III

(Подготвителни актове)

ЕВРОПЕЙСКА ЦЕНТРАЛНА БАНКА

СТАНОВИЩЕ НА ЕВРОПЕЙСКАТА ЦЕНТРАЛНА БАНКА

от 4 юни 2021 година

относно предложение за регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор

(CON/2021/20)

(2021/C 343/01)

Въведение и правно основание

На 22, 23 и 29 декември 2020 г. Европейската централна банка (ЕЦБ) получи искания съответно от Съвета на Европейския съюз и от Европейския парламент за становище относно предложение за регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014 и (ЕС) № 909/2014 ([1]) (наричан по-долу „предложеният регламент“) и предложение за директива за изменение на директиви 2006/43/ЕО, 2009/65/ЕО, 2009/138/ЕО, 2011/61/ЕС, 2013/36/ЕС, 2014/65/ЕС, (ЕС) 2015/2366 и (ЕС) 2016/2341 ([2]) (наричана по-долу „предложената директива за изменение“, наричани по-долу заедно с предложения регламент „предложените актове“).

ЕЦБ е компетентна да даде становище на основание член 127, параграф 4 и член 282, параграф 5 от Договора за функционирането на Европейския съюз, тъй като предложените актове съдържат разпоредби, попадащи в областите на компетентност на ЕЦБ, по-специално определянето и осъществяването на паричната политика, насърчаването на нормалното функциониране на платежните системи, приноса за гладкото провеждане на следваните от компетентните органи политики, свързани със стабилността на системата на финансовите пазари, и задачите на ЕЦБ по отношение на пруденциалния надзор над кредитните институции съгласно член 127, параграф 2, първо и четвърто тире и член 127, параграфи 5 и 6 от Договора. Управителният съвет прие настоящото становище съгласно член 17.5, изречение първо от Процедурния правилник на Европейската централна банка.

1. **Общи забележки**

1.1 ЕЦБ приветства предложения регламент, който има за цел да повиши киберсигурността и оперативната устойчивост на финансовия сектор. По-специално ЕЦБ приветства целта на предложения регламент за премахване на пречките на вътрешния пазар на финансови услуги и подобряване на изграждането и функционирането му чрез хармонизиране на приложимите правила в областта на управлението на риска при информационните и комуникационните технологии (ИКТ), уведомяването, тестването и риска при ИКТ, пораждан от трета страна. Освен това ЕЦБ приветства целта на предложения регламент за оптимизиране и хармонизиране на припокриващите се регулаторни изисквания или надзорни очаквания, които понастоящем се прилагат за финансовите субекти съгласно правото на Съюза.

1.2 ЕЦБ разбира, че по отношение на финансовите субекти, определени като оператори на основни услуги ([3]), предложеният регламент представлява специален за сектора правен акт (lex specialis), по смисъла на член 1, параграф 7 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([4]) (наричана по-долу „Директивата за МИС“); това означава, че изискванията съгласно предложения регламент по принцип ще имат предимство пред Директивата за МИС. На практика финансовите субекти, определени като оператори на основни услуги ([5]), наред с другото, би следвало да уведомяват за инциденти в съответствие с предложения

([1]) COM(2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Вж. член 1, параграф 2 от предложения регламент.
([4]) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).
([5]) Вж. член 5 от Директивата за МИС.

регламент, а не с Директивата за МИС. Въпреки че ЕЦБ приветства намаляването на потенциалните припокриващи се изисквания за финансовите субекти в областта на уведомяването за инциденти, следва да се обърне допълнително внимание на взаимодействието между предложения регламент и Директивата за МИС. Например съгласно предложения регламент по отношение на доставчик трета страна на услуги в областта на ИКТ ([6]) могат да се прилагат препоръки, издадени от водещия надзорник ([7]). В същото време същият този доставчик може да бъде класифициран като оператор на основни услуги съгласно Директивата за МИС и спрямо него да се прилагат задължителните указания, издадени от компетентния орган ([8]). В този случай доставчикът би могъл да бъде адресат на противоречащи си препоръки, издадени съгласно предложения регламент, и на задължителни указания, издадени съгласно Директивата за МИС. ЕЦБ предлага на законодателните органи на Съюза да обмислят допълнително потенциалните несъответствия между предложения регламент и Директивата за МИС, които могат да възпрепятстват хармонизацията и намаляването на припокриващите се и противоречащите си изисквания за финансовите субекти.

1.3 ЕЦБ също така разбира, че съгласно предложението за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 ([9]) (наричана по-нататък „предложената директива за МИС2“) „ситуациите, близки до инциденти“ ([10]) ще бъдат предмет на задължения за уведомяване ([11]). Въпреки че съображение 39 от предложената директива за МИС2 се отнася до значението на термина „ситуации, близки до инциденти“, не е ясно дали намерението е да се изисква от финансовите субекти, изброени в член 2 от предложения регламент, да уведомяват за ситуации, близки до инциденти. Във връзка с това и като се има предвид, че ситуациите, близки до инциденти, могат да бъдат идентифицирани като такива само след тяхното възникване, ЕЦБ би приветствала своевременното получаване на уведомление за значими ситуации, близки до инциденти, какъвто понастоящем е случаят с киберинцидентите. ЕЦБ предлага да има по-добра координация между предложения регламент и предложената директива за МИС2, за да се изясни точният обхват на уведомяването, за което могат да бъдат задължени финансовите субекти съгласно тези два отделни, но свързани законодателни акта на Съюза. В същото време ще трябва да се определят „ситуациите, близки до инциденти“ и да се разработят разпоредби, които изясняват тяхната значимост.

1.4 ЕЦБ приветства стимулите за финансовите субекти да обменят помежду си на доброволна основа разузнавателни сведения за киберзаплахи, за да подобрят и укрепят киберустойчивостта си. Самата ЕЦБ помогна с обусловената от пазара Инициатива за обмен на информация и разузнавателни сведения за киберзаплахи (Cyber Information and Intelligence Sharing Initiative — CIISI-EU) и направи достъпни за всеки подробните планове за изграждане и насърчаване на такава инициатива ([12]).

1.5 ЕЦБ подкрепя сътрудничеството между компетентните органи за целите на предложения регламент, Европейските надзорни органи (ЕНО) и екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС) ([13]). От съществено значение е да се обменя информация, за да се гарантира оперативната устойчивост на Съюза, тъй като обменът на информация и сътрудничеството между органите могат да допринесат за предотвратяването на кибератаки и да спомогнат за намаляване на разпространението на заплахите, свързани с ИКТ. Следва да се насърчава общо разбиране за свързаните с ИКТ рискове и да се гарантира последователно оценяване на тези рискове в целия Съюз. От изключително значение е информацията да се обменя с единното звено за контакт ([14]) и националните ЕРИКС от компетентните органи ([15]) само когато са налице ясно установени механизми за класификация и обмен на информация, съчетани с подходящи гаранции за защита на поверителност.

1.6 И на последно място, ЕЦБ би приветствала въвеждането в предложения регламент на правила относно личните данни и съхранението на данни. Продължителността на срока на съхранение следва да взема предвид разследването, проверката, искането за информация, съобщаването, публикуването, оценката, удостоверяването, оценката и изготвянето на планове за контрол или надзор, които компетентните органи трябва да извършват като част от съответните си задължения и задачи съгласно предложения регламент. В това отношение би бил подходящ 15-годишен срок на съхранение на данни. Той може да бъде съкратен или

([6]) Вж. член 3, точка 15 от предложения регламент.
([7]) Вж. член 31, параграф 1, буква г) от предложения регламент.
([8]) Вж. член 15, параграф 3 от Директивата за МИС.
([9]) COM (2020) 823 final.
([10]) Събития, които потенциално са могли да причинят вреда, но тяхното пълно настъпване е било успешно предотвратено. Вж. съображение 39 от Директивата за МИС2.
([11]) Вж. член 11 от Директивата за МИС2.
([12]) Инициативата за обмен на разузнавателни сведения за киберзаплахи (CIISI-EU) е достъпна на уебсайта на ЕЦБ www.ecb.europa.eu.
([13]) Вж. член 42 от предложения регламент.
([14]) Вж. член 8, параграф 3 от Директивата за МИС.
([15]) Виж също членове 11, 26 и 27 от Директивата за МИС2.

удължен според изискванията на конкретните случаи. Във връзка с това ЕЦБ предлага при формулирането на съответната разпоредба относно личните данни и съхранението на данни законодателните органи на Съюза да вземат предвид и принципа за свеждане на данните до минимум, както и по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели ([16]).

2. **Специфични забележки относно надзора, клиринга и сетълмента на ценни книжа**

2.1 *Надзорни правомощия на ЕСЦБ и Евросистемата*

2.1.1 Тясно свързани с нейните основни задачи в областта на паричната политика, Договорът и Уставът на Европейската система на централните банки и на Европейската централна банка (наричан по-долу „Уставът на ЕСЦБ“) предвиждат осъществяването на надзор от страна на Евросистемата върху клиринговите и платежните системи. Съгласно член 127, параграф 2, четвърто тире от Договора, отразен в член 3.1 от Устава на ЕСЦБ, една от основните задачи, осъществявани чрез Европейската система на централните банки (ЕСЦБ), е да насърчава нормалното функциониране на платежните системи. При изпълнението на тази основна задача ЕЦБ и националните централни банки могат да осигурят улеснения, а ЕЦБ да приеме регламенти, гарантиращи ефикасни и стабилни клирингови и платежни системи в рамките на Съюза и с други страни ([17]). В съответствие с надзорната си функция ЕЦБ прие Регламент (ЕС) № 795/2014 на Европейската централна банка (ЕЦБ/2014/28) (наричан по-долу „Регламентът за СВПС“) ([18]). С Регламента за СВПС в предписателна форма се прилагат Принципите за инфраструктурите на финансовите пазари от април 2012 г., издадени от Комитета за платежни системи и системи за сетълмент и Международната организация на комисиите за ценни книжа ([19]), които са правно обвързващи и обхващат както платежни системи за големи плащания, така и системи за плащания на дребно от системно значение, управлявани от централна банка от Евросистемата или от частен субект. В Рамката на надзорната политика на Евросистемата ([20]) платежните инструменти са описани като „неразделна част от платежните системи“ и така се включват в обхвата на нейния надзор. Понастоящем надзорната рамка за платежни инструменти е в процес на преразглеждане ([21]). Съгласно тази рамка платежният инструмент (напр. карта, кредитен превод, директен дебит, превод на електронни пари и цифров токен за плащане ([22])) се определя като персонализирано устройство (или набор от устройства) и/или набор от процедури, договорени между ползвателя на платежни услуги и доставчика на платежни услуги, използван за иницииране на прехвърляне на стойност ([23]).

2.1.2 Предвид гореизложеното ЕЦБ приветства изключването от члена за приложното поле на предложения регламент на системните оператори съгласно определението в член 2, буква п) от Директива 98/26/ЕО на Европейския парламент и на Съвета ([24]), платежните системи (включително управляваните от централни банки), платежните

([16]) Вж. член 4, параграф 1, буква б) и член 13 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

([17]) Вж. член 22 от Устава на ЕСЦБ.

([18]) Регламент (ЕС) № 795/2014 на Европейската централна банка от 3 юли 2014 г. относно надзорните изисквания за системно важните платежни системи (ЕЦБ/2014/28) (ОВ L 217, 23.7.2014 г., стр. 16).

([19]) Достъпни на уебсайта на Банката за международни разплащания www.bis.org.

([20]) Рамка на надзорната политика на Евросистемата, преработена версия (юли 2016 г.), достъпна на уебсайта на ЕЦБ www.ecb.europa.eu.

([21]) Вж. преразгледаната и консолидирана Надзорна рамка на Евросистемата за електронни платежни инструменти, схеми и споразумения от октомври 2020 г. (рамка за PISA), достъпна на уебсайта на ЕЦБ www.ecb.europa.eu.

([22]) Цифров токен за плащане е цифрово представяне на стойност, обезпечена с вземания или активи, записани другаде, което дава възможност за прехвърляне на стойност между крайни потребители. В зависимост от базовия проект цифровите токени за плащания могат да предвиждат прехвърляне на стойност, без непременно да включват централна трета страна и/или да използват платежни сметки.

([23]) „Прехвърляне на стойност“: „Действието, инициирано от платеца или от негово име или от получателя, по прехвърляне на средства или цифрови токени за плащане, или внасяне или теглене на пари в брой по/от потребителска сметка, независимо от базисните задължения между платеца и получателя. Прехвърлянето може да включва един или повече доставчици на платежни услуги.“ Това определение на „прехвърляне на стойност“ съгласно рамката за PISA се различава от определянето на прехвърляне на „средства“ съгласно Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ОВ L 337, 23.12.2015 г., стр. 35). „Прехвърляне на стойност“ в контекста на „платежен инструмент“ съгласно определението в посочената директива може да се отнася само до прехвърляне на „средства“. Съгласно посочената директива „средства“ не включва цифрови токени за плащане, освен ако токените могат да бъдат класифицирани като електронни пари (или по-хипотетично като безналични пари).

([24]) Директива 98/26/ЕО на Европейския парламент и на Съвета от 19 май 1998 г. относно окончателността на сетълмента в платежните системи и в системите за сетълмент на ценни книжа (ОВ L 166, 11.6.1998 г., стр. 45).

схеми и платежните механизми предвид прилагането на посочените по-горе надзорни рамки. Поради тези причини компетенциите на ЕСЦБ съгласно Договора и компетенциите на Евросистемата съгласно Регламента за СВПС следва да бъдат ясно формулирани в съображенията на предложения регламент.

2.1.3 По същата причина ЕЦБ приветства изключването от прилагането на надзорната рамка, установена в предложения регламент, на доставчиците трети страни на услуги в областта на ИКТ, които са обхванати от надзорни рамки, създадени с оглед на задачите, посочени в член 127, параграф 2 от Договора ([25]). В това отношение ЕЦБ би искала да подчертае, че централните банки от ЕСЦБ, действащи в качеството си на органи на паричната политика ([26]), и Евросистемата, когато предоставят услуги чрез TARGET2, TARGET2-Securites (T2S) ([27]) и сетълмента на незабавни плащания в TARGET (TIPS) ([28]), не са включени в члена за приложното поле на предложения регламент, нито могат да се считат за трета страна — доставчик на услуги в областта на ИКТ, и по този начин потенциално да бъдат класифицирани като възлови доставчици трети страни на услуги в областта на ИКТ за целите на предложения регламент. Евросистемата упражнява надзор върху T2S във връзка с правомощията си да гарантира ефикасни и стабилни клирингови и платежни системи. Освен това ЕОЦКП поясни, че T2S не е възлов доставчик на услуги ([29]) по смисъла на Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета ([30]) (наричан по-долу „Регламентът за ЦДЦК“). В резултат на това организационната и оперативната безопасност, ефикасност и устойчивост на T2S се гарантират чрез приложимата правна, регулаторна и оперативна рамка и договорените правила за управление на T2S, а не чрез Регламента за ЦДЦК.

2.1.4 Освен това рамката на надзорната политика на Евросистемата ([31]) обхваща възловите доставчици на услуги като Обществото за световна междубанкова финансова телекомуникация (SWIFT). SWIFT е кооперативно дружество с ограничена отговорност, учредено в Белгия, което предоставя международни услуги по защитен пренос на съобщения. Nationale Bank van België/Banque Nationale de Belgique действа като водещ надзорник на SWIFT и въз основа на споразумение за съвместен надзор осъществява надзор над SWIFT в сътрудничество с другите централни банки от Г-10, включително ЕЦБ. Надзорните органи на Г-10 признават, че основният акцент на надзора е операционният риск на SWIFT, тъй като това се счита за основната рискова категория, чрез която SWIFT може да представлява системен риск за финансовата система в Съюза. Във връзка с това групата за съвместен надзор на SWIFT разработи специфичен набор от принципи и общи очаквания, които се прилагат за SWIFT, като например идентифициране и управление на риска, информационна сигурност, надеждност и устойчивост, технологично планиране и комуникация с потребителите. Надзорните органи на Г-10 очакват SWIFT да се придържа към Насоките за киберустойчивост на Комитета за плащания и пазарна инфраструктура (КППИ) и Международната организация на комисиите по ценни книжа (МОКЦК) ([32]), както и към други международни стандарти за сигурност на ИКТ, които, взети заедно, надхвърлят изискванията, определени в предложения регламент.

2.1.5 Не може да бъде сигурно, че SWIFT и евентуално други доставчици на услуги, спрямо които се прилага Рамката на надзорната политика на Евросистемата, могат да попаднат в приложното поле на предложения регламент като доставчици трети страни на услуги в областта на ИКТ, ако предоставят услуги, които не попадат в приложното поле на член 127, параграф 2 от Договора. Поради това ЕЦБ горещо приветства изключването на доставчиците на услуги, които вече са обхванати от Рамката на надзорната политика на Евросистемата, включително, но не само, SWIFT, от приложното поле на надзорната рамка, определена в предложения регламент.

([25]) Вж. член 28, параграф 5 от предложения регламент.

([26]) Вж. параграф 1.3 от Становище на Европейската централна банка от 19 февруари 2021 г. относно предложение за регламент относно пазарите на криптоактиви и за изменение на Директива (ЕС) 2019/1937 (CON/2021/4). Всички становища на ЕЦБ се публикуват в EUR-Lex.

([27]) Вж. приложение IIа към Насоки ЕЦБ/2012/27 на Европейската централна банка от 5 декември 2012 г. относно Трансевропейската автоматизирана система за брутен сетълмент на експресни преводи в реално време (TARGET2) (ОВ L 30, 30.1.2013 г., стр. 1). Насоки ЕЦБ/2012/13 на Европейската централна банка от 18 юли 2012 г. относно TARGET2-Securities (ОВ L 215, 11.8.2012 г., стр. 19); Решение ЕЦБ/2011/20 на Европейската централна банка от 16 ноември 2011 г. за определяне на подробни правила и процедури за прилагане на критериите за допустимост за централни депозитари за ценни книжа за достъп до услуги на TARGET2 — Securities (ОВ L 319, 2.12.2011 г., стр. 117). Вж. също Рамковото споразумение за T2S и Колективното споразумение.

([28]) Вж. приложение IIб към Насоки ЕЦБ/2012/27.

([29]) Вж. член 30, параграф 5 от Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. за подобряване на сетълмента на ценни книжа в Европейския съюз и за централните депозитари на ценни книжа, както и за изменение на директиви 98/26/ЕО и 2014/65/ЕС и Регламент (ЕС) № 236/2012 (ОВ L 257, 28.8.2014 г., стр. 1) и член 68 от Делегиран регламент (ЕС) 2017/392 от 11 ноември 2016 г. за допълване на Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти относно лицензирането, надзора и оперативните изисквания за централни депозитари на ценни книжа (ОВ L 65, 10.3.2017 г., стр. 48).

([30]) Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. за подобряване на сетълмента на ценни книжа в Европейския съюз и за централните депозитари на ценни книжа, както и за изменение на директиви 98/26/ЕО и 2014/65/ЕС и Регламент (ЕС) № 236/2012 (ОВ L 257, 28.8.2014 г., стр. 1).

([31]) Рамка на надзорната политика на Евросистемата, преработена версия (юли 2016 г.), достъпна на уебсайта на ЕЦБ www.ecb.europa.eu.

([32]) Достъпни на уебсайта на Банката за международни разплащания www.bis.org.

2.2 *Компетентност на ЕСЦБ в областта на сетълмента на ценни книжа*

2.2.1 Централните депозитари на ценни книжа (ЦДЦК) са инфраструктури на финансовите пазари (ИФП), които са строго регулирани и които са под надзора на различни органи съгласно Регламента за ЦДЦК, в който се определят изискванията за сетълмента на финансови инструменти, както и правилата за организацията и дейността на ЦДЦК. Освен това ЦДЦК трябва да вземат предвид Насоките за киберустойчивост на КППИ — МОКЦК, които се прилагат чрез Надзорните очаквания за киберустойчивост за инфраструктурите на финансовите пазари (декември 2018 г.) ([33]). В допълнение към надзорните правомощия, възложени на националните компетентни органи (НКО) съгласно Регламента за ЦДЦК, членовете на ЕСЦБ действат като „съответни органи“ в качеството си на органи, отговарящи за надзора над управлявани от ЦДЦК системи за сетълмент на ценни книжа, в качеството си на централни банки, емитиращи валутите, в които най-често се извършва сетълмент, и в качеството си на централни банки, в чиито сметки се извършва сетълмент на паричното рамо от сделките ([34]). Във връзка с това в съображение 8 от Регламента за ЦДЦК се посочва, че регламентът следва да се прилага, без да се засягат отговорностите на ЕЦБ и на националните централни банки по осигуряването на ефикасни и стабилни клирингови и платежни системи в рамките на Съюза и в трети държави. Освен това в съображение 8 се посочва, че регламентът за ЦДЦК не следва да възпрепятства достъпа на членовете на ЕСЦБ до информация, която е от значение за изпълнението на задълженията им ([35]), включително надзора върху ЦДЦК и други ИФП ([36]).

2.2.2 Освен това членовете на ЕСЦБ често действат като агенти по сетълмента за паричното рамо от сделките с ценни книжа и Евросистемата предлага услуги по сетълмент чрез T2S на ЦДЦК. Надзорът на Евросистемата върху T2S е свързан със задачата ѝ да осигури ефикасни и стабилни клирингови и платежни системи, докато компетентните и съответните органи на ЦДЦК имат за цел да гарантират безпрепятственото им функциониране, безопасността и ефикасността на сетълмента и правилното функциониране на финансовите пазари в съответните им юрисдикции.

2.2.3 Съгласно предложения регламент ([37]) централните банки от ЕСЦБ не участват в разработването на технически стандарти във връзка с определянето на рисковете при ИКТ. Аналогично, съгласно предложения регламент ([38]) съответните органи не са информирани за инцидентите с ИКТ. Централните банки от ЕСЦБ следва да запазят същото равнище на участие, както е предвидено понастоящем в Регламента за ЦДЦК, а съответните органи следва да бъдат уведомявани за инцидентите с ИКТ. Евросистемата е съответният орган за всички ЦДЦК от еврозоната и за няколко други ЦДЦК от ЕС. Централните банки от ЕСЦБ ще трябва да бъдат информирани за инцидентите с ИКТ, които са от значение за изпълнението на техните задължения, включително за надзора на ЦДЦК и други ИФП. Рисковете, на които са изложени ЦДЦК, включително рисковете при ИКТ, могат да застрашат доброто функциониране на ЦДЦК. Поради това рисковете при ИКТ са от значение за съответните органи, на които следва да се предостави пълен и подробен преглед на тези рискове, за да ги оценят и да повлияят на подхода на ЦДЦК към управлението на риска. Предложеният регламент не би трябвало да предвижда по-леки изисквания по отношение на рисковете при ИКТ от предвидените в Регламента за ЦДЦК и действащите регулаторни технически стандарти.

2.2.4 Освен това законодателните органи на Съюза следва да изяснят взаимодействието между предложения регламент ([39]) и регулаторните технически стандарти, допълващи Регламента за ЦДЦК. По-специално не е ясно дали ЦДЦК трябва да бъде освободен от задължението да има алтернативен център, ако неговият доставчик трета страна на услуги в областта на ИКТ поддържа такъв ([40]). Ако ЦДЦК бъде освободен от задължението да поддържа алтернативен център, не е ясно каква би

([33]) Достъпни на уебсайта на ЕЦБ www.ecb.europa.eu.

([34]) Вж. член 12 от Регламент (ЕС) № 909/2014.

([35]) Вж. също член 13, член 17, параграф 4 и член 22, параграф 6 от Регламент (ЕС) № 909/2014.

([36]) Вж. параграф 7.3 от Становище на Европейската централна банка от 6 април 2017 г. относно установяването на критичните инфраструктури за целите на сигурността на информационните технологии (CON/2017/10); параграф 7.2 от Становище на Европейската централна банка от 8 ноември 2018 г. относно определянето на основните услуги и операторите на основни услуги за целите на сигурността на мрежите и информационните системи (CON/2018/47); параграф 3.5.2 от Становище на Европейската централна банка от 2 май 2019 г. относно сигурността на мрежовите и информационните системи (CON/2019/17); и параграф 3.5.2 от Становище на Европейската централна банка от 11 ноември 2019 г. относно сигурността на мрежовите и информационните системи (CON/2019/38).

([37]) Вж. член 54, параграф 5 от предложения регламент и член 45, параграф 7 от Регламент (ЕС) № 909/2014.

([38]) Вж. член 54, параграф 4 от предложения регламент и член 45, параграф 6 от Регламент (ЕС) № 909/2014.

([39]) Вж. член 11, параграф 5 от предложения регламент.

([40]) Вж. член 78, параграф 3 от Делегиран регламент (ЕС) 2017/392 на Комисията от 11 ноември 2016 г. за допълване на Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти относно лицензирането, надзора и оперативните изисквания за централни депозитари на ценни книжа (ОВ L 65, 10.3.2017 г., стр. 48).

била правната стойност на това изискване. По същата причина в предложения регламент ([41]) се съдържа разпоредба във връзка с целите за времето и точката на възстановяване на информацията за всяка функция ([42]), а в съответния регулаторен технически стандарт се прави разграничение между критични функции ([43]) и критични операции ([44]) във връзка с времето за възстановяване, определено за критичните операции на ЦДЦК. Необходими са допълнителни разяснения и размисъл от страна на законодателните органи на Съюза относно взаимодействието между предложения регламент и регулаторните технически стандарти, допълващи Регламента за ЦДЦК, за да се предотврати рискът от противоречиви изисквания. Накрая следва да се поясни, че освобожденията, предоставени на ЦДЦК, управлявани от определени публични субекти съгласно Регламента за ЦДЦК ([45]), се разширяват съгласно предложения регламент.

2.3 *Компетентност на ЕСЦБ в областта на клиринга на ценни книжа*

2.3.1 На централните банки от ЕСЦБ са възложени контролни правомощия по отношение на централните контрагенти (ЦК). Във връзка с това националните централни банки от Евросистемата често си сътрудничат със съответните национални компетентни органи при изпълнението на контролните и надзорните функции на ЦК и участват в съответната колегия на ЦК, създадена съгласно Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета ([46]) (наричан по-долу „Регламентът за европейската пазарна инфраструктура“). Съответните членове на Евросистемата ([47]) участват в колегиите съгласно Регламента за европейската пазарна инфраструктура в качеството си на контролен орган и представляват Евросистемата като емитираща централна банка за ЦК, когато еврото е една от най-важните валути за финансовите инструменти, за които се извършва клиринг (и за офшорните ЦК, които извършват клиринг на значителен дял от финансовите инструменти в евро). ЕЦБ е емитиращата централна банка за ЦК извън еврозоната.

2.3.2 Съгласно предложения регламент ([48]) централните банки от ЕСЦБ не участват в разработването на технически стандарти във връзка с определянето на рисковете при ИКТ. Освен това в предложения регламент ([49]) липсва препращане към изискванията за целите за времето и точката на възстановяване на информация съгласно Регламента за европейската пазарна инфраструктура ([50]). Предложената регулаторна уредба не би трябвало да предвижда по-леки изисквания по отношение на рисковете при ИКТ от съществуващите понастоящем. Поради това е важно да се определят ясни цели за времето и точката на възстановяване на информация, за да има стабилна рамка за управлението на непрекъснатостта на дейността. Поддържането на конкретни цели за времето и точката на възстановяване на информация е част и от Принципите на КППИ—МОКЦК за инфраструктурите на финансовите пазари ([51]). Настоящата разпоредба на Регламента за европейската пазарна инфраструктура трябва да бъде запазена, а предложеният регламент – съответно адаптиран. Централните банки от ЕСЦБ следва да участват в изготвянето на вторично законодателство, както и в по-нататъшното изясняване и обмисляне от страна на законодателните органи на Съюза на взаимодействието между предложения регламент и допълващите регулаторни технически стандарти, така че да се избегне рискът от противоречащи си или припокриващи се изисквания.

3. **Специфични забележки относно аспектите на пруденциалния надзор**

3.1 С Регламент (ЕС) № 1024/2013 на Съвета ([52]) (наричан по-долу „Регламентът за ЕНМ“) на ЕЦБ се възлагат конкретни задачи във връзка с пруденциалния надзор над кредитните институции в еврозоната, както и отговорността за ефективното и последователно функциониране на единния надзорен механизъм (ЕНМ), в рамките на който между ЕЦБ и участващите НКО се разпределят конкретни отговорности по надзора. По-специално ЕЦБ има задачата да издава и отнема лицензите на всички кредитни институции. Освен това ЕЦБ има за задача да гарантира спазването на съответното законодателство на Съюза, с което на кредитните институции се налагат пруденциални изисквания, включително изискването да разполагат с надеждни управленски правила, като например процеси за стабилно управление на риска и механизми за вътрешен контрол ([53]). За тази цел на ЕЦБ се предоставят всички надзорни

([41]) Вж. член 11, параграф 6 от предложения регламент.
([42]) Вж. член 3, параграф 17 от предложения регламент.
([43]) Вж. член 76, параграф 2, букви г) и д) от Делегиран регламент (ЕС) 2017/392 на Комисията.
([44]) Член 78, параграфи 2 и 3 от Делегиран регламент (ЕС) 2017/392 на Комисията.
([45]) Вж. член 1, параграф 4 от Регламент (ЕС) № 909/2014.
([46]) Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ L 201, 27.7.2012 г., стр. 1).
([47]) Вж. член 18, параграф 2, букви ж) и з) от Регламента за европейската пазарна инфраструктура.
([48]) Вж. член 53, точка 2, буква б) и член 53, точка 3 от предложения регламент и член 34, параграф 3 от Регламента за европейската пазарна инфраструктура.
([49]) Вж. член 53, точка 2, буква а) от предложения регламент.
([50]) Вж. член 34 от Регламента за европейската пазарна инфраструктура.
([51]) Вж. Принципите на КППИ-МОКЦК за инфраструктурите на финансовите пазари, достъпни на уебсайта на Банката за международни разплащания www.bis.org.
([52]) Регламент (ЕС) № 1024/2013 на Съвета от 15 октомври 2013 г. за възлагане на Европейската централна банка на конкретни задачи относно политиките, свързани с пруденциалния надзор над кредитните институции (ОВ L 287, 29.10.2013 г., стр. 63).
([53]) Вж. член 4, параграф 1, буква д) и член 6, параграф 4 от Регламент (ЕС) № 1024/2013.

правомощия за намеса в дейността на кредитните институции, които са необходими за изпълнението на нейните функции. Поради това ЕЦБ и съответните НКО са компетентните органи, които упражняват определените правомощия за пруденциален надзор съгласно Регламент № 575/2013 на Европейския парламент и на Съвета ([54]) (наричан по-долу „Регламентът за капиталовите изисквания“) и Директива 2013/36/ЕС на Европейския парламент и на Съвета ([55]) (наричана по-долу „Директивата за капиталовите изисквания“).

3.2 В предложения регламент се посочва, че единната нормативна уредба и надзорната система следва да бъдат доразвити, за да обхванат оперативната устойчивост на цифровите технологии и сигурността на ИКТ, като се разширят правомощията на финансовите надзорни органи, чиято задача е да наблюдават и защитават финансовата стабилност и целостта на пазара ([56]). Целта е да се насърчи създаването на обща уредба на риска при ИКТ или на операционния риск чрез хармонизиране на основните изисквания за оперативната устойчивост на цифровите технологии за всички финансови субекти ([57]). По-специално предложеният регламент има за цел да консолидира и подобри изискванията за риска при ИКТ, които до момента са разпръснати в различни законодателни актове ([58]).

3.3 Изискванията, свързани с риска при ИКТ за финансовия сектор, понастоящем са разпръснати в редица актове на правото на Съюза, включително в Директивата за капиталовите изисквания, и в правни актовете с незадължителна сила (като насоките на ЕБО), разнообразни са, а понякога са непълни. В някои случаи мерките за риска при ИКТ са предвидени само косвено като част от мерките за операционния риск, а в други — въобще не са предвидени мерки. Това следва да бъде коригирано чрез осигуряването на съгласуваност между предложения регламент и тези актове. За тази цел в предложената директива за изменение са включени изменения, които изглеждат необходими, за да внесат правна яснота и последователност във връзка с прилагането на различните изисквания за оперативна устойчивост на цифровите технологии. Измененията на Директивата за капиталовите изисквания, които се предлагат с предложената директива за изменение ([59]), обаче се отнасят само до разпоредбите за плановете за действие при непредвидени обстоятелства и за осигуряване на непрекъснатост на дейността ([60]) предвид това, че се твърди, че те косвено служат като основа за управлението на риска при ИКТ.

3.4 Освен това съгласно предложения регламент ([61]) финансовите субекти, включително кредитните институции, разполагат с вътрешни управленски и контролни механизми, които осигуряват ефективното и благоразумно управление на всички рискове при ИКТ. Съгласно предложения регламент ([62]) предвидените в него изисквания се прилагат на индивидуално и консолидирано равнище, но без достатъчна координация с посоченото специфично секторно законодателство. На последно място, съгласно предложения регламент ([63]), без да се засягат разпоредбите относно предвидената в него надзорна рамка за възловите доставчици трети страни на услуги в областта на ИКТ ([64]), спазването на предвидените в него задължения се осигурява, за кредитните институции, от компетентния орган, определен в съответствие с член 4 от Директивата за капиталовите изисквания, без да се засягат конкретните задачи, възложени на ЕЦБ с Регламента за ЕНМ.

3.5 Предвид гореизложеното ЕЦБ разбира, че по отношение на кредитните институции и с изключение на разпоредбите на предложения регламент относно надзорната рамка за възловите доставчици трети страни на услуги в областта на ИКТ ([65]), предложеният регламент има за цел да създаде пруденциална вътрешна управленска рамка за управлението на риска при ИКТ, която ще бъде интегрирана в общата рамка за вътрешно управление съгласно Директивата за капиталовите изисквания. Освен това, предвид пруденциалния характер на предложената рамка, компетентните органи, отговарящи за надзора върху спазването на предвидените в нея задължения, включително ЕЦБ, ще бъдат органите, отговарящи за банковия надзор в съответствие с Регламента за ЕНМ.

([54]) Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г., стр. 1).

([55]) Директива 2013/36/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно достъпа до осъществяването на дейност от кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници, за изменение на Директива 2002/87/ЕО и за отмяна на директиви 2006/48/ЕО и 2006/49/ЕО (ОВ L 176, 27.6.2013 г., стр. 338).

([56]) Вж. съображение 8 от предложения регламент.

([57]) Вж. съображение 11 от предложения регламент.

([58]) Вж. съображение 12 от предложения регламент.

([59]) Вж. съображения 4 и 5 от предложената директива за изменение.

([60]) Вж. член 85 от Директивата за капиталовите изисквания.

([61]) Вж. член 4, параграф 1 от предложения регламент.

([62]) Вж. член 25, параграфи 3 и 4 от предложения регламент.

([63]) Вж. член 41 от предложения регламент.

([64]) Вж. глава V, раздел II от предложението за регламент.

([65]) Вж. глава V, раздел II от предложения регламент.

3.6 Поради това законодателните органи на Съюза биха могли да вземат предвид следните предложения за повишаване на яснотата и координацията между предложения регламент и Директивата за капиталовите изисквания. Първо, изискванията съгласно предложения регламент могат изрично да бъдат определени като пруденциални, както е направено в Регламента за ЦДЦК ([66]). Второ, съображенията на предложената директива за изменение ([67]) могат да бъдат разширени, тъй като изискванията съгласно предложения регламент надхвърлят единствената фаза на плановете за действие при непредвидени обстоятелства и за осигуряване на непрекъснатост на дейността. Мерките за управление на риска при ИКТ като цяло попадат в по-общото приложно поле на надеждните правила за управление съгласно член 74 от Директивата за капиталовите изисквания ([68]). Трето, предложеният регламент ([69]) следва да бъде изменен, за да се припомни в съображенията компетентността на ЕЦБ за пруденциалния надзор над кредитните институции съгласно Договора и Регламента за ЕНМ. Четвърто, прилагането на предвидените изисквания на индивидуална и консолидирана основа ([70]) следва да бъде преразгледано, тъй като в предложения регламент няма определение на понятията за подконсолидирана и консолидирана основа, а спрямо някои видове посредници (напр. платежните институции) не се извършва консолидиран надзор съгласно съответното законодателство. Освен това основата на прилагане на изискванията съгласно предложения регламент следва да произтича единствено от законодателството, приложимо за всеки вид финансов субект. За кредитните институции е предвидена ясна връзка между Директивата за капиталовите изисквания и предложения регламент, така че изискванията съгласно предложения регламент ще се прилагат автоматично на индивидуална, подконсолидирана или консолидирана основа ([71]), в зависимост от случая. Накрая, законодателните органи на Съюза биха могли да обмислят въвеждането на преходен режим за периода между влизането в сила на предложения регламент и влизането в сила на регулаторните технически стандарти, предвидени в предложения регламент, тъй като спрямо някои посредници, включително кредитните институции, вече се прилагат правилата за рисковете при ИКТ, приложими за конкретните сектори, които са по-подробни от общите разпоредби на предложения регламент.

3.7 Съгласно Регламента за ЕНМ на ЕЦБ е възложена задачата да гарантира, че кредитните институции спазват изискванията на правото на Съюза да разполагат с надеждни процеси за управление на риска и механизми за вътрешен контрол ([72]). Това означава, че ЕЦБ трябва да гарантира, че кредитните институции прилагат политики и процедури за оценка и управление на експозициите към операционен риск, включително към риска във връзка с използвания модел, и за рядко възникващи събития с голямо въздействие. Кредитните институции трябва да определят какво е операционен риск за целите на тези политики и процедури ([73]).

3.8 През юли 2017 г. Управителният съвет на Европейската централна банка (ЕЦБ) прие рамката на ЕНМ за съобщаване за киберинциденти (наричана по-долу „рамката“) въз основа на проект на предложение на Надзорния съвет в съответствие с член 26, параграф 8 и член 6, параграф 2 от Регламента за ЕНМ и член 21, параграф 1 от Регламент (ЕС) № 468/2014 на Европейската централна банка (ЕЦБ/2014/17) ([74]). Рамката се състои от обвързващо искане (индивидуални решения, адресирани до кредитни институции) за информация и/или съобщаване на основание член 10 от Регламента за ЕНМ ([75]). В някои държави вече има процедура за съобщаване на инциденти, съгласно която кредитните институции трябва да съобщават за всички значими киберинциденти на своите НКО. В тези държави значимите кредитни институции ще продължат да съобщават за инцидентите на НКО, които след това без ненужна забава ще ги препращат на ЕЦБ от името на поднадзорните лица. Поради това посочените по-горе решения

([66]) Вж. заглавието на глава II, раздел 4 „Пруденциални изисквания“ от Регламента за ЦДЦК.

([67]) Вж. съображение 4 от предложената директива за изменение.

([68]) Член 85 от Директива 2013/36/ЕС е само конкретизация. Във връзка с това вж. също стр. 4, 11 и 37 от Насоките на Европейския банков орган относно управлението на риска в областта на ИКТ и сигурността от 29 ноември 2019 г. (наричани по-долу „Насоките на ЕБО“), където общото правно основание е изрично посочено в член 74 от Директива 2013/36/ЕС.

([69]) Вж. член 41, параграф 1 от предложения регламент.

([70]) Вж. член 25, параграфи 3 и 4 от предложения регламент.

([71]) Вж. също член 109 от Директивата за капиталовите изисквания.

([72]) Вж. член 4, параграф 1, буква д) от Регламента за ЕНМ.

([73]) Вж. член 85 от Директивата за капиталовите изисквания.

([74]) Регламент (ЕС) № 468/2014 на Европейската централна банка от 16 април 2014 г. за създаване на рамката за сътрудничество в единния надзорен механизъм между Европейската централна банка и националните компетентни органи и с определените на национално равнище органи (Рамков регламент за ЕНМ) (ЕЦБ/2014/17) (ОВ L 141, 14.5.2014 г., стр. 1).

([75]) По-специално, киберинцидентите (идентифициран възможен пробив в информационната сигурност, било то злонамерен или случаен), трябва да се съобщават на ЕЦБ, ако е изпълнено поне едно от следните условия: 1) потенциалното финансово въздействие е 5 млн. евро или 0,1% от базовия собствен капитал от първи ред; 2) за инцидента е съобщено публично или той причинява репутационна вреда; 3) инцидентът е отнесен нагоре по йерархията до главния директор по информационните системи извън рамките на редовното отчитане; 4) банката е съобщила за инцидента на екипа за незабавно реагиране при компютърни инциденти, на агенция за сигурност или на полицията; 5) задействани са процедури за възстановяване от срив или за непрекъснатост на дейността или е подаден застрахователен иск за киберинцидент; 6) нарушени са правни или регулаторни изисквания; или 7) банката прилага вътрешни критерии и експертна преценка (включително за потенциално системно въздействие) и решава да уведоми ЕЦБ.

са адресирани и до тези национални компетентни органи, за да предадат тази информация на ЕЦБ въз основа на рамката. ЕЦБ подкрепя усилията на законодателните органи на Съюза да насърчат хармонизацията и рационализирането на набора от правила и задължения, приложими за кредитните институции във връзка със съобщаването за инциденти. Затова ЕЦБ е готова да измени (и евентуално да отмени) рамката, ако е необходимо, предвид евентуалното приемане на предложения регламент.

4. Специфични забележки относно управлението на риска при ИКТ, съобщаването за инциденти, тестването на оперативната устойчивост и риска при ИКТ, породен от трета страна

4.1 *Управление на риска при ИКТ*

4.1.1 ЕЦБ приветства въвеждането с предложения регламент на стабилна и всеобхватна рамка за управление на риска при ИКТ, която обхваща Насоките за киберустойчивост на КППИ — МОКЦК и е тясно съгласувана с най-добрите практики, включително Надзорните очаквания на Евросистемата за киберустойчивост на ИФП.

4.1.2 ЕЦБ подкрепя идеята финансовите субекти да извършват оценки на риска при всяка „съществена промяна“ в инфраструктурата на мрежите и информационните системи ([76]). Предложеният регламент обаче не съдържа определение за „съществена промяна“, което създава нежелана възможност за различно тълкуване от страна на финансовите субекти, което в крайна сметка би могло да възпрепятства постигането на целите на предложения регламент за хармонизация. От съображения за правна сигурност законодателните органи на Съюза биха могли да обмислят включването на определение на „съществена промяна“ в предложения регламент.

4.1.3 ЕЦБ като цяло подкрепя идеята финансовите субекти с изключение на микропредприятията да уведомяват компетентните органи за съответните разходи и загуби, причинени от сривове на ИКТ и инциденти с ИКТ ([77]). За да се гарантира обаче цялостната ефективност на системата и да се избегне възможното обременяване на компетентните органи и финансовите субекти с прекалено голям брой уведомления, законодателните органи на Съюза биха могли да обмислят въвеждането на подходящи прагове, евентуално от количествено естество.

4.1.4 ЕЦБ признава възможността финансовите субекти да поверят на предприятия от своята група или на външни предприятия задачите по проверка на съблюдаването на изискванията за управление на риска при ИКТ след одобрение от компетентните органи ([78]) В същото време е важно законодателните органи на Съюза да изяснят как ще бъде дадено одобрението от компетентните органи в случаите, когато даден финансов субект е подчинен на множество компетентни органи. Такава ситуация и могла да възникне, ако финансовият субект е кредитна институция, доставчик на услуги за криптоактиви и/или доставчик на платежни услуги. На последно място, във връзка с установяването и класифицирането, които трябва да бъдат извършени от финансовите субекти съгласно предложения регламент ([79]), ЕЦБ би счела за разумно, за целите на класификацията на активите, с предложения регламент от финансовите субекти да се изисква да вземат предвид и критичността на тези активи (т.е. дали поддържат критични функции).

4.2 *Уведомяване за инциденти*

4.2.1 ЕЦБ приветства усилията, очертани в предложения регламент, за хармонизиране на правилата за уведомяване за инциденти с ИКТ в рамките на Съюза и за постигане на централизирано уведомяване за съществените инциденти с ИКТ ([80]). Въвеждането на хармонизирана рамка за уведомяване на съответните компетентни органи за съществените инциденти с ИКТ ([81]) по принцип би рационализирало и хармонизирало бремето, свързано с уведомяването, за финансовите субекти, включително кредитните институции. Компетентните органи ще извлекат полза от по-широкия кръг от обхванати инциденти, който надхвърлят киберинцидентите, които понастоящем са уредени от съществуващите рамки ([82]). Бъдещото приемане на предложения регламент ще наложи преразглеждането и евентуалното отменяне на съществуващите рамки, включително рамката на ЕНМ за съобщаване за киберинциденти. За да се постигне обаче истинско рационализиране и пълно съгласуване на всички рамки, от решаващо значение е да се гарантира, че разпоредбите за съобщаване за инциденти съгласно предложения регламент, включително всички

([76]) Вж. член 7, параграф 3 от предложения регламент.
([77]) Вж. член 10, параграф 9 от предложения регламент.
([78]) Вж. член 5, параграф 10 от предложения регламент.
([79]) Вж. член 7 от предложения регламент.
([80]) Вж. член 19 от предложения регламент.
([81]) Вж. член 3, точки 7, 17 и 18 от предложения регламент.
([82]) Вж. например рамката.

относими определения, прагове и параметри за съобщаване, са изцяло съгласувани със съответните рамки. По-специално, от изключително значение е да се осигури съгласуваност между предложения регламент, от една страна, и Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета ([83]) (наричана по-нататък „ДПУ2“) и Насоките на ЕБО относно съобщаването за значими инциденти (наричани по-долу „Насоките на ЕБО“), от друга страна. Предложената директива за изменение ([84]) съдържа изменения на ДПУ2 във връзка с разграничаването на съобщаването за инциденти между предложения регламент и ДПУ2, което би засегнало основно доставчиците на платежни услуги, които също биха могли да бъдат лицензирани като кредитни институции, както и компетентните органи. Липсва яснота във връзка с процеса на уведомяване за инциденти и съществува потенциално припокриване между някои от инцидентите, за които трябва да бъде съобщавано както съгласно предложения регламент, така и съгласно Насоките на ЕБО.

4.2.2 Съгласно процедурите за уведомяване за съществени инциденти съгласно предложения регламент ([85]), ДПУ2 и Насоките на ЕБО доставчиците на платежни услуги трябва да представят доклад за инцидента на съответния компетентен орган, след като инцидентът е класифициран. Всъщност първоначалните доклади не обхващат същността, причината или функционалната област, засегната от инцидента, а доставчиците на платежни услуги могат да направят такива разграничения едва на по-късен етап, когато има по-подробна информация за инцидента. В резултат на това първоначалните доклади за инцидент могат да бъдат представени както съгласно предложения регламент, така и съгласно Насоките на ЕБО, или доставчиците на платежни услуги могат да вземат решение относно единна рамка за докладването и да коригират подадения доклад на по-късен етап. Тази несигурност (например по отношение на първопричината за инцидента) може да бъде отразена и в неокончателните и окончателните доклади. Това отново би повишило потенциала за паралелно подаване на доклади до компетентните органи съгласно предложения регламент и ДПУ2.

4.2.3 Някои инциденти, които могат да бъдат категоризирани като инциденти с ИКТ, могат да окажат въздействие и върху други области и в резултат на това за тях ще трябва да се уведоми съгласно Насоките на ЕБО. Такъв може да бъде случаят, когато даден инцидент оказва въздействие от гледна точка на ИКТ, но същевременно е засегнал предоставянето на платежни услуги пряко и/или други функционални области или канали, които не са ИКТ. Освен това може да има случаи, в които не е възможно да се направи разграничение между оперативни инциденти и инциденти с ИКТ. Освен това, в случай че един и същ финансов субект е значима кредитна институция и доставчик на платежни услуги, съгласно предложения регламент той ще трябва да съобщи за инцидента с ИКТ два пъти, тъй като е подчинен на два компетентни органа. Предвид гореизложеното в предложения регламент следва да се посочи по-ясно как трябва да се осъществи на практика взаимодействието между ДПУ2 и Насоките на ЕБО. По-важно е, за целите на хармонизирането и рационализирането на задълженията за съобщаване за инциденти, законодателните органи на Съюза да обмислят остатъчните въпроси, свързани с двойното съобщаване, както и да изяснят дали предложеният регламент, от една страна, и ДПУ2 и Насоките на ЕБО, от друга страна, ще съществуват съвместно, или трябва да има единен набор от изисквания за съобщаване за инциденти.

4.2.4. С предложения регламент се въвежда изискването ([86]) при получаването на доклада компетентният орган да потвърди, че е бил уведомен и възможно най-бързо да предостави на финансовия субект всички необходими сведения или указания, по-специално с оглед на корективните мерки, които субектът трябва да предприеме, или на начините за свеждане до минимум на неблагоприятните последици в секторите. Това би означавало, че компетентните органи следва активно да допринасят за овладяването на инцидентите и отстраняването на последиците от тях, като същевременно оценяват реакцията на поднадзорния субект при критични инциденти. ЕЦБ подчертава, че отговорността за последиците от инцидента и за тяхното отстраняване следва да продължи да се носи единствено и недвусмислено от съответния финансов субект. Поради това ЕЦБ предлага сведенията и указанията да се ограничат само до общите пруденциални сведения и указания. Предоставянето на по-широки сведения изисква специалисти със значителни технически познания, каквито обикновено няма в резерва от таланти на органите за пруденциален надзор.

4.3 *Тестване на оперативната устойчивост на цифровите технологии*

4.3.1 ЕЦБ приветства изискванията, определени в предложения регламент ([87]), за тестването на оперативната устойчивост на цифровите технологии на финансовите субекти, както и необходимостта всяка институция да има своя собствена програма за тестване. В предложения регламент ([88]) са описани различни видове примерни тестове за финансовите субекти. Видовете тестове не са много ясни, а някои от тях, като например тестовете за съвместимост, анкетите и тестването на различни сценарии, могат да бъдат тълкувани различно от ЕНО, компетентните органи или

([83]) Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар, за изменение на директиви 2002/65/ЕО, 2009/110/ЕО и 2013/36/ЕС и Регламент (ЕС) № 1093/2010 и за отмяна на Директива 2007/64/ЕО (ОВ L 337, 23.12.2015 г., стр. 35).

([84]) Вж. член 7, точка 9 от предложената директива за изменение.

([85]) Вж. член 17, параграф 3 от предложения регламент.

([86]) Вж. член 20 от предложения регламент.

([87]) Вж. членове 21 и 22 от предложения регламент.

([88]) Вж. член 22, параграф 1 от предложения регламент.

финансовите субекти. Освен това няма указания за честотата на всеки тест. Един от възможните подходи е с предложения регламент да се определят общи изисквания за тестване, а по-точното описание на видовете тестове да бъде определено в регулаторните технически стандарти и техническите стандарти за изпълнение.

4.3.2 Тестването на проникване (ТП) е мощен инструмент за тестване на защитата на сигурността и подготвеността. Поради това ЕЦБ насърчава ТП от финансовите субекти. С този инструмент се тестват не само техническите мерки, но и персонала и процесите. Резултатите от тези тестове могат значително да повишат осведомеността по въпросите на сигурността на висшето ръководство в тестваните субекти. Европейската рамка за червени екипи за етично хакерство въз основа на оперативни сведения за заплахи (TIBER-EU) ([89]) и други вече съществуващи инструменти за ТП извън Съюза са основни инструменти, чрез които самите субекти оценяват, тестват, практикуват и подобряват своята киберустойчивост и защита.

4.3.3 В повечето държави членки, в които се прилага TIBER-EU, контролните и надзорните органи не играят активна роля в изпълнението на местната програма TIBER-XX и в почти всички случаи екипът TIBER Cyber Team (TCT) е независим от тези функции. Поради тази причина обстойното тестване съгласно предложения регламент ([90]), посредством ТП, следва да се прилага като инструмент за укрепване на финансовата екосистема и повишаване на финансовата стабилност, а не само като надзорен инструмент. Освен това не е необходимо да се разработва нова усъвършенствана рамка за тестване на киберустойчивостта, тъй като държавите членки вече широко са приели TIBER— EU – единствената такава рамка в ЕС в момента.

4.3.4 Изискванията за лицата, провеждащи тестове, не би трябвало да се съдържат в основния текст на предложения регламент, тъй като секторът, свързан с ТП, все още се развива и иновациите могат да бъдат възпрепятствани от налагането на специфични изисквания. ЕЦБ обаче е на мнение, че за да се гарантира висока степен на независимост при провеждането на тестове, финансовите субекти не трябва да сключват трудов договор или договор за услуга с лица, провеждащи тестове, с които други финансови субекти от тяхната група са сключили трудов договор или договор за услуга или които са притежавани и/или контролирани от финансовите субекти, които се тестват.

4.3.5 За да се намали рискът от фрагментация и за да се гарантира хармонизация, в предложения регламент следва да се предвиди една рамка за ТП, която да се прилага за финансовия сектор в целия Съюз. Фрагментацията може да доведе до увеличаване на разходите и на нуждите от технически, оперативни и финансови ресурси както за компетентните органи, така и за финансовите институции. Тези повишени разходи и нужди могат в крайна сметка да окажат отрицателно въздействие върху взаимното признаване на тестовете. Тази липса на хармонизация и произтичащите от нея проблеми с взаимното признаване са особено важни за финансовите субекти, които имат множество лицензи и/или да извършват дейност в множество юрисдикции в Съюза. Регулаторните технически стандарти и техническите стандарти за изпълнение, които трябва да бъдат изготвени съгласно предложения регламент за ТП, трябва да бъдат в съответствие с TIBER-EU. Освен това ЕЦБ приветства възможността да участва в изготвянето на тези регулаторни технически стандарти и технически стандарти за изпълнение в сътрудничество с ЕНО.

4.3.6 Активното участие на компетентните органи в тестовете би могло да доведе до потенциален конфликт на интереси с другата изпълнявана от тях функция, а именно оценяването на рамката за тестване на финансовия субект. В този контекст ЕЦБ предлага от предложения регламент да се премахнат задълженията на компетентните органи във връзка с валидирането на документи и издаването на удостоверение за тест на проникването.

4.4 Риск при ИКТ, пораждан от трета страна

4.4.1 ЕЦБ приветства въвеждането на всеобхватен набор от ключови принципи и стабилна надзорна рамка за идентифициране и управление на рисковете при ИКТ, произтичащи от доставчиците на услуги в областта на ИКТ, които са трети страни, независимо дали те принадлежат към една и съща група финансови субекти. За да се постигне обаче ефективно идентифициране и управление на риска при ИКТ, е важно правилно да се идентифицират и класифицират възловите доставчици на услуги в областта на ИКТ, които са трети страни. Във връзка с това, въпреки че приветства приемането на делегирани актове ([91]), които ще допълнят критериите за класификация ([92]), ЕЦБ трябва да бъде консултирана преди приемането на тези актове.

([89]) Достъпна на уебсайта на ЕЦБ www.ecb.europa.eu.
([90]) Членове 23 и 24 от предложения регламент.
([91]) Вж. член 28, параграф 3 от предложения регламент.
([92]) Вж. член 28, параграф 2 от предложения регламент.

4.4.2 Що се отнася до структурата на надзорната рамка ([93]), е необходимо допълнително изясняване на ролята на съвместният комитет. В същото време ЕЦБ приветства включването ѝ Надзорния форум като наблюдател, тъй като тази роля ще ѝ предостави същия достъп до документация и информация като членовете с право на глас ([94]). ЕЦБ би искала да насочи вниманието на законодателните органи на Съюза към това, че като наблюдател тя ще допринесе за работата на Надзорния форум както в качеството си на емитираща централна банка, която отговаря за надзора на пазарните инфраструктури, така и в качеството си на орган за пруденциален надзор над кредитните институции. Освен това ЕЦБ отбелязва, че освен наблюдател в Надзорния форум тя, в качеството си на компетентен орган, също ще бъде част от съвместния разследващ екип. Във връзка с това законодателните органи на Съюза биха могли да обмислят допълнително състава на съвместните разследващи екипи ([95]), за да се гарантира подходящо балансирано участие на съответните компетентни органи. По същата причина ЕЦБ счита, че максималният брой участници в съвместните разследващи екипи трябва да бъде увеличен, като се вземат предвид критичността, сложността и обхватът на услугите в областта на ИКТ, предоставяни от трети страни.

4.4.3 ЕЦБ отбелязва, че съгласно предложения регламент водещият надзорник може да попречи на възловите доставчици трети страни на услуги в областта на ИКТ да сключват допълнителни споразумения за подизпълнение, когато: i) подизпълнителят е доставчик на услуги в областта на ИКТ – трета страна или подизпълнител в областта на ИКТ, учреден в трета държава, и ii) възлагането на подизпълнители се отнася до възлова или важна функция на финансовия субект. ЕЦБ би искала да подчертае, че тези правомощия могат да бъдат упражнявани само от водещия надзорник в случаите на споразумения за подизпълнение, когато възлов доставчик трета страна на услуги в областта на ИКТ възлага възлова или важна функция на самостоятелно юридическо лице, учредено в трета държава. Водещият надзорник не би могъл да упражнява сравними правомощия, за да попречи на възлов доставчик трета страна на услуги в областта на ИКТ да възлага възлови или важни функции на финансовия субект на съоръжения на този доставчик на услуги, които се намират в трета държава. Например може да се окаже, че от оперативна гледна точка критичните данни и/или информация могат да се съхраняват или обработват от съоръжения, разположени извън Европейското икономическо пространство (ЕИП). В такъв случай правомощията на водещия надзорник може да не са достатъчни, за да могат компетентните органи да получат достъп до цялата информация, помещения, инфраструктури и персонал, които са от значение за изпълнението на всички възлови или важни функции на финансовия субект. За да се гарантира, че компетентните органи могат да изпълняват задачите си безпрепятствено, ЕЦБ предлага на водещия надзорник да се предостави правомощието да ограничава също така използването от възлови доставчици трети страни услуги в областта на ИКТ на съоръжения, намиращи се извън ЕИП. Това правомощие може да бъде упражнено в случаите, когато не са налице административни споразумения със съответните органи на трети държави, както е предвидено в предложения регламент ([96]), или когато представителите на възловите доставчици трети страни на услуги в областта на ИКТ не предоставят достатъчно гаранции съгласно рамката на съответната трета държава за достъпа до информацията, помещенията, инфраструктурата и персонала, необходими за осъществяването на контролните или надзорни задачи .

4.4.4 На последно място, изискването компетентните органи да предприемат последващи действия във връзка с препоръките на водещия надзорник ([97]) би могло да се окаже неефективно, тъй като компетентните органи може да нямат цялостен поглед върху рисковете, генерирани от всеки възлов доставчик трета страна на услуги в областта на ИКТ. Освен това от компетентните органи може да се изиска да предприемат действия срещу своите поднадзорни финансови субекти, когато препоръките не са изпълнени от възловите доставчици трета страна на услуги в областта на ИКТ. Съгласно предложения регламент ([98]) компетентните органи могат да поискат от своите поднадзорни финансови субекти временно да преустановят възловите услуги на третата страна или да прекратят неизтеклите договори с възловите доставчици на услуги — трети страни. Трудно е предвиденият последващ процес да се изрази в конкретни действия. По-специално, не е ясно дали поднадзорният финансов субект ще бъде в състояние да спре изпълнението на договор с възлов доставчик на услуги — трета страна или да го прекрати. Причината за това е, че възловият доставчик трета страна на услуги в областта на ИКТ може да бъде значим доставчик за финансовия субект или че финансовият субект може да направи разходите и претърпи щети, договорни или други, в резултат на такова спиране или прекратяване. Освен това този подход не благоприятства сближаването на надзорните практики, тъй като компетентните органи могат да тълкуват една и съща препоръка по различен начин. Това в крайна сметка би могло да възпрепятства предвидената хармонизация и последователния подход при наблюдението на критичния риск при ИКТ, пораждан от трета страна, на равнището на Съюза. Предвид гореизложеното законодателните органи на Съюза биха могли да обмислят да предоставят на законовите надзорни органи специални правомощия за правоприлагане спрямо възловите доставчици трети страни на услуги в областта на ИКТ, като вземат предвид ограниченията, наложени от доктрината Meroni, частично смекчени от Съда в решението му по делото ЕОЦКП ([99]).

([93]) Вж. член 29 от предложения регламент.
([94]) Вж. член 29, параграф 3 от предложения регламент.
([95]) Вж. член 35 от предложения регламент.
([96]) Вж. член 39, параграф 1 от предложения регламент.
([97]) Вж. член 29, параграфи 4 и член 37 от предложения регламент.
([98]) Вж. член 37, параграф 3 от предложения регламент.
([99]) Вж. Решение на Съда от 22 януари 2014 г., Обединено кралство Великобритания и Северна Ирландия/Европейски парламент и Съвет на Европейския съюз, C-270/12, ECLI:EU:C:2014:18.

Когато ЕЦБ отправя препоръки за изменения на предложения регламент, конкретните предложения с обяснителен текст към тях се представят в технически работен документ. Техническият работен документ е достъпен на английски език на EUR-Lex.

Съставено във Франкфурт на Майн на 4 юни 2021 година.

Председател на ЕЦБ
Christine LAGARDE