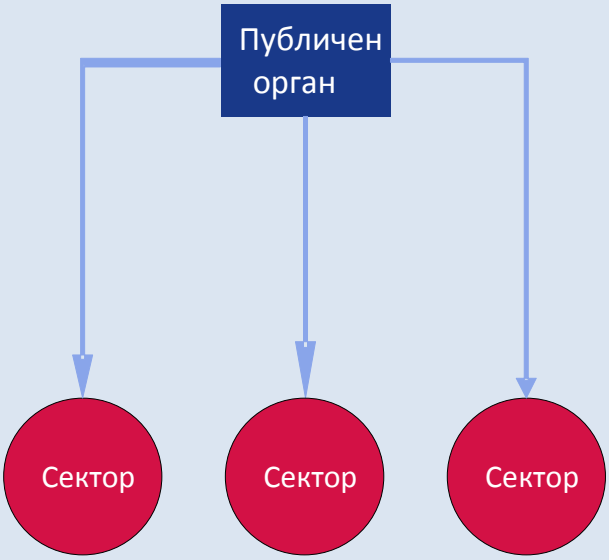
Централен орган за всички сектори.

В държавите членки, които следват централизиран подход, има органи със задължения и широки компетентности в няколко или всички критични сектори, или правомощията на съществуващите органи са разширени. Тези главни органи в областта на CIIP изпълняват комбинация от задачи, като например изготвяне на планове за действие при извънредни ситуации, управление на непредвидени ситуации, регулаторни задачи и подпомагане на частните оператори. В много случаи националният или правителствен CSIRT е част от основния орган за CIIP. Вероятно е централният орган да притежава повече натрупани експертни знания по киберсигурност, отколкото множеството секторни органи, като се има предвид цялостният недостиг на умения по киберсигурност.

Всеобхватно законодателство.

Всеобхватното законодателство създава задължения и изисквания за всички оператори на CII във всички сектори. Това може да се постигне чрез нови всеобхватни закони или чрез допълване на съществуващите специфични за сектора регламенти. Този подход би улеснил съгласуваното прилагане на директивата за МИС във всички обхванати сектори и услуги. С него би се избегнал рискът от пропуски в прилагането, който би могъл да възникне в случай на множество органи със специфичен обхват на задачите.

Фигура 3 — Централизиран подход.



Примери за централизиран подход

Франция е добър пример за държава — членка на ЕС с централизиран подход. През 2011 г. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) на Франция беше обявена за основния национален орган за отбрана на информационните системи. ANSSI има силна надзорна роля за „операторите от основно значение“ (ООЗ): агенцията може да възложи на ООЗ да спазват мерките за сигурност и има правомощието да ги подлага на одит на сигурността. Освен това тя е основното звено за контакт за ООЗ, които са задължени да докладват на агенцията за свързани със сигурността инциденти.

В случаи на свързани със сигурността инциденти ANSSI изпълнява ролята на орган за извънредни ситуации, налагащи CIIP, и взема решения относно мерките, които операторите трябва да предприемат в отговор на кризата. Действията на правителството се координират в рамките на центъра за операции на ANSSI. Засичането на заплахи и реагирането при инциденти на оперативно равнище извършва CERT–FR, който е част от ANSSI.

Във Франция е установена всеобхватна правна рамка за CIIP. През 2006 г. министър-председателят разпореди да бъде съставен списък на секторите с критична инфраструктура. Въз основа на този списък, в който бяха посочени дванадесет сектора от основно значение, правителството определи около 250 ООЗ. През 2013 г. беше обнародван Законът за военно програмиране (LPM)[13]. С него са въведени различни

[13] La loi de programmation militaire

задължения за ООЗ, като например докладване на инциденти или прилагане на мерки за сигурност. Тези изисквания са задължителни за всички ООЗ от всички сектори (френски Сенат, 2013 г.).

3.3. Директива за МИС, член 9: Екипи за реагиране при инциденти с компютърната сигурност (CSIRT).

Съгласно член 9 държавите членки са задължени да определят един или повече CSIRT, натоварени със задачата да предприемат действия при рискове и инциденти за секторите, посочени в приложение II към директивата за МИС, и услугите, посочени в приложение III. Като се има предвид задължението за минимална хармонизация, заложено в член 3 от директивата, държавите членки са свободни да използват CSIRT и за други сектори, които не са обхванати от директивата, като например сектора на публичната администрация.

Държавите членки могат по свой избор да създадат CSIRT в рамките на националния компетентен орган[14].

3.4. Задачи и изисквания.

Задачите на определените CSIRT, изложени в приложение I към директивата за МИС, включват следното:

- Наблюдение на инциденти на национално равнище;
- Подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните заинтересовани страни;
- Реагиране на инциденти;
- Осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация; и
- Участие в мрежата на националните CSIRT (мрежа на CSIRT), създадена съгласно член 12.

В член 14, параграфи 3, 5 и 6 и в член 16, параграфи 3, 6 и 7 са предвидени специфични допълнителни задачи, свързани с уведомленията за инциденти, когато държава членка реши, че CSIRT могат да изпълняват такава роля успоредно с националните компетентни органи или вместо тях.

[14] Вж. член 9, параграф 1, последното изречение.

При транспониране на директивата държавите членки имат опции относно ролята на CSIRT във връзка с изискванията за уведомяване за инциденти. Възможно е пряко задължително докладване на CSIRT, предимството на което е административната ефикасност; като алтернатива държавите членки могат да изберат пряко докладване на националните компетентни органи, като CSIRT имат право на достъп до докладваната информация. Главният интерес на CSIRT е разрешаването на проблеми, свързани с предотвратяването, откриването, реагирането и смекчаването на въздействието на киберинциденти (включително и тези, които не са критични, за да бъдат задължително докладвани) върху заинтересованите им страни, като законосъобразността е отговорност на националните компетентни органи.

Съгласно член 9, параграф 3 от директивата държавите членки трябва да гарантират също, че тези CSIRT имат достъп до сигурна и устойчива инфраструктура на ИКТ.

Според член 9, параграф 4 от директивата държавите членки са задължени да уведомяват Комисията за обхвата на задачите на CSIRT, както и за основните елементи от тяхната процедура за предприемане на действия при инциденти.

Изискванията за CSIRT, определяни от държавите членки, са посочени в приложение I към директивата за МИС. CSIRT трябва да гарантира високо ниво на достъпност на своите комуникационни канали. CSIRT и поддържащите дейността на CSIRT информационни системи се разполагат в зони за сигурност и имат възможността да гарантират непрекъснатост на дейността. Освен това CSIRT следва да има възможност да участва в международни мрежи за сътрудничество.

3.5. Съдействие за развитието на CSIRT.

Програмата за инфраструктурите за цифрови услуги (DSI) в областта на киберсигурността от Механизма за свързване на Европа (MCE) може да осигури значително финансиране от ЕС в помощ на CSIRT на държавите членки, за да бъде подобрен техният капацитет и тяхното взаимно сътрудничество чрез механизъм за сътрудничество и обмен на информация. Механизмът за сътрудничество, разработван в рамките на проекта SMART 2015/1089, е предназначен за улесняване на бързото и ефективно оперативно сътрудничество на доброволна основа между CSIRT на държавите членки, именно в подпомагане на задачите, възложени на мрежата на CSIRT съгласно член 12 от директивата.

Информация за съответните покани за представяне на предложения за изграждане на капацитета на CSIRT на държавите членки е достъпна на уебсайта на Изпълнителната агенция за иновации и мрежи (INEA) на Европейската комисия[15].

Управителният съвет на MCE относно DSI в областта на киберсигурността осигурява неформална структура за насоки на политическо равнище и съдействие на CSIRT на държавите членки за целите на изграждането на капацитет и за прилагането на доброволния механизъм за сътрудничество.

[15] Достъпно на: https://ec.europa.eu/inea/en/connecting-europe-facility

Новосъздаденият CSIRT или определеният за изпълнение на задачите съгласно приложение I към директивата за МИС CSIRT може да разчита на съвета и експертните знания на ENISA, за да подобрява своите резултати и ефективно да изпълнява своята дейност[16]. В тази връзка е важно да се отбележи, че CSIRT на държавата членка би могъл да вземе под внимание част от последно извършените от ENISA дейности. По-специално, както е посочено в раздел 7 от настоящото приложение, Агенцията издаде редица документи и изследвания, в които са описани добри практики, препоръки на техническо равнище, обхващащи оценки на нивото на развитие на CSIRT, за различни способности и услуги на CSIRT. В допълнение към това мрежи на CSIRT на световно (FIRST[17]) и европейско равнище (Trusted Introducer, TI[18]) обмениха насоки и най-добри практики.

3.6. Ролята на единното звено за контакт.

Съгласно член 8, параграф 3 от директивата за МИС всяка държава членка трябва да определи национално единно звено за контакт, което ще изпълнява функция за връзка, така че да се осигури трансграничното сътрудничество със съответните органи в други държави членки и с групата за сътрудничество, както и с мрежата на CSIRT[19], създадена по силата на самата директива. Съображение 31 и член 8, параграф 4 съдържат *обосновката* за това изискване, т.е. за улесняване на трансграничното сътрудничество и комуникация. Това е от особена необходимост, като се има предвид, че държавите членки може да решат да имат повече от един национален орган. Следователно единното звено за контакт би улеснило определянето и сътрудничеството на органите между различните държави членки.

Свързващата роля на единното звено за контакт вероятно ще включва взаимодействие със секретариатите на групата за сътрудничество и на мрежата на CSIRT в случаите, когато националното единно звено за контакт не е нито CSIRT, нито член на групата за сътрудничество. Освен това държавите членки трябва да гарантират, че на единното звено за контакт се предоставя информация за получените уведомления от операторите на основни услуги и доставчиците на цифрови услуги.[20]

Член 8, параграф 3 от директивата предвижда, че ако държава членка възприеме централизиран подход, т.е. назначи само един компетентен орган, този орган ще има ролята и на единно звено за контакт. Ако държава членка избере децентрализиран подход, тя може да избере един от различните компетентни органи като единно звено за контакт. Независимо от избрания институционален модел, когато компетентен орган, CSIRT и единното звено за контакт са отделни субекти, държавите членки имат

[16] Вж. член 9, параграф 5 от директивата за МИС.
[17] Forum of Incident Response and Security Teams (Форум за реагиране при инциденти и екипи за сигурност (https://www.first.org/)
[18] https://www.trusted-introducer.org/
[19] Мрежа от национални CSIRT за оперативно сътрудничество между държавите членки съгласно член 12
[20] Вж. член 10, параграф 3

задължението да гарантират ефективното сътрудничество помежду им, за да изпълнят задълженията си, изложени в директивата[21].

Единното звено за контакт е задължено до 9 август 2018 г. и всяка година след това да подава обобщен доклад до групата за сътрудничество относно получените уведомления, който включва броя уведомления, естеството на инцидентите и предприетите от органите мерки, като например уведомяване на други засегнати държави членки относно инцидента или предоставянето на съответна информация на уведомяващото предприятие за предприемането на действия по отношение на инцидента.[22] При поискване от страна на компетентния орган или CSIRT, единното звено за контакт трябва да препрати уведомленията на операторите на основни услуги до единните звена за контакт на други държави членки, засегнати от инцидентите.[23]

В рамките на срока за транспониране държавите членки трябва да уведомяват Комисията относно определянето на единното звено за контакт и неговите задачи. Определянето на единното звено за контакт трябва да стане публично, по същия начин, както националните компетентни органи. Комисията публикува списъка на определените единни звена за контакт.

3.7. Санкции.

Член 21 предоставя свобода на държавите членки да вземат решение относно вида и естеството на приложимите санкции, при условие че те са ефективни, пропорционални и възпиращи. С други думи държавите членки по принцип могат свободно да избират максималната сума на санкциите изложени в тяхното национално законодателство, но избраната сума или процент следва да позволява на националните органи при всеки отделен случай да налагат ефективни, пропорционални и възпиращи санкции, отчитайки различни фактори, като например тежестта или честотата на нарушението.

4. Субекти, имащи задължения относно изискванията за сигурност и уведомленията за инциденти.

Субектите, които имат важна роля за обществото и икономиката, посочени в член 4, параграфи 4 и 5 от директивата като оператори на основни услуги (ООУ), и доставчиците на цифрови услуги (ДЦУ), трябва да предприемат подходящи мерки за сигурност и да уведомяват съответните национални органи за сериозни инциденти. *Обосновката* е, че последиците от свързаните със сигурността инциденти в такива служби биха могли да представляват сериозна заплаха за функционирането на тези услуги, което може да предизвика значителни смущения в икономическите дейности и

[21] Вж. член 10, параграф 1
[22] Пак там
[23] Вж. член 14, параграф 5

за обществото като цяло и потенциално да подкопае доверието на потребителите и да причини големи вреди на икономиката на Съюза[24].

Този раздел съдържа преглед на субектите, включени в обхвата на приложения II и III от директивата за МИС, както и списък с техните задължения. Определянето на оператори на основни услуги е подробно разгледано, като се има предвид значението на тази процедура за хармонизираното прилагане на директивата за МИС в целия ЕС. В него са посочени също и подробни обяснения на определенията за цифрови инфраструктури и доставчици на цифрови услуги. Разгледано е и възможното включване на допълнителни сектори и е дадено допълнително обяснение за специфичния подход във връзка с ДЦУ.

4.1. Оператори на основни услуги (ООУ).

Директивата за МИС не съдържа изрично определение за субектите, които се считат за ООУ съгласно нейния обхват. Вместо това в нея са предвидени критерии, които държавите членки ще трябва да прилагат, за да проведат процес на определяне, чрез който ще се определят окончателно отделните предприятия, принадлежащи към категорията субекти, изброени в приложение II, които ще бъдат считани за оператори на основни услуги и следователно ще бъдат предмет на задълженията съгласно директивата.

4.1.1. Категории субекти, посочени в приложение II към директивата за МИС.

В член 4, параграф 4 ООУ са определени като публични или частни субекти от категориите, посочени в приложение II към директивата за МИС, които отговарят на изискванията на член 5, параграф 2. В приложение II са посочени секторите, подсекторите и категориите субекти, за които всяка държава членка трябва да изпълни процеса на определяне съгласно член 5, параграф 2[25]. Секторите включват енергетика, транспорт, банково дело, инфраструктури на финансовия пазар, здравеопазване, води и цифрова инфраструктура.

За повечето субекти, които принадлежат към „традиционните сектори“, законодателството на ЕС съдържа добре разработени определения, на които е направено позоваване в приложение II. Това обаче не важи за сектора на цифровата инфраструктура, посочен в точка 7 от приложение II, включително точките за обмен в интернет, системите за имена на домейни и регистрите на имена на домейни от първо ниво. Следователно с цел пояснияване на тези определения. те са подробно обяснени в следващия параграф.

1) Точка за обмен в интернет (ТОИ).

[24] Вж. съображение 2.
[25] Вж. по-долу под раздел 4.1.6 за повече информация относно процеса на определяне

Понятието „точка за обмен в интернет“ е определено в член 4, параграф 13 и допълнително пояснено в съображение 18, и може да се опише като мрежово средство, което дава възможност за свързване на повече от две технически независими автономни системи, преди всичко с цел улесняване на обмена на интернет трафик. Точката за обмен в интернет може да бъде описана също като физическо местоположение, в което редица мрежи могат да обменят интернет трафик помежду си посредством суич. Основната цел на ТОИ е да се даде възможност за пряко свързване на мрежите посредством тази точка на обмен, вместо чрез една или повече мрежи на трети страни. Обикновено доставчикът на ТОИ няма задължение за насочване на интернет трафика. Това се извършва от доставчиците на мрежата. Предимствата на прякото свързване са многобройни, но основните сред тях са свързани с цената, забавянето и честотната лента. Трафикът, преминаващ през такава точка на обмен, обикновено не се таксува от страните, за разлика от трафика до доставчик на интернет услуги (ДИУ) нагоре по веригата. Пряката връзка, често намираща се в същия град, в който са и двете мрежи, спомага да се избегне необходимостта данните да изминават дълги разстояния, за да достигнат от една мрежа до друга, с което се намалява забавянето.

Следва да се отбележи, че определението за ТОИ не обхваща физическите точки, в които се свързват само две физически мрежи (т.е. доставчиците на мрежа, като например BASE и PROXIMUS). Следователно при транспониране на директивата държавите членки трябва да направят разграничение между операторите, които улесняват обмена на агрегиран интернет трафик между множество оператори на мрежи и тези, които са оператори с една мрежа и физически свързват своите мрежи въз основа на споразумение за свързване. В последния случай доставчиците на мрежи не са обхванати от определението в член 4, параграф 13. В съображение 18 има пояснение по този въпрос, което гласи, че ТОИ не осигуряват достъп до мрежа, нито служат като транзитен доставчик или превозвач. Последната категория доставчици са предприятия, които предоставят обществени съобщителни мрежи и/или услуги, които са предмет на задължения за сигурност и уведомление съгласно член 13а и член 13б от Директива 2002/21/ЕО, и следователно са изключени от приложното поле на директивата за МИС[26].

2) Система за имена на домейни (Domain Name System — DNS).

Понятието „система за имена на домейни“ е определено в член 4, параграф 14 като *„йерархично разпределена и мрежова система за именуване на домейни, която разпределя заявки за имена на домейни“*. По-конкретно DNS може да се опише като йерархично разпределена система за именуване за компютри, услуги или всякакъв друг ресурс, свързан с интернет, който позволява кодиране на имена на домейни в IP (интернет протокол) адреси. Основната роля на системата е да превръща дадените

[26] Вж. раздел 5.2 за повече информация относно връзката между директивата за МИС и Директива 2002/21/ЕО

имена на домейни в IP адреси. За тази цел DNS управлява база данни и използва сървъри за имена и преобразувател, за да позволи този вид „преобразуване“ на имената на домейни във функциониращи IP адреси. Въпреки че кодирането на имена на домейни не е единствената отговорност на DNS, то е основна задача на системата. Правното определение в член 4, параграф 14 акцентира върху основната роля на системата от гледна точка на потребителя, без да навлиза в по-технически детайли, като например функционирането на пространството за името на домейна, сървърите за имена, преобразувателите и др. И накрая, в член 4, параграф 15 се пояснява кой трябва да се счита за доставчик на услугите на DNS.

3) Регистър на имена на домейни от първо ниво (регистър на имена TLD).

Регистърът на имена на домейни от първо ниво е определен в член 4, параграф 16 като субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от първо ниво. Това администриране и управление на имена на домейни включва кодиране на TLD имена в IP адреси.

IANA (Служба за присвояване на имена и адреси в интернет) е отговорна за общата координация на DNS Root, изготвянето на адреси по интернет протокол и други ресурси на интернет протокол. По-специално IANA отговаря за определянето на генерични домейни от първо ниво (gTLD), напр. „com“, и имена на национални домейни от първо ниво (ccTLD), напр. „.be“ на оператори (регистри) и поддръжката на техните технически и административни детайли. IANA поддържа общ регистър на разпределените TLD и има роля в разпространението на този списък до потребителите на интернет по целия свят, както и във въвеждането на нови TLD.

Важна задача на регистрите е определянето на имена на второ ниво на така наречените регистранти към съответните им TLD. Тези регистранти могат също самостоятелно да предоставят имена на домейни на трето ниво, ако решат. ccTLD имат за цел да представляват държава или територия въз основа на стандарт ISO 3166-1. Генеричните TLD обикновено нямат определено географско или държавно наименование.

Следва да се отбележи, че функционирането на регистъра на имена TLD може да включва предоставяне на DNS. Например съгласно правилата на IANA за делегиране определеният субект, отговарящ за ccTLD, трябва – наред с другото – да извършва надзор над имената на домейни и да управлява DNS на тази държава[27]. Държавите членки трябва да вземат под внимание тези обстоятелства, когато провеждат процеса на определяне на операторите на основни услуги съгласно член 5, параграф 2.

4.1.2. Определяне на операторите на основни услуги.

Съгласно изискванията на член 5 от директивата всяка държава членка е задължена да проведе процес на определяне във връзка с всички субекти от категориите, изброени в приложение II, които имат законосъобразно установяване на територията на тази

[27] Информацията е достъпна на адрес: https://www.icann.org/resources/pages/delegation-2012-02-25-en

държава членка. В резултат на тази оценка всички субекти, които отговарят на критериите, изложени в член 5, параграф 2, се определят като ООУ и са предмет на задълженията за сигурност и уведомяване съгласно член 14.

До 9 ноември 2018 г. държавите членки трябва да определят оператори за всеки сектор и подсектор. В помощ на държавите членки през целия този процес групата за сътрудничество понастоящем разработва документ с насоки, който съдържа съответна информация относно необходимите стъпки и най-добрите практики, свързани с определянето на ООУ.

Освен това, в съответствие с член 24, параграф 2, групата за сътрудничество обсъжда процеса, същността и вида на националните мерки, даващи възможност за определяне на операторите на основни услуги в конкретен сектор. Преди 9 ноември 2018 г. в групата за сътрудничество държавите членки може да обсъдят своите проекти на национални мерки, даващи възможност за определяне на операторите на основни услуги.

4.1.3. Включване на допълнителни сектори.

При отчитане на задължението за минимална хармонизация, заложено в член 3, държавите членки може да приемат или запазват разпоредби, с което да постигнат по-високо ниво на сигурност на мрежите и информационните системи. В тази връзка държавите членки имат свободата да разширяват задълженията за сигурност и уведомяване съгласно член 14, така че те да обхващат субекти, които принадлежат и към други сектори и подсектори, различни от посочените в приложение II към директивата за МИС. Различни държави членки са решили или в момента обмислят дали да включат някои от следните допълнителни сектори:

i) Публични администрации

Публичните администрации може да предлагат основните услуги съгласно приложение II към директивата, като спазват изискванията на член 5, параграф 2. В такива случаи публичните администрации, предлагащи такива услуги, ще бъдат обхванати от съответните изисквания за сигурност и задължения за уведомяване. И обратно, когато публичните администрации предлагат услуги, които не попадат в горепосочения обхват, тези услуги няма да бъдат обхванати от съответните задължения.

Публичните администрации имат задължението надлежно да предоставят публичните услуги, извършвани от правителствени органи, регионални и местни органи, агенции и свързани предприятия. Тези услуги често предполагат създаване и управление на лични и корпоративни данни относно лица и организации, които могат да бъдат споделяни и предоставяни на множество публични органи. В по-широк план високото ниво на сигурност на използваните от публичните администрации мрежови и информационни системи е важен интерес за обществото и икономиката като цяло. Затова Комисията е на мнение, че би било разумно държавите членки да обмислят включване на публичната администрация в обхвата на националното законодателство за транспониране на директивата отвъд предоставянето на основни услуги, изложени в приложение II и член 5, параграф 2.

ii) Пощенски сектор

Пощенският сектор обхваща предоставянето на пощенски услуги, като например събиране, сортиране, транспортиране и доставка на пощенски пратки.

iii) Сектор на хранителните продукти

Секторът на хранителните продукти се отнася до производството на селскостопански и други хранителни продукти и би могъл да включва основни услуги, като например осигуряване на продоволствена сигурност и гарантиране на качеството и безопасността на храните.

iv) Химическа и ядрена промишленост

Химическата и ядрената промишленост се отнася по-специално до съхранението, производството и преработването на химически и нефтохимически продукти или ядрени материали.

v) Сектор на околната среда

Дейностите в областта на околната среда обхващат предоставянето на стоките и услугите, необходими за защита на околната среда и управление на ресурсите. Следователно дейностите са насочени към предотвратяване, намаляване и премахване на замърсяването и съхраняване на наличните запаси от природни ресурси. В този сектор основните услуги биха могли да бъдат наблюдение и контрол на замърсяването (напр. на въздуха и водите) и метеорологичните явления.

vi) Гражданска защита

Целта на сектора на гражданската защита е предотвратяване, подготвяне за и реагиране на природни и предизвикани от човека бедствия. Предвидените за тази цел услуги могат да бъдат активиране на номера за спешни повиквания и извършване на действия по предоставяне на информация за, задържане и реагиране на извънредни ситуации.

4.1.4. Юрисдикция.

Съгласно член 5, параграф 1 всяка държава членка трябва да определи ООУ с място на установяване на тяхна територия. В разпоредбата не се конкретизира типът законосъобразно установяване, но в съображение 21 е пояснено, че това установяване предполага ефективно и реално упражняване на дейност чрез стабилни правила, докато правната форма на тези правила не следва да бъде определящ фактор. Това означава, че държава членка може да има юрисдикция над оператор на основни услуги не само в случаите, когато главното управление на оператора се намира на нейна територия, но и в случаите, когато операторът има например филиал или друг тип законосъобразно установяване.

В резултат на това е възможно няколко държави едновременно да имат юрисдикция над един и същ субект.

4.1.5. Информация, която се предоставя на Комисията.

За целите на прегледа, който Комисията трябва да извърши съгласно член 23, параграф 1 от директивата за МИС, държавите членки са задължени да представят на Комисията до 9 ноември 2018 г. и на всеки две години след това следната информация:

- Национални мерки, даващи възможност за определяне на ООУ;
- Списъка на основните услуги;
- Броят ООУ, определени за всеки сектор, посочен в приложение II, и значението на тези оператори за сектора; и
- Праговете, когато има такива, използвани за определяне на равнището на доставките спрямо броя на ползвателите, разчитащи на тази услуга, в съответствие с посоченото в член 6, параграф 1, буква а), или значението на оператора в съответствие с член 6, параграф 1, буква е).

Предвиденият в член 23, параграф 1 преглед, който предшества подробния преглед на директивата, отразява значението, което съзаконодателите придават на правилното транспониране на директивата във връзка с определянето на оператори на основни услуги, за да се избегне разпокъсаност на пазара.

За да може този процес да се извърши по възможно най-добър начин, Комисията насърчава държавите членки да обсъдят тази тема, както и да обменят съответния опит в групата за сътрудничество. Освен това Комисията насърчава държавите членки да споделят с Комисията — поверително, ако е необходимо — списъците на определените оператори на основни услуги (които са избрани окончателно) в допълнение към цялата информация, която държавите членки трябва да представят на Комисията съгласно директивата. Наличието на такива списъци би улеснило и довело до по-висока оценка на Комисията на съгласуваността на процеса на определяне и би дало възможност да се направи сравнение между подходите на държавите членки, с което ще се гарантира по-добро постигане на целите на директивата.

4.1.6. Как се провежда процесът на определяне?

Както е показано на фигура 4, националният орган следва да провери шест ключови въпроса при провеждане на процеса на определяне относно конкретен субект. В следващия параграф всеки въпрос съответства на стъпка, която трябва да се предприеме съгласно член 5 във връзка с член 6, както и при отчитане на приложимостта на член 1, параграф 7.

Стъпка 1 – **Принадлежи ли субектът към сектор/подсектор и съответства ли на категорията, обхваната от приложение II към директивата?**

Националният орган следва да оцени дали субект, установен на негова територия, принадлежи към секторите и подсекторите, посочени в приложение II към директивата. Приложение II обхваща различни икономически сектори, които се считат за ключови за

гарантиране на правилното функциониране на вътрешния пазар. По-специално приложение II се отнася до следните сектори и подсектори:

- Енергетика: електроенергия, нефт и газ
- Транспорт: въздушен, железопътен, воден и сухопътен
- Банково дело: кредитни институции
- Инфраструктури на финансовия пазар: места за търговия, централни контрагенти
- Здравеопазване: доставчици на здравно обслужване (включително болници и частни клиники)
- Вода: доставка и снабдяване с питейна вода
- Цифрова инфраструктура: точки за обмен в интернет, доставчици на услуги за система за имена на домейни, регистри на имена на домейни от първо ниво[28]

Стъпка 2 — **Приложим ли е *lex specialis*?**

Като следваща стъпка националният орган трябва да оцени дали е приложима разпоредбата за *lex specialis*, заложена в член 1, параграф 7. По-специално в разпоредбата се посочва, че ако има правен акт на Съюза, който налага на доставчиците на цифрови услуги или операторите на основни услуги задължения за сигурност и/или уведомяване, които са най-малкото равностойни на съответните задължения, съдържащи се в директивата за МИС, се прилагат задълженията съгласно специалния правен акт. Освен това в съображение 9 се пояснява, че ако задълженията по член 1, параграф 7 са изпълнени, държавите членки следва да прилагат разпоредбите на специфичните за конкретен сектор правни актове на ЕС, включително онези от тях, които се отнасят за юрисдикцията. В противен случай съответните разпоредби от директивата за МИС няма да бъдат приложими. В този случай компетентният орган не следва да продължава процеса на определяне съгласно член 5, параграф 2[29].

Стъпка 3 – **Предоставя ли операторът основна услуга по смисъла на директивата?**

Съгласно член 5, параграф 2, буква а), е необходимо субектът, който е предмет на определяне, да предоставя услуга, която е от основно значение за поддържането на особено важни обществени и/или стопански дейности. Когато извършват тази оценка, държавите членки следва да отчетат факта, че един субект може да предоставя както основни, така и неосновни услуги. Това означава, че изискванията за сигурност и уведомяване от директивата за МИС ще бъдат приложими към конкретен оператор само доколкото той предоставя основни услуги.

В съответствие с член 5, параграф 3 всяка държава членка следва да изготви списък на всички основни услуги, предоставяни от ООУ на тяхна територия. Този списък ще

[28]Тези субекти са допълнително изяснени в раздел 4.1.1.

[29] Повече информация относно приложимостта на *lex specialis* се съдържа в раздел 5.1

трябва да бъде представен на Комисията до 9 ноември 2018 г. и на всеки две години след това[30].

Стъпка 4 — **Зависи ли услугата от мрежа и информационна система?**

Освен това следва да се поясни дали тази услуга отговаря на втория критерий по член 5, параграф 2, буква б), и по-специално дали предоставянето на основна услуга зависи от мрежата и информационните системи съгласно определението в член 4, параграф 1.

Стъпка 5 — **Би ли имал инцидентът значително увреждащо въздействие?**

Съгласно член 5, параграф 2, буква в) националният орган има задължението да оценява дали един инцидент би имал значително увреждащо въздействие върху предоставянето на услугата. В този контекст в член 6, параграф 1 са изложени няколко междусекторни фактора, които трябва да бъдат отчетени при извършването на оценката. Освен това в член 6, параграф 2 е предвидено, че държавите членки вземат предвид и характерните за сектора фактори, когато е целесъобразно.

Изброените в член 6, параграф 1 **междусекторни фактори** са следните:

- Броят на ползвателите, разчитащи на услугите, предоставяни от субекта;
- Зависимостта на други сектори, посочени в приложение II, от услугата, предоставяна от субекта;
- Въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или обществената безопасност;
- Пазарният дял на субекта;
- Географският обхват, що се отнася до областта, която би била засегната от даден инцидент;
- Значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга.

Във връзка с **характерните за сектора фактори** в съображение 28 са дадени няколко примера (вж. таблица 4), които биха могли да предоставят полезни насоки за националните органи.

Таблица 4: Примери за характерни за сектора фактори, които трябва да се вземат под внимание при определяне на значителното увреждащо въздействие в случай на инцидент.

Сектор	Примери за характерни за сектора фактори
Доставчици на енергия	обем или дял на произведената енергия в национален

[30] Вж. член 5, параграф 7, буква б)

	план
Доставчици на нефт	дневен обем на доставения нефт
Въздушен транспорт (включително летища и въздушни превозвачи) **Железопътен транспорт** **Морски пристанища**	дял от националния обем на трафика; брой на пътниците или товарните операции за година.
Банкови инфраструктури или инфраструктури на финансовите пазари	системно значение въз основа на общите активи; съотношение на общите активи и БВП
Сектор на здравеопазването	брой пациенти, обслужени от доставчика на здравни услуги за година
Добив, обработка и доставка на вода	обем и брой на ползвателите, за които е доставена водата, и техният вид (включително например болници, учреждения за обществени услуги, организации или физически лица); наличието на алтернативни източници на вода, които да покриват същата географска територия

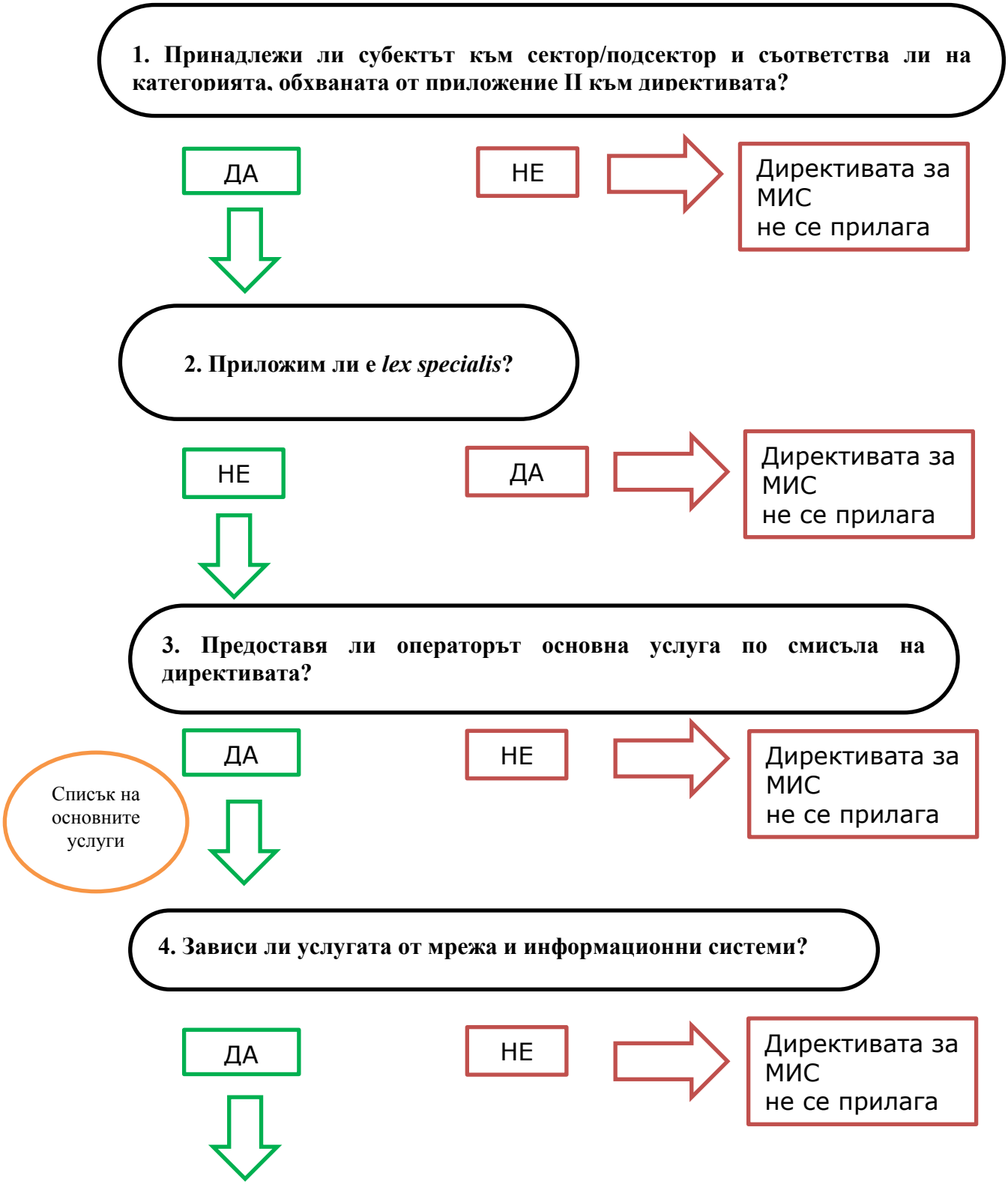
Следва да се отбележи, че при извършване на оценката съгласно член 5, параграф 2 държавите членки не следва да добавят допълнителни критерии към посочените в тази разпоредба, понеже това би ограничило броя на определените ООУ и би застрашило минималната хармонизация за ООУ, заложена в член 3 от директивата.

Стъпка 6 **— Въпросният оператор предоставя ли основни услуги в други държави членки?**

Стъпка 6 се отнася до случаите, в които операторът предоставя своите основни услуги в две или повече държави членки. Съгласно член 5, параграф 4, преди завършване на процеса на определяне въпросните държави членки трябва да проведат процес на консултации[31].

[31] За повече информация относно процеса на консултации вж. раздел 4.1.7.

Фигура 4: Процес на определяне в 6 стъпки.



5. Би ли имал инцидентът значително увреждащо въздействие?

Междусекторни фактори (член 6, параграф 1)

- **Брой ползватели**, разчитащи на услугите
- **Зависимост** на други основни сектори от услугата
- Възможно въздействие на инцидентите върху **икономиката и обществените дейности** или **обществената безопасност**
- Възможен **географски обхват**
- Значение на субекта за поддържането на достатъчно **ниво на услугата**

Характерни за сектора фактори (примери, посочени в съображение 28)

- **Енергетика**: обем или дял на произведената енергия в национален план
- **Транспорт**: дял от националния трафик, обем и брой операции на година
- **Здравеопазване**: брой пациенти, обслужени от доставчика на здравни услуги за година

ДА

НЕ → Директивата за МИС не се прилага

6. Въпросният оператор предоставя ли основни услуги в други държави членки?

ДА

НЕ → Директивата за МИС не се прилага

Задължителна консултация с въпросните държави членки

Приемане на национални мерки (напр. списък с оператори на основни услуги, политически и правни мерки).

4.1.7. Процес на трансгранична консултация.

Когато оператор предоставя основни услуги в две или повече държави членки, съгласно член 5, параграф 4 тези държави членки трябва да се консултират помежду си, преди да завършат процеса на определяне. Целта на тази консултация е да се улесни оценката на влиянието на оператора от гледна точка на трансгранично влияние.

Желаният резултат от консултацията е, че въпросните национални органи обменят аргументи и позиции и в идеалния случай достигат до един и същ резултат относно определянето на въпросния оператор. Директивата за МИС не изключва възможността държавите членки да достигнат до различни заключения относно това дали даден субект се определя като ООУ, или не. В съображение 24 се посочва възможността държавите членки да се обърнат за съдействие към групата за сътрудничество по този въпрос.

По мнение на Комисията държавите членки следва да се стремят да постигат консенсус по тези въпроси, за да се избегне ситуация, при която едно и също предприятие е с различен правен статут в различните държави членки. Отклоненията следва да бъдат само по изключение, напр. когато субект, определен като ООУ в една държава членка, има незначителна дейност в друга.

4.2. Изисквания за сигурност.

Съгласно член 14, параграф 1, държавите членки имат задължението да гарантират, че ООУ, като вземат предвид достиженията на техническия прогрес, предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тези доставчици при предоставянето на своите услуги. Съгласно член 14, параграф 2, подходящите мерки възпрепятстват и свеждат до минимум въздействието на инцидента.

В момента групата за сътрудничество провежда специализиран работен процес по изготвяне на необвързващи насоки относно мерките за сигурност за ООУ[32]. Групата ще финализира документа с насоки до четвъртото тримесечие на 2017 г. Комисията насърчава държавите членки да следят отблизо документа с насоки, който групата за сътрудничество ще разработи, за да се гарантира привеждането в съответствие във възможно най-голяма степен на националните разпоредби относно изискванията за сигурност. Хармонизацията на тези изисквания би улеснила съществено спазването на изискванията от ООУ, които често предоставят основни услуги в повече от една държава членка, и надзорните функции на националните компетентни органи и CSIRT.

[32] За целите на този работен процес списъците с международни стандарти, добри практики и методологии за оценка/управление на риска за всички сектори, обхванати от директивата за МИС, са разпространени и използвани за информация за предложените домейни за сигурност и мерки за сигурност

4.3 Изисквания за уведомяване.

Съгласно член 14, параграф 3 държавите членки трябва да гарантират, че ООУ уведомяват за „*инцидентите, които имат значително въздействие върху непрекъснатостта на предоставяните от тях основни услуги*“. Следователно ООУ не следва да уведомяват за незначителни инциденти, а само за сериозни инциденти, които засягат непрекъснатостта на основната услуга. Съгласно член 4, параграф 7 инцидент се определя като *„събитие, което има реално неблагоприятно въздействие върху сигурността на мрежите и информационните системи“*. Понятието „сигурност на мрежите и информационните системи“ е допълнително определено в член 4, параграф 2 като *„способността на мрежите да издържат — при дадено равнище на увереност — на действия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.“* Следователно всяко събитие, което има неблагоприятно въздействие не само върху наличието, но и върху истинността, целостта и поверителността на данните или свързаните услуги, потенциално би могло да породи задължение за уведомяване. Всъщност непрекъснатостта на услугата, посочена в член 14, параграф 3, може да бъде накърнена не само в случаите, свързани с физическата наличност, но и от друг свързан със сигурността инцидент, който засяга правилното предоставяне на услугата[33].

Специално работно направление в групата за сътрудничество понастоящем подготвя необвързващи насоки относно обстоятелствата, при които от операторите на основни услуги се изисква да уведомяват за инциденти по член 14, параграф 7, и относно формата и процедурата за такива национални уведомления. Предвижда се насоките да бъдат завършени до четвъртото тримесечие на 2017 г.

Различните национални изисквания за уведомяване могат да доведат до правна несигурност, по-сложни и тромави процедури и значителни административни разходи за доставчиците на услуги, извършващи трансгранична дейност. Поради това Комисията приветства работата на групата за сътрудничество. Както и в случая на изискванията за сигурност, Комисията насърчава държавите членки да следят отблизо документа с насоки, който групата за сътрудничество ще разработи, за да се гарантира привеждането в съответствие във възможно най-голяма степен на националните разпоредби относно уведомяването за инциденти.

4.4. Директива за МИС, приложение III: Доставчици на цифрови услуги.

Доставчиците на цифрови услуги (ДЦУ) са втората категория субекти, включени в приложното поле на директивата за МИС. Тези субекти се считат за важни икономически участници поради факта, че се използват от много фирми за

[33] Същото се отнася и до ДЦУ.

предоставяне на собствените им услуги, така че прекъсването на цифрова услуга би оказало въздействие върху ключовите икономически и обществени дейности.

4.4.1. Категории ДЦУ.

В член 4, параграф 5, който съдържа определение за цифрова услуга, е направено позоваване на правното определение в член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 чрез стесняване на обхвата до категориите услуги, посочени в приложение III. По-специално в член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 тези услуги са определени като „*каквато и да е услуга на информационното общество, тоест, каквато и да е услуга, нормално предоставяна срещу възнаграждение, от разстояние, чрез електронно средство и по индивидуална молба на получателя на услугите*“, а в приложение III към директивата са изброени три специфични категории услуги: онлайн място за търговия, онлайн търсачка и компютърни услуги „в облак“. За разлика от операторите на основни услуги, директивата не задължава държавите членки да определят доставчиците на цифрови услуги, които в такъв случай биха били предмет на съответните задължения. Следователно съответните задължения съгласно директивата, а именно изискванията за сигурност и уведомяване, изложени в член 16, ще бъдат приложими към всички ДЦУ, попадащи в нейния обхват.

Следните раздели съдържат допълнителни обяснения относно трите вида цифрови услуги, включени в приложното поле на директивата.

1. Доставчик на онлайн място за търговия.

Онлайн мястото за търговия дава възможност на голям брой и разнообразие от фирми да изпълняват своите търговски дейности по отношение на потребителите и да осъществяват междуфирмени отношения. То осигурява на предприятията основната инфраструктура за търгуване онлайн и презгранична търговия. Доставчиците на онлайн мястото за търговия изпълняват съществена роля в икономиката, по-специално чрез предоставяне на достъп на МСП до по-широкия цифров единен пазар на ЕС. Предоставянето на отдалечени изчислителни услуги, които улесняват икономическата дейност на клиента, включително обработването на трансакции и агрегирането на информация относно купувачи, доставчици и продукти, също може да принадлежи към дейностите на доставчик на онлайн място за търговия, както и улесняването на търсенето на подходящи продукти, предоставянето на продукти, експертни знания относно сключването на сделки и свързването на купувачи с продавачи.

Понятието „онлайн място за търговия“ е определено в член 4, параграф 17 и допълнително пояснено в съображение 15. Описан е като услуга, позволяваща на потребители и търговци да сключват онлайн договори за продажба или услуги с търговци, и представлява крайното място за сключването на тези договори. Например доставчик като *E-bay* може да се счита за онлайн място за търговия, понеже дава възможност на други страни да създават магазини в неговата платформа, за да предоставят своите продукти или услуги онлайн на потребителите или фирмите. Счита

се, че онлайн магазините за разпространение на приложения и софтуер попадат в определението за онлайн място за търговия, понеже позволяват на разработчиците на приложения да продават или разпространяват своите услуги до потребители или други фирми. За разлика от това посредниците на услуги на трети страни, като например *Skyscanner*, и услугите за сравняване на цените, които препращат потребителя към уебсайта на търговеца, където се включва реалният договор за услугата или продукта, не са обхванати от определението в член 4, параграф 17.

2. Доставчик на онлайн търсачка.
Понятието „онлайн търсачка“ е определено в член 4, параграф 18 и допълнително пояснено в съображение 16. То е описано като цифрова услуга, която позволява на потребителите да извършват търсения по принцип във всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякаква тема. Не са обхванати набори от функции за търсене, които се ограничават до търсене в сайта, и уебсайтове за сравнение на цени. Например търсачка от типа на предоставената от EUR LEX[34] не може да се счита за търсачка по смисъла на директивата, понеже нейната функция за търсене е ограничена до съдържанието на този конкретен уебсайт.

3. Доставчик на компютърни услуги „в облак“.
В член 4, параграф 19 компютърната услуга в облак е определена като „цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно“, а съображение 17 съдържа допълнителни пояснения на понятията „изчислителни ресурси“, „променлив по мащаб и еластичен набор от компютърни ресурси“.

Накратко, компютърните услуги в облак могат да се опишат като конкретен вид компютърна услуга, използваща споделени ресурси за обработване на данни при поискване, и при която споделените ресурси се отнасят до всякакъв вид хардуерни или софтуерни компоненти (напр. мрежи, сървъри или друга инфраструктура, средства за съхранение, приложения и услуги), които се предоставят на потребителите при поискване за целите на обработването на данни. Изразът „които могат да бъдат ползвани съвместно“ определя компютърни услуги, при които много потребители използват една и съща инфраструктура за обработване на данни. Компютърният ресурс може да се определи като позволяващ съвместно ползване, ако наборът ресурси, използван от доставчика, може да бъде разширен или намален по всяко време в зависимост от изискванията на потребителя. По този начин би било възможно да се добавят или премахват центрове за данни или отделни компоненти в рамките на един център за данни, ако общият компютърен капацитет или капацитет за съхранение е необходимо да бъде актуализиран. Понятието „еластичен набор“ може да бъде описано като промени в работното натоварване чрез автоматично осигуряване и отнемане на

[34] Достъпно на адрес: http://eur-lex.europa.eu/homepage.html?locale=bg

ресурси, така че във всеки един момент наличните ресурси да отговарят на текущото търсене във възможно най-голяма степен[35].

Понастоящем има три вида модели на компютърни услуги „в облак“, които доставчикът може да предложи:

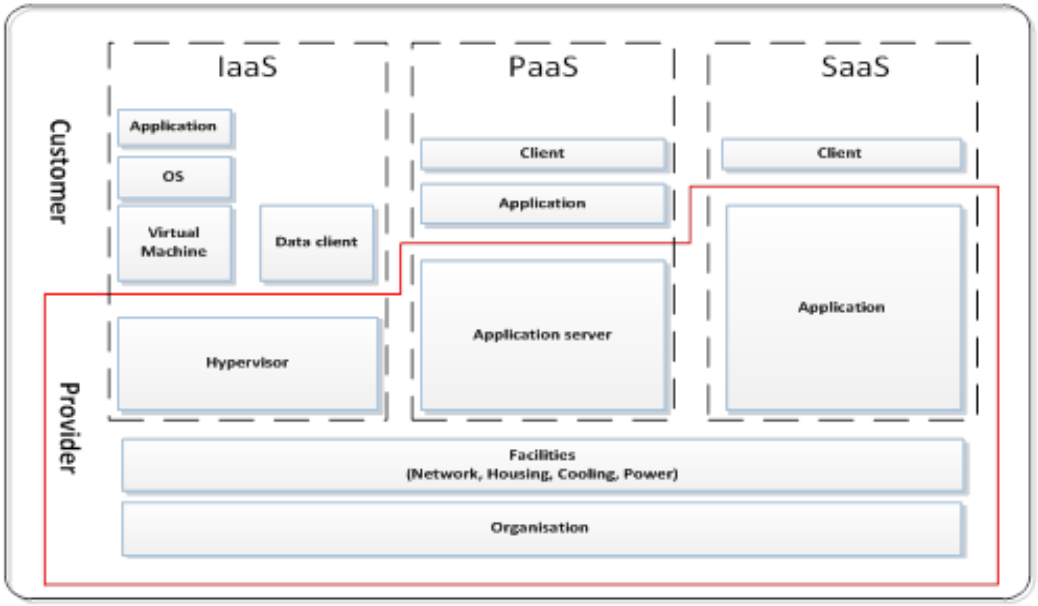
- Инфраструктура като услуга (IaaS): Категория на изчислителна услуга „в облак“, в която предоставяните на потребителя възможности „в облак“ са под формата на инфраструктура. Това включва виртуалното предоставяне на компютърни ресурси под формата на хардуер, услуги по изграждане на мрежи и съхранение. IaaS предоставя сървъри, средства за съхранение, мрежи и операционни системи. Тя предоставя инфраструктура на предприятие, в която предприятието може да съхранява своите данни и да управлява приложенията, необходими за ежедневното му функциониране.

- Платформа като услуга (PaaS): Категория на изчислителна услуга „в облак“, в която предоставяните на потребителя възможности „в облак“ са под формата на платформа. Тя включва онлайн компютърни платформи, които дават възможност на предприятията да използват съществуващи приложения или да разработват и тестват нови.

- Софтуер като услуга (SaaS): Категория на изчислителна услуга „в облак“, в която предоставяните на потребителя възможности „в облак“ са под формата на приложение или софтуер, разгърнат в интернет. При този вид услуги „в облак“ за крайния потребител не е необходимо да купува, инсталира и управлява софтуер и той има предимството, че софтуерът е достъпен отвсякъде с интернет връзка.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Технологичен институт, Карлсруе, “Elasticity in Cloud Computing: What It Is, and What It Is Not” („Еластичност на компютърните услуги в облак: какво е и какво не е тя“), достъпен на адрес: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Вж. също страници 2—5 от COM(2012) 529.

Фигура 5: Модели на услуги и активи в компютърните услуги „в облак“



Подробни насоки по конкретни теми в областта на изчисленията „в облак“[36] и ръководство относно основите на изчисленията „в облак“[37] са предоставени от ENISA.

4.4.2. Изисквания за сигурност.

Съгласно член 16, параграф 1, държавите членки имат задължението да гарантират, че ДЦУ предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тези предприятия при предоставянето на своите услуги. Тези мерки за сигурност следва да вземат предвид актуалното състояние на технологиите и следните пет елемента: i) сигурност на системите и съоръженията; ii) действия при инциденти; iii) управление на непрекъснатостта на дейностите; iv) наблюдение, одит и изпитване; v) спазване на международни стандарти.

В тази връзка Комисията е оправомощена съгласно член 16, параграф 8 да приема актове за изпълнение, в които тези елементи са пояснени допълнително, и в които се гарантира високо равнище на хармонизация за тези доставчици на услуги. Очаква се актовете за изпълнение да бъдат приети от Комисията през есента на 2017 г. Освен това от държавите членки се изисква да гарантират, че доставчиците на цифрови услуги предприемат необходимите мерки за предотвратяване и свеждане до минимум на въздействието на инцидентите с оглед на гарантиране на непрекъснатостта на техните услуги.

[36] Достъпно на адрес: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs (Ръководство по киберсигурност за МСП)* (2015 г.). Достъпно на адрес: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

4.4.3. Изисквания за уведомяване.

ДЦУ следва да са задължени да уведомяват компетентните органи или CSIRT за сериозни инциденти. Съгласно член 16, параграф 3 от директивата за МИС изискването към доставчиците на цифрови услуги за уведомяване се поражда в случаи, когато свързаният със сигурността инцидент има съществено въздействие върху предоставянето на услугата. За определяне на въздействието в член 16, параграф 4 са изброени по-специално пет параметъра, които доставчиците на цифрови услуги трябва да отчетат. В тази връзка Комисията е оправомощена съгласно член 16, параграф 8 да приема актове за изпълнение, които да включват по-подробни описания на параметрите. Допълнителното конкретизиране на тези параметри ще бъде част от акта за изпълнение, определящ елементите за сигурност съгласно точка 4.4.2, които Комисията смята да приеме през есента.

4.4.4. Основан на риска регулаторен подход.

В член 17 е предвидено, че ДЦУ са предмет на последващ надзорен контрол от страна на националните компетентни органи. Държавите членки трябва да гарантират, че компетентните органи предприемат действия, когато получат доказателства за това, че даден ДЦУ не спазва изискванията по член 16 от директивата.

Освен това, съгласно член 16, параграфи 8 и 9 Комисията е оправомощена да приема актове за изпълнение във връзка с изискванията за уведомяване и сигурност, което ще повиши равнището на хармонизация за ДЦУ. В допълнение, съгласно член 16, параграф 10 държавите членки не може да налагат на ДЦУ никакви други изисквания за сигурност или уведомяване, освен предвидените в директивата, с изключение на случаите, в които такива мерки са необходими за защита на техните основни държавнически функции, по-специално за защита на националната сигурност, както и за да се даде възможност за разследване, разкриване и наказателно преследване на престъпления.

И накрая, като отчита трансграничния характер на ДЦУ, директивата не следва модела на множество успоредни юрисдикции, а подход, основан на критерия за основното място на установяване на предприятието в рамките на ЕС.[38] Този подход дава възможност за прилагане на единен набор от правила спрямо ДЦУ, при което има един компетентен орган, отговарящ за надзора и това е от особено голямо значение, понеже много ДЦУ предлагат своите услуги в много държави членки едновременно. С прилагането на този подход се свежда до минимум тежестта, свързана със спазване на изискванията от ДЦУ и се гарантира правилното функциониране на цифровия единен пазар.

4.4.5. Юрисдикция.

Както е посочено по-горе, съгласно член 18, параграф 1 от директивата за МИС, държавата членка, където е основното място на установяване на ДЦУ, има юрисдикция над предприятието. В случаите, в които конкретен ДЦУ предлага услуги в ЕС, но не е

[38] Вж. по-специално член 18 от директивата.

установен на територията на ЕС, член 18, параграф 2 налага на ДЦУ задължението за определяне на представител в Съюза. В този случай държавата членка, в която е установен представителят, има юрисдикция над предприятието. В случаите, когато ДЦУ предоставя услуги в държава членка, но не е определил представител в ЕС, държавата членка по принцип може да предприеме действия срещу ДЦУ, понеже доставчикът нарушава своите задължения, произлизащи от директивата.

4.4.6. Освобождаване на доставчици на цифрови услуги в ограничен мащаб от изискванията за сигурност и уведомяване.

Съгласно член 16, параграф 11 доставчиците на цифрови услуги, които са микро- и малки предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията[39], са изключени от обхвата на изискванията за сигурност и уведомяване, изложени в член 16. Това означава, че тези фирми, в които са назначени по-малко от 50 лица и които имат годишен оборот и/или годишен счетоводен баланс, не по-голям от 10 милиона евро, не са обвързани с тези изисквания. При определяне на размера на субекта не е от значение дали въпросното предприятие предоставя само цифрови услуги по смисъла на директивата за МИС или и други услуги.

5. Връзката между директивата за МИС и друго законодателство.

Този раздел акцентира върху разпоредбите относно *lex specialis*, заложени в член 1, параграф 7 от директивата за МИС, и дава три примера за оценените досега от Комисията *lex specialis*, като пояснява изискванията за сигурност и уведомяване, прилагани към доставчиците на телекомуникационни и удостоверителни услуги.

5.1. Директива за МИС, член 1, параграф 7: Разпоредбата относно *lex specialis.*

Съгласно член 1, параграф 7 от директивата за МИС разпоредбите относно изискванията за сигурност и/или уведомяване за доставчиците на цифрови услуги или операторите на основни услуги съгласно директивата не са приложими, ако в специфично за сектора законодателство на ЕС са предвидени изисквания за сигурност и/или уведомяване, които са най-малкото равностойни на съответните задължения, съдържащи се в директивата за МИС. Държавите членки трябва да вземат под внимание член 1, параграф 7 в цялостното транспониране на директивата и да предоставят информация на Комисията за прилагането на разпоредбите относно *lex specialis*.

Методология.

При оценяване на еквивалентността на специфичен за сектора законодателен акт на ЕС със съответните разпоредби на директивата за МИС следва да се отдаде особено голямо значение на въпроса дали задълженията за сигурност в специфичното за сектора законодателство обхващат мерки, които гарантират сигурността на мрежите и

[39] ОВ L 24, 20.5.2003 г., стр. 36

информационните системи съгласно определението в член 4, параграф 2 от директивата.

Що се отнася до изискванията за уведомяване, в член 14, параграф 3 и член 16, параграф 3 от директивата за МИС е предвидено, че операторите на основни услуги и доставчиците на цифрови услуги трябва да уведомяват без неоправдано забавяне компетентния орган или CSIRT относно всеки инцидент, който има значително/съществено въздействие върху непрекъснатостта на предоставяните от тях основни услуги. Тук е необходимо да се обърне специално внимание на задълженията на оператора/доставчика на цифрови услуги да включва в уведомлението информация, с помощта на която компетентният орган или CSIRT може да определи трансграничното въздействие на свързан със сигурността инцидент.

Понастоящем няма специфично за сектора законодателство за категорията на доставчиците на цифрови услуги, което да предвижда изисквания за сигурност и уведомяване, сравними с изложените в член 16 от директивата за МИС, които могат да бъдат взети под внимание при прилагането на член 1, параграф 7 от директивата за МИС[40].

Що се отнася до операторите на основни услуги, финансовият сектор, и по-специално секторът на банковите услуги и секторът на инфраструктурите на финансовите пазари, посочени в точки 3 и 4 от приложение II понастоящем са предмет на изисквания за сигурност и/или уведомяване, произтичащи от специфично за сектора законодателство на ЕС. Това се дължи на факта, че сигурността и стабилността на ИТ и мрежите и информационните системи, използвани от финансовите институции, са основна част от изискванията за операционен риск, налагани на финансовите институции по силата на законодателството на ЕС.

Примери.

i) Директива за платежните услуги 2.

Във връзка с банковия сектор, и по-специално що се отнася до предоставянето на разплащателни услуги от кредитните институции, определени в член 4, точка 1 от Регламент (ЕС) 575/2013, в така наречената Директива за платежните услуги 2 (ДПУ 2)[41] са предвидени изисквания за сигурност и уведомяване, изложени в членове 95 и 96 от тази директива.

По-конкретно съгласно член 95, параграф 1 от доставчиците на платежни услуги се изисква да приемат подходящи мерки за смекчаване и механизми за контрол, които позволяват управлението на оперативните рискове, включително рисковете, свързани със сигурността, във връзка с предоставяните от тях платежни услуги. Тези мерки

[40] Това не накърнява уведомяването на надзорния орган за нарушение на сигурността на личните данни, включено в член 33 от Общия регламент относно защитата на данните.
[41] Директива (ЕС) 2015/2366, ОВ L 337, 23.12.2015 г., стр. 35

следва да съдържат установяването и поддържането на ефективни процедури за управление на инциденти, включително процедури за откриване и класифициране на значимите операционни инциденти и инциденти, свързани със сигурността. В съображения 95 и 96 от ДПУ 2 допълнително е изяснено естеството на тези мерки за сигурност. От тези разпоредби е очевидно, че предвидените мерки имат за цел управление на рисковете, свързани със сигурността, във връзка с мрежите и информационните системи, използвани при предоставяне на платежните услуги. Следователно тези изисквания за сигурност могат да се считат като най-малкото равностойни на съответната разпоредба в член 14, параграфи 1 и 2 от директивата за МИС.

Що се отнася до изискванията за уведомяване, в член 96, параграф 1 от ДПУ 2 е предвидено задължение за доставчиците на платежни услуги да уведомяват без неоснователно забавяне компетентния орган за значими свързани със сигурността инциденти. Освен това, подобно на член 14, параграф 5 от директивата за МИС, в член 96, параграф 2 от ДПУ 2 се съдържа изискването компетентният орган да уведомява органите на други държави членки, ако даден инцидент е от значение за тях. Това задължение същевременно предполага, че докладването за свързани със сигурността инциденти трябва да включва информация, която да позволява на органите да оценяват трансграничното въздействие на инцидента. В тази връзка Европейският банков орган (ЕБО) е оправомощен по член 96, параграф 3, буква а) от ДПУ 2 да разработи в сътрудничество с Европейската централна банка (ЕЦБ) насоки относно точното съдържание и формат на уведомлението.

Следователно може да се заключи, че съгласно член 1, параграф 7 от директивата за МИС, що се отнася до предоставянето на платежни услуги от кредитни институции, следва да се прилагат както изискванията за сигурност, така и изискванията за уведомяване, изложени в член 95 и 96 от ДПУ 2, вместо съответстващите разпоредби на член 14 от директивата за МИС.

ii) Регламент (ЕС) 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на трансакции.

Във връзка с инфраструктурата на финансовия пазар Регламент (ЕС) 648/2012 във връзка с Делегиран регламент (ЕС) 153/2013 на Комисията съдържа разпоредби относно изискванията за сигурност за централните контрагенти (ЦК), които може да се считат за *lex specialis.* По-специално правните актове предвиждат технически и организационни мерки, свързани със сигурността на мрежовите и информационните системи, които са дори по-подробни от изискванията на член 14, параграфи 1 и 2 от директивата за МИС и следователно може да се счита, че отговарят на изискванията на член 1, параграф 7 от директивата за МИС по отношение на изискванията за сигурност.

По-конкретно член 26, параграф 1 от Регламент (ЕС) 648/2012 гласи, че субектът следва да разполага с *„надеждни правила за управление, включващи ясна организационна структура с добре определена, прозрачна и последователна йерархия*

на отговорностите, ефективни процеси за определяне, управление, наблюдение и отчитане на рисковете, на които ЦК е изложен или може да бъде изложен, и адекватни механизми за вътрешен контрол, в т.ч. надеждни административни и счетоводни процедури.“ Член 26, параграф 3 съдържа изискването организационната структура да гарантира непрекъснатост и нормално функциониране на услугите и дейностите посредством подходящи и пропорционални системи, средства и процедури.

Освен това в член 26, параграф 6 се пояснява, че за да осигури *„високи стандарти за сигурност, както и надеждност и поверителност на съхраняваната информация, ЦК поддържа системи за информационни технологии, съответстващи на сложността, разнообразието и вида на осъществяваните услуги и дейности“*. Освен това член 34, параграф 1 налага установяването, прилагането и поддържането на адекватна политика за непрекъснатост на стопанската дейност и план за възстановяване при „катастрофично събитие“, за да се осигури своевременно възстановяване на дейността.

Тези задължения са описани по-подробно в Делегиран регламент ЕС/153/2013 на Комисията от 19 декември 2012 г. за допълване на Регламент ЕС/648/2012 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти относно изискванията към централните контрагенти[42]. По-специално с член 4 от него на ЦК се налага задължението да разработват подходящи инструменти за управление на риска, които биха позволили управляването и докладването за всички свързани рискове, и да конкретизират допълнително вида мерки (напр. използване на надеждни информационни системи и системи за контрол на риска, наличието на ресурси, експертни знания и достъп до цялата съответна информация за звеното за управление на риска, наличие на адекватни механизми за вътрешен контрол, като например строги административни и счетоводни процедури в помощ на съвета на ЦК при наблюдението и оценяването на адекватността и ефективността на неговите политики, процедури и системи за управление на риска).

В допълнение към това в член 9 изрично се посочва сигурността на системите за информационни технологии и се налагат конкретни технически и организационни мерки, свързани с поддържането на надеждна рамка за информационна сигурност за управлението на рисковете за ИТ сигурността. Тези мерки следва да включват механизми и процедури, които гарантират наличността на услугите и защитата на истинността, целостта и поверителността на данните.

iii) Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС[43].

Във връзка с местата на търговия член 48, параграф 1 от Директива 2014/65/ЕС съдържа изискването операторите да гарантират непрекъснато предоставяне на

[42] ОВ L 52, 23.2.2013 г., стр. 41
[43] ОВ L 173, 12.6.2014 г., стр. 349

услугите на регулирания пазар при нестабилност на системите му за търговия. Това общо задължение неотдавна беше допълнително конкретизирано и допълнено от Делегиран регламент (ЕС) 2017/584 на Комисията[44] от 14 юли 2016 г. за допълване на Директива 2014/65/ЕС на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти, с които се уточняват организационните изисквания към местата на търговия[45]. По-специално член 23, параграф 1 от регламента предвижда, че местата на търговия разполагат с процедури и правила за физическа и електронна сигурност, разработени за защита на техните системи от злоупотреба или непозволен достъп и за гарантиране на целостта на данните. Тези мерки следва да позволяват свеждане до минимум на рисковете от атаки срещу информационните системи.

Член 23, параграф 2 съдържа допълнителното изискване поетите от операторите мерки и правила да позволяват бързо установяване и управляване на риска, свързан с непозволен достъп, намеса в системата, която силно затруднява или прекъсва функционирането на информационна система и намеса в данните, която накърнява наличността, целостта или истинността на данните. Освен това с член 15 от регламента се налага задължението местата на търговия да разполагат с ефективни правила за непрекъснатост на дейността с цел гарантиране на стабилността на системата и преодоляване на сривове. По-специално тези мерки следва да позволяват на оператора да възобнови търговията в срок от два часа или около два часа, като същевременно обемът данни, които може да бъдат загубени, е близо до нула.

В член 16 се предвижда още, че определените мерки за отстраняване и управление на сривове следва да бъдат част от плана за непрекъснатост на дейността на местата на търговия, както и се предвиждат конкретни елементи, които операторите трябва да вземат под внимание при приемането на плана за непрекъснатост на дейността (напр. създаване на специален оперативен екип за сигурност, извършване на оценка на въздействието, която установява рисковете и периодично се преглежда).

С оглед на съдържанието на тези мерки изглежда, че предназначението им е да управляват и отстраняват рисковете, свързани с наличността, истинността, целостта и поверителността на данните или предоставяните услуги и в резултат на това може да се заключи, че горепосоченото специфично за сектора законодателство на ЕС съдържа задължения за сигурност, които имат най-малко равностоен ефект на този на съответните задължения по член 14, параграфи 1 и 2 от директивата за МИС.

5.2. Директива за МИС, член 1, параграф 3: Доставчици на телекомуникационни услуги и доставчици на удостоверителни услуги.

Съгласно член 1, параграф 3 изискванията за сигурност и уведомяване, предвидени в директивата не се прилагат за доставчиците на удостоверителни услуги, за които се прилагат изискванията по членове 13а и 13б от Директива 2002/21/ЕО. Членове 13а и

[44] ОВ L 87, 31.3.2017 г., стр. 350
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf

13б от Директива 2002/21/ЕО са приложими към предприятия, които предоставят обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги. Следователно, що се отнася до предоставянето на обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги, предприятието трябва да спазва изискванията за сигурност и уведомяване на Директива 2002/21/ЕО.

Ако същото предприятие обаче предоставя и други услуги, като например цифровите услуги (напр. компютърни услуги „в облак“ или онлайн място за търговия), посочени в приложение III към директивата за МИС, или услуги като DNS или ТОИ съгласно приложение II, точка 7 от директивата за МИС, дружеството е предмет на изискванията за сигурност и уведомяване на директивата за МИС за предоставянето на тези конкретни услуги. Следва да се отбележи, че поради факта, че доставчиците на услугите, посочени в приложение II, точка 7, спадат към категорията „оператор на основни услуги“, държавите членки са задължени да проведат процес на определяне съгласно член 5, параграф 2 и да определят кои отделни доставчици на DNS, ТОИ или TLD услуги следва да спазват изискванията на директивата за МИС. Това означава, че в следствие на такава оценка единствено доставчиците на DNS, ТОИ или TLD, които отговарят на критериите в член 5, параграф 2 от директивата за МИС, ще имат задължението да спазват изискванията на директивата за МИС.

В член 1, параграф 3 се посочва още, че изискванията за сигурност и уведомяване на директивата не са приложими към доставчици на удостоверителни услуги, които са предмет на подобни изисквания по член 19 от Регламент (ЕС) № 910/2014.

6. Публикувани национални документи за стратегии за киберсигурност.

	Държава членка	Заглавие на стратегията и налични връзки
1	Австрия	*Стратегия за киберсигурност на Австрия* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Белгия	*Обезопасяване на киберпространството* (2012 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	България	*Киберустойчива България 2020 г.* (2016 г.) http://www.cyberbg.eu/ (BG)
4	Хърватия	*Националната стратегия за киберсигурност на Република Хърватия* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Чешка република	*Национална стратегия за киберсигурност на Чешката република за периода от 2015 до 2020 г.* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Кипър	*Стратегия за киберсигурност на Република Кипър* (2012 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Дания	*Датската стратегия за кибер- и информационна сигурност* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Естония	*Стратегия за киберсигурност* (2014 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Финландия	*Стратегия за киберсигурност на Финландия* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Франция	*Национална стратегия за цифрова сигурност на Франция* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-

		strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Ирландия	*Национална стратегия за киберсигурност 2015—2017 г.* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Италия	*Национална стратегическа рамка за сигурност на киберсигурността* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Германия	*Стратегия за киберсигурност за Германия* (2016 г.) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Унгария	*Национална стратегия за киберсигурност на Унгария* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Латвия	*Стратегия за киберсигурност на Латвия 2014—2018 г.* (2014 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Литва	*Програмата за развитие на сигурността на електронната информация (киберсигурността) за 2011—2019 г.* (2011 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Люксембург	*Национална стратегия за киберсигурност II (2015 г.)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Малта	*Зелена книга на националната стратегия за киберсигурност* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Нидерландия	*Национална стратегия за киберсигурност 2* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Полша	*Политика за защита на киберпространството на Република Полша* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Румъния	*Стратегия за киберсигурност на Румъния* (2011 г.)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Португалия	*Национална стратегия за сигурност на киберпространството* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Словашка република	*Концепция за киберсигурност на Словашката република за 2015—2020 г.* (2015 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Словения	*Стратегия за киберсигурност за установяване на система за гарантиране на високо равнище на киберсигурност* (2016 г.) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Испания	*Национална стратегия за киберсигурност* (2013 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Швеция	*Националната стратегия за киберсигурност на Швеция* (2017 г.) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Обединеното кралство	*Национална стратегия за киберсигурност (2016—2021 г.)* (2016 г.) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Списък на добри практики и препоръки, изготвен от ENISA.

За реагиране на инциденти

- ✓ Стратегии за реагиране на инциденти и сътрудничество при кибернетични кризи[46]

За действия при инциденти

- ✓ Incident handling automation project (Проект за автоматизиране на действията при инциденти)[47]
- ✓ Good Practice Guide for Incident Management (Наръчник за добри практики в управлението на инциденти)[48]

За класификация и таксономия на инциденти

- ✓ Преглед на съществуващите таксономии[49]
- ✓ Наръчник за добри практики за използване на таксономии за предотвратяване и установяване на инциденти[50]

За ниво на развитие на CSIRT

- ✓ Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity (Предизвикателства пред националните CSIRT в Европа през 2016 г.: изследване на нивото на развитие на CSIRT)[51]
- ✓ Study on CSIRT Maturity – Evaluation Process (Изследване на нивото на развитие на CSIRT — процес на оценяване)[52]
- ✓ Guidelines for national and governmental CSIRTs on how to assess maturity (Насоки за национални и правителствени CSIRT за оценяване на нивото на развитие)[53]

За изграждане на капацитет и обучение на CSIRT

---

[46] ENISA, *Strategies for incident response and cyber crisis cooperation* (Стратегии за реакция при инциденти и сътрудничеството при кибернетични кризи) (2016 г.). Достъпни на:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[47] За повече информация: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

[48] ENISA, *Good Practice Guide for Incident Management* (Наръчник за добри практики в управлението на инциденти) (2010 г.). Достъпен на адреснttps://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[49] За повече информация: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies

[50] ENISA, *Наръчник за добри практики за използване на таксономии за предотвратяване и установяване на инциденти,* (2017 г.). Достъпен на адрес:https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection

[51] ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (Предизвикателства пред националните CSIRT в Европа през 2016 г.: изследване на нивото на развитие на CSIRT) (2017 г.). Достъпно на адрес:https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (Изследване на нивото на развитие на CSIRT — процес на оценяване) (2017 г.). Достъпно на адрес:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[53] ENISA, CSIRT Capabilities (Способности на CSIRT). *How to assess maturity? Guidelines for national and governmental CSIRTs* (Как се оценява нивото на развитие? Насоки за национални и правителствени CSIRT) (2016 г.). Достъпни на адрес: https://www.enisa.europa.eu/publications/csirt-capabilities

- ✓ Good Practice Guide on Training Methodologies (Наръчник за добри практики в методологиите за обучение)[54]

За информация относно съществуващите CSIRT в Европа ─ Преглед на CSIRT по държави[55]

[54] ENISA, *Good Practice Guide for Incident Management* (Наръчник за добри практики в методологиите за обучение) (2014 г.). Достъпен на адрес:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies

[55] За повече информация: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map