ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 24.9.2020 г.
COM(2020) 595 final

2020/0266 (COD)

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

(текст от значение за ЕИП)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

- Основания и цели на предложението

Настоящото предложение е част от пакета за цифрови финанси — пакет от мерки за допълнително разкриване и насърчаване на потенциала на цифровите финансови услуги за иновациите и конкуренцията, при същевременно ограничаване на пораждaните рискове. То е съобразено с приоритетите на Комисията за привеждане на Европа в готовност за цифровата ера и за изграждането на приспособена към бъдещите предизвикателства икономика, която функционира в интерес на хората. Пакетът за цифровите финансови услуги включва нова стратегия за цифровизиране на финансовите услуги в ЕС[1], чиято цел е в ЕС да се внедрят цифровите технологии и с тяхна помощ европейските иновативни дружества да заемат водеща роля, така че ползата от цифровите финансови услуги да бъде достъпна за европейските граждани и предприемачи. В допълнение към това предложение пакетът включва предложение за регламент относно пазарите на криптоактиви[2], предложение за регламент относно пилотна уредба на пазарните инфраструктури, основани на технологията на децентрализирания регистър (ТДР)[3], и предложение за директива за изясняване или изменение на някои разпоредби за финансовите услуги в ЕС[4].Цифровизацията и оперативната устойчивост на финансовия сектор са две страни на една и съща монета. Цифровите — или информационните и комуникационните — технологии (ИКТ) откриват възможности, но пораждат и рискове. Те трябва да бъдат добре разбирани и управлявани, особено в периоди на напрежение.

Поради това отговорните за политиките лица и надзорните органи започнаха да отделят все по-голямо внимание на рисковете, които осланянето на ИКТ поражда. Фокусът им в частност бе насочен към повишаване на устойчивостта на дружествата чрез въвеждането на стандарти и координирането на нормотворчески или надзорни стъпки. Тези усилия — в международен и европейски план, обхванаха не само различни отрасли, а и редица специфични сектори, в т.ч. финансовите услуги.

Рисковете при ИКТ обаче продължават да представляват предизвикателство за оперативната устойчивост, функциониране и стабилност на финансовата система на ЕС. С реформата, последвала финансовата криза от 2008 г., главно бе засилена финансовата устойчивост[5] на финансовия сектор на ЕС, като рисковете при ИКТ бяха едва косвено засегнати в някои сфери като част от по-общите мерки за преодоляване на операционните рискове.

---

1 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно стратегия за цифровизиране на финансовите услуги в ЕС, 23 септември 2020 г., COM(2020)591.

2 Предложение за регламент на Европейския парламент и на Съвета относно пазарите на криптоактиви и за изменение на Директива (ЕС) 2019/1937, COM(2020)593.

3 Предложение за регламент на Европейския парламент и на Съвета относно пилотна уредба на пазарните инфраструктури, основани на технологията на децентрализирания регистър, COM(2020)594.

4 Предложение за директива на Европейския парламент и на Съвета 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, COM(2020)596.

5 Главната цел на приетите различни мерки бе да се увеличат капиталовите ресурси и ликвидността на финансовите субекти, както и да се ограничи пазарният и кредитният риск.

Въпреки че следкризисните промени във финансовото законодателство на ЕС обхванаха в единна нормативна уредба значителна част от финансовите рискове при финансовите услуги, те не разгледаха обстойно въпроса с оперативната устойчивост на цифровите технологии. Предприетите във връзка с тази устойчивост мерки притежаваха редица белези, които ограничиха ефективността им. Например те често бяха под формата на директиви за минимално хармонизиране или въвеждащи принципни положения регламенти, което остави значителна възможност за различаващи се подходи в рамките на единния пазар. Освен това рисковете при ИКТ бяха разглеждани, в контекста на покриването на операционния риск, слабо или само отчасти. Дори самите мерки се различаваха при отделните секторни норми на финансовото законодателство. Поради това намесата на равнище Съюза не отговори напълно на това, от което европейските финансови субекти имаха нужда, за да могат в контекста на управлението на операционните рискове да устояват, да реагират и да се възстановяват от инцидентите с ИКТ. Тя също така не предостави на надзорните органи на финансовия сектор най-подходящите инструменти за изпълнение на техните мандати за предотвратяване на финансова нестабилност при възникването на тези рискове.

Липсата на равнище ЕС на подробни и всеобхватни норми за оперативната устойчивост на цифровите технологии доведе до множество национални нормотворчески инициативи (например за тестване на оперативната устойчивост на цифровите технологии) и надзорни подходи (например за преодоляване на зависимостта от доставчици трети страни на услуги в областта на ИКТ). Действията на равнище държава членка обаче са с ограничен ефект предвид трансграничния характер на рисковете при ИКТ. Нещо повече: от една страна несъгласуваните национални инициативи доведоха до припокривания, различия, дублиращи се изисквания, високи административни разходи и разходи за съблюдаване на изискванията — особено за трансграничните финансови субекти, а от друга — оставиха скрити и следователно без решение някои рискове при ИКТ. Тази ситуация разпокъсва единния пазар, подкопава стабилността и целостта на финансовия сектор на ЕС и застрашава защитата на потребителите и инвеститорите.

Поради това е необходимо да се въведе подробна и всеобхватна уредба на оперативната устойчивост на цифровите технологии, използвани от финансовите субекти от ЕС. Тази уредба ще задълбочи измерението на единната нормативна уредба, посветено на управлението на цифровия риск. По-специално тя ще усъвършенства и оптимизира управлението на риска при ИКТ от страна на финансовите субекти, ще въведе обстойно тестване на системите на ИКТ, ще повиши осведомеността на надзорните органи за рисковете за киберсигурността и за инцидентите с ИКТ, пред които са изправени финансовите субекти, и ще оправомощи надзорните органи на финансовия сектор да следят рисковете, произтичащи от зависимостта на финансовите субекти от доставчиците трети страни на услуги в областта на ИКТ. С предложението ще се създаде стабилен механизъм за уведомяване за инцидентите, с който ще се намали административното бреме за финансовите институции и ще се засили ефективността на надзора.

- Съгласуваност с действащите разпоредби в тази област на политиката

Настоящото предложение е част от мащабните усилия на европейско и международно равнище за укрепване на киберсигурността при финансовите услуги и за преодоляване на операционните рискове в по-общ план[6].

То е отговор и на съвместното техническо становище[7] на Европейските надзорни органи (ЕНО) от 2019 г., в което се призовава за по-съгласуван подход към рисковете при ИКТ във финансовия сектор, като на Комисията се препоръчва да засили оперативната устойчивост на цифровите технологии при финансовите услуги чрез секторно насочена инициатива на ЕС, която да е съизмерима с целта. Становището на ЕНО бе в отговор на изготвения от Комисията през 2018 г. План за действие в областта на финансовите технологии[8].

- Съгласуваност с другите политики на Съюза

Както посочи председателят Урсула фон дер Лайен в политическите си насоки[9] и както бе обявено в съобщението „Изграждане на цифровото бъдеще на Европа“[10], Европа на всяка цена трябва да се възползва изцяло от потенциала на цифровата ера и да засили промишления и иновативния си капацитет при съблюдаването на подходяща защита и етични принципи. В Европейската стратегия за данните[11] се определят четири стълба — защита на данните, основни права, безопасност и киберсигурност — като основни предпоставки за общество, на което данните позволяват да функционира. Неотдавна Европейският парламент започна работа по доклад за цифровите финансови услуги, в който наред с другото се призовава за общ подход към киберустойчивостта на финансовия сектор[12].Една нормативна уредба, насочена към засилването на оперативната устойчивост на цифровите технологии, използвани от финансовите субекти от ЕС, е в съответствие с тези политически цели. С предложението ще бъдат подкрепени и политическите усилия за възстановяване от коронавируса, тъй като навлизането на цифрово финансиране ще бъде обвързано с оперативната устойчивост.

Инициативата ще запази ползата от хоризонталната уредба на киберсигурността (например Директивата за сигурността на мрежите и информационните системи — Директива за МИС), като остави финансовия сектор в нейния обхват. Финансовият

---

6 Cyber-resilience: Range of practices [Устойчивост на кибератаки: набор от практики], Базелски комитет по банков надзор, декември 2018 г. и Principles for sound management of operational risk (PSMOR) [Принципи на стабилното управление на операционния риск], октомври 2014 г.

7 Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector [Съвместно становище на Европейските надзорни органи до Европейската комисия за необходимостта от законодателни подобрения във връзка с изискванията за управление на риска при ИКТ във финансовия сектор на ЕС], JC 2019 26 (2019).

8 Съобщение на Европейската комисия „План за действие в областта на финансовите технологии“, COM/2018/0109 final.

9 Урсула фон дер Лайен, Политически насоки за следващата Европейска комисия (2019—2024 г.), https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_bg_1.pdf.

10 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Изграждане на цифровото бъдеще на Европа“, COM(2020) 67 final.

11 Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Европейска стратегия за данните“, COM(2020) 66 final.

12 Доклад с препоръки към Комисията относно цифровото финансиране: нововъзникващи рискове, свързани с криптоактивите – регулаторни и надзорни предизвикателства в областта на финансовите услуги, институции и пазари, 2020/2034(INL), https://www.europarl.europa.eu/doceo/document/TA-9-2020-0265_BG.html

сектор ще продължи да бъде тясно свързан с групата за сътрудничество за МИС, а надзорните органи на финансовия сектор ще могат да обменят съответната информация в рамките на съществуващата екосистема на МИС. Инициативата е в съответствие и с Директивата за европейските критични инфраструктури (ЕКИ), която понастоящем се преразглежда с цел да се подобри защитата и устойчивостта на критичните инфраструктури срещу заплахи, различни от киберзаплахите. Накрая, настоящото предложение е в пълно съответствие със Стратегията за Съюза за сигурност[13], в която се призовава за инициатива за оперативна устойчивост на цифровите технологии във финансовия сектор, предвид силната му зависимост от услугите в областта на ИКТ и уязвимост на кибератаки.

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

- Правно основание

Настоящото предложение за регламент се основава на член 114 от ДФЕС.

С него, чрез хармонизиране на разпоредбите относно управлението на риска при ИКТ, уведомяването, тестването и риска при ИКТ, пораждан от трета страна, се премахват пречките пред вътрешния пазар на финансови услуги и се подобрява неговото изграждане и функциониране. Сегашните различия от нормативно и надзорно естество в тази област — както на национално равнище, така и на равнище ЕС, възпрепятстват единния пазар на финансови услуги, тъй като финансовите субекти, които извършват дейност в трансграничен план, са изправени пред припокриващи се или разнородни нормативни изисквания или надзорни очаквания, които потенциално могат да ги затрудняват да упражняват свободата си на установяване и на предоставяне на услуги. Разнопосочните правила водят и до нарушаване на конкуренцията между един и същ вид финансови субекти в различни държави членки. Освен това в областите, в които няма хармонизация или тя е частична или ограничена, разнородните национални правила или подходи – вече в сила или в процес на приемане и прилагане на национално равнище, могат да попречат на упражняването на свободите на единния пазар при финансовите услуги. Това особено важи за рамките за тестване на оперативните цифрови технологии и за надзора на възловите доставчици трети страни на услуги в областта на ИКТ.

Предложението има отражение върху няколко директиви на Европейския парламент и на Съвета, приети на основание член 53, параграф 1 от ДФЕС, поради което същевременно се приема предложение за директива с цел да се отрази необходимото изменение на тези директиви.

- Субсидиарност

Тясната взаимосвързаност на финансовите услуги, значителното трансгранично измерение в дейността на финансовите субекти и силната зависимост на финансовия сектор като цяло от доставчиците трети страни на услуги в областта на ИКТ налагат наличието на силна оперативна устойчивост на цифровите технологии като въпрос от общ интерес с оглед на стабилността на финансовите пазари на ЕС. Различията в резултат на уредби с различна нормативна строгост или частично съгласувани помежду

[13] Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейския икономически и социален комитет и Комитета на регионите относно Стратегията на ЕС за Съюза на сигурност, COM(2020) 605 final.

си, припокривания или множество изисквания към едни и същи финансови субекти, извършващи трансгранична дейност или притежаващи няколко лицензa[14] на единния пазар, могат да бъдат преодолени ефективно само на равнището на Съюза.

Настоящото предложение хармонизира измерението на оперативните цифрови технологии в един тясно интегриран и взаимосвързан сектор, който в повечето други възлови области вече е обхванат от единна нормативна уредба и надзор. По въпроси като уведомяването за инцидентите с ИКТ, само едни единни норми на Съюза са в състояние да намалят административното бреме и финансовите разходи, свързани с уведомяването на различни съюзни и национални органи за един и същ инцидент с ИКТ. Действия на равнище ЕС са нужни и за да се улесни взаимното признаване на резултатите от обстойното тестване на оперативната устойчивост на цифровите технологии при дружествата с трансгранична дейност, които при липсата на съюзни норми подлежат — или биха могли да подлежат — на различни уредби в различните държави членки. Различията в тестовите подходи на държавите членки могат да се преодолеят само с действия на равнището на Съюза. Такива действия са нужни и за да се запълни липсата на подходящи надзорни правомощия за наблюдение на рисковете, които доставчиците трети страни на услуги в областта на ИКТ крият за финансовия сектор на ЕС, в т.ч. риска от концентрация и от верижно разпространение на проблемите.

- Пропорционалност

Предложените норми не надхвърлят необходимото за постигането на целите на предложението. Те обхващат само аспектите, които държавите членки не могат да постигнат самостоятелно и където административното бреме и разходите са съизмерими с конкретните и общите цели, които трябва да бъдат постигнати.

Използването на качествени и количествени критерии за оценка осигурява пропорционалност както по отношение на обхвата, така и на интензитета. Тяхната цел е новите норми, които обхващат всички финансови субекти, същевременно да са съобразени с рисковете и нуждите, присъщи на размера и стопанския профил на всеки от тях. Пропорционалността е заложена и в разпоредбите относно управлението на риска при ИКТ, тестването на оперативната устойчивост на цифровите технологии, уведомяването за съществените инциденти с ИКТ и надзора на възловите доставчици трети страни на услуги в областта на ИКТ.

- Избор на инструмент

Разпоредбите относно управлението на риска при ИКТ, уведомяването за инцидентите с ИКТ, тестването, както и надзора на възловите доставчици трети страни на услуги в областта на ИКТ трябва да се съдържат в регламент, така че подробните изисквания да бъдат приложими ефективно, пряко и еднакво за всички, без при това да се засягат предвидените в настоящия регламент пропорционалност и специални разпоредби. Съгласуваността при преодоляването на оперативните рискове при цифровите технологии е фактор за доверието във финансовата система и нейната стабилност. Когато изборът е регламент, това спомага за намаляване на нормативната сложност, насърчава сближаването на надзорните практики и повишава правната сигурност; в

[14] Един и същ финансов субект може да има лиценз за банка, за инвестиционен посредник и за платежна институция, като всеки от тях е издаден от различен надзорен орган в една или няколко държави членки.

тази връзка настоящият регламент допринася и за намаляване на разходите за съблюдаване на изискванията за финансовите субекти, особено за тези, които извършват трансгранична дейност, и оттам — за премахване на изкривяванията на конкуренцията.

С настоящия регламент се премахват също така нормативните несъответствия, а и различията в строгостта на националните нормативни или надзорни подходи към риска при ИКТ и оттам — пречките пред единния пазар на финансови услуги, по-специално за безпрепятственото упражняване от страна на финансовите субекти с трансгранично присъствие на свободата на установяване и на предоставяне на услуги.

Накрая, единната нормативна уредба е въведена предимно чрез регламенти, така че при нейната актуализация с компонента за оперативната устойчивост на цифровите технологии следва да се избере същият правен инструмент.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

- Последващи оценки/проверки за пригодност на действащото законодателство

Понастоящем няма финансови актове на Съюза, които да са насочени изключително към оперативната устойчивост или обстойното проучване на рисковете, които цифровизирането крие, като тук се включват дори тези, чиито норми обхващат в по-общ план измерението на операционния риск, в което рискът при ИКТ е подкомпонент. Досега намесата на Съюза помогна да се посрещнат потребностите и проблемите, които се оказаха налице след финансовата криза от 2008 г.: недостатъчно капитализирани кредитни институции, недостатъчно добре интегрирани финансови пазари и минимална към онзи момент хармонизация. Рискът при ИКТ не бе сред приоритетите, в резултат на което нормативната уредба на отделните финансови подсектори се разви при липсата на координация. Въпреки това действията на Съюза постигнаха целта си за осигуряване на финансова стабилност и въвеждане за финансовите институции в ЕС на единен набор от хармонизирани пруденциални изисквания и етични правила. Явната оценка е трудна поради факта, че в миналото факторите, обуславящи законодателните намеси на Съюза, не доведоха до въвеждането на специални или широко приложими правила с оглед на широкоразпространеното използване на цифровите технологии и произтичащите от това рискове за финансовия сектор. Във всеки стълб на настоящия регламент обаче се съдържа имплицитна оценка и са отразени съответните законодателни изменения във връзка с нея.

- Консултации със заинтересованите страни

При изготвянето на настоящото предложение Комисията се консултира със заинтересованите страни, а именно:

i) Комисията проведе открита обществена консултация по тази тема (19 декември 2019 г. — 19 март 2020 г.)[15];

ii) Комисията се допита до обществеността чрез първоначална оценка на въздействието (19 декември 2019 г. — 16 януари 2020 г.)[16];

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

iii) на два пъти (18 май 2020 г. и 16 юли 2020 г.) службите на Комисията се допитаха до експерти от държавите членки в Експертната група по банково дело, плащания и застраховане[17];

iv) в рамките на предвидените за 2020 г. прояви на кампанията за популяризиране на цифровите финансови услуги, на 19 май 2020 г. службите на Комисията проведоха специален уебинар, посветен на оперативната устойчивост на цифровите технологии.

С обществената консултация Комисията целеше да събере информация с оглед на потенциалното изготвяне на многосекторна уредба на ЕС на оперативната устойчивост на цифровите технологии при финансовите услуги. Отговорилите широко подкрепиха въвеждането на специална уредба с действия в четирите области на консултацията, като същевременно подчертаха необходимостта да се гарантира пропорционалност и внимателно да се проучи и обясни взаимодействието с хоризонталните норми на Директивата за МИС. Комисията получи два отговора по първоначалната оценка на въздействието, в които респондентите се бяха спрели на конкретни аспекти, свързани с областта на тяхната дейност.

На срещата на 18 май 2020 г., организирана от Експертната група по банково дело, плащания и застраховане, държавите членки недвусмислено подкрепиха засилването на оперативната устойчивост на цифровите технологии във финансовия сектор чрез предвидените действия в четирите очертани от Комисията области. Държавите членки подчертаха също така необходимостта от ясно формулиране на връзката на новите разпоредби с нормите относно операционния риск (както е уреден във финансовото законодателство на ЕС) и с хоризонталните норми относно киберсигурността (Директивата за МИС). При второто заседание някои държави членки изтъкнаха необходимостта да се гарантира пропорционалност и да се проучи специфичното положение на малките предприятия или дъщерните дружества от по-големи групи, както и необходимостта от силен мандат за участващите в надзора НКО.

В предложението са включени и взети предвид и становищата, получени при срещите със заинтересованите страни и с органите и институциите на ЕС. Заинтересованите страни, в т.ч. доставчиците трети страни на услуги в областта на ИКТ, като цяло изразиха подкрепата си. Анализът на получената обратна информация показа желание за запазване на пропорционалността и следването, при изготвянето на разпоредбите, на принципен и отчитащ риска подход. В институционален аспект основната информация дойде от Европейския съвет за системен риск (ЕССР), ЕНО, Агенцията на Европейския съюз за киберсигурност (ENISA) и Европейската централна банка (ЕЦБ), както и от компетентните органи на държавите членки.

- Събиране и използване на експертни становища

При изготвянето на настоящото предложение Комисията се базира на качествен и количествен емпиричен материал от реномирани източници, в т.ч. двете съвместни технически становища на ЕНО. Този материал бе допълнен с поверителни сведения и

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

обществено достъпни доклади от надзорни органи, международни органи за стандартизация и водещи научноизследователски институти, както и с количествени и качествени данни от установените заинтересовани страни от световния финансов сектор.

- Оценка на въздействието

Настоящото предложение е придружено от оценка на въздействието, която бе представена на Комитета за регулаторен контрол (КРК) на 29 април 2020 г. и бе одобрена на 29 май 2020 г.[18] КРК препоръча подобрения в някои области, така че: i) да се доизясни как ще се гарантира пропорционалността; ii) да се обясни по-ясно в каква степен предпочетеният вариант се отклонява от съвместните технически становища на ЕНО и защо той е оптимален; както и iii) да се обясни по-подробно как предложението взаимодейства с действащото законодателство на ЕС, в т.ч. с понастоящем преразглежданите норми. Оценката на въздействието бе коригирана с оглед на тези въпроси, като бяха взети предвид и по-подробните коментари на КРК.

Комисията проучи няколко варианта за разработване на уредба на оперативната устойчивост на цифровите технологии:

- „Без промени“: изискванията за оперативна устойчивост ще продължат да се определят от настоящия разнопосочен набор от норми на ЕС в областта на финансовите услуги, отчасти от Директивата за МИС, и от действащите или бъдещи национални режими;
- Вариант 1: засилване на капиталовите буфери: въвеждане на допълнителни капиталови буфери, за да се увеличи капацитетът на финансовите субекти да поемат загубите, които биха могли да възникнат вследствие на липсата на оперативна устойчивост на цифровите технологии;
- Вариант 2: въвеждане на акт относно оперативната устойчивост на цифровите технологии при финансовите услуги: създаване на всеобхватна уредба на равнище ЕС със съгласувани норми, насочени към потребностите на всички подлежащи на регламентиране финансови субекти във връзка с оперативната устойчивост на цифровите технологии, и на надзорна рамка на възловите доставчици трети страни на ИКТ;
- Вариант 3: акт относно оперативната устойчивост на цифровите технологии при финансовите услуги заедно с централизиран надзор на възловите доставчици трети страни на услуги в областта на ИКТ: в допълнение към акта за оперативна устойчивост на цифровите технологии (вариант 2) се създава нов орган, който да упражнява надзор над предоставяните в областта на ИКТ услуги от доставчици трети страни на такива услуги.

Бе предпочетен вторият вариант, тъй като той постига повечето от планираните цели по ефективен, ефикасен и съгласуван с останалите политики на Съюза начин. Повечето заинтересовани страни също предпочетоха този вариант.

[18] Работен документ на службите на Комисията — Доклад за оценката на въздействието, придружаващ Регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите услуги във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014 и (ЕС) № 909/2014, SWD(2020)198 от 24.9.2020 г.

Предпочетеният вариант ще доведе до еднократни и постоянни разходи[19]. Еднократните разходи се дължат главно на инвестициите в информационни системи и е трудно да се определят количествено предвид различното състояние на сложните информационни инфраструктури на дружествата и по-специално — на техните традиционни информационни системи. Дори и така, размерът на тези разходи вероятно ще бъде ограничен при големите дружества предвид значителните инвестиции в ИКТ, които те вече са направили. Разходите се очаква да бъдат ограничени и при по-малките дружества, тъй като приложимите спрямо тях мерки ще бъдат съобразени с по-ниския риск при тях.

В социално-икономически и екологичен аспект предпочетеният вариант ще има положително въздействие върху МСП с дейност в сектора на финансовите услуги. Предложението ще изясни какви са приложимите за МСП норми и така ще намали разходите за съблюдаване на изискванията.

Основното социално въздействие на предпочетения вариант ще бъде върху потребителите и инвеститорите. Засилената оперативна устойчивост на цифровите технологии във финансовата система на ЕС ще намали броя на инцидентите и средните разходи при тях. Обществото като цяло ще извлече полза от повишеното доверие към сектора на финансовите услуги.

Накрая, що се отнася до въздействието върху околната среда, избраният вариант ще насърчи навлизането на най-новите инфраструктури на ИКТ и услуги в областта на ИКТ, които се очаква, че ще бъдат по-устойчиви от тази гледна точка.

- Пригодност и опростяване на законодателството

Премахването на припокриващите се изисквания за уведомяване за инцидентите с ИКТ ще намали административното бреме и свързаните с него разходи. Освен това хармонизирането на тестването на оперативната устойчивост на цифровите технологии, т.е. взаимното му признаване в рамките на единния пазар, ще намали разходите, особено за трансграничните дружества, на които иначе би могло да се наложи да провеждат отделни тестове в отделните държавите членки[20].

- Основни права

ЕС е решен да разполага с високи стандарти за защита на основните права. Всички насърчавани от настоящия регламент споразумения за доброволен обмен на информация между финансовите субекти ще се изпълняват в защитена среда при пълно спазване на нормите на Съюза за защита на данните, в частност Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[21], особено когато обработването на лични данни се прави с оглед на законния интерес на контролиращия субект.

4. ОТРАЖЕНИЕ ВЪРХУ БЮДЖЕТА

[19] Пак там, стр. 89–94.

[20] Пак там.

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

Що се отнася до отражението върху бюджета, в настоящия регламент се предвижда засилена роля на ЕНО посредством предоставени им правомощия за подходящо наблюдение на възловите доставчици трети страни на ИКТ, поради което предложението ще доведе до увеличаване на ресурсите, в частност за провеждане на надзорните мисии (проверки и одити на място и онлайн), както и до използването на персонал с експертни познания по защитата на ИКТ.

Размерът и разпределението на тези разходи ще зависят от обхвата на новите надзорни правомощия и (конкретните) задачи, които ЕНО ще изпълняват. Когато разпоредбите на предложението влязат в сила, допълнителните човешки ресурси, които ще са необходими на ЕБО, ЕОЦКП и ЕОЗППО, са общо 18 служители на пълно работно време (ЕПРВ) — по 6 ЕПРВ за всеки орган, като разчетът за тях е 15,71 млн. евро за периода 2022—2027 г. ЕНО ще имат и допълнителни разходи за информационни технологии, за командировъчни във връзка с проверките на място, както и за превод — като разчетът за тях е 12 млн. евро за периода 2022—2027 г., а така също и други административни разходи в размер на 2,48 млн. евро за периода 2022—2027 г. Следователно разчетното общо отражение върху разходите за периода 2022—2027 г. е приблизително 30,19 млн. евро.

Следва също така да се отбележи, че макар числеността на необходимия за прекия надзор персонал (например нови служители и други разходи, свързани с новите задачи) да зависи с времето от броя и размера на поднадзорните възлови доставчици трети страни на услуги в областта на ИКТ, съответните разходи ще бъдат изцяло финансирани от таксите, начислявани на тези пазарни участници. Следователно не се предвижда отражение върху бюджетните кредити на ЕС (с изключение на допълнителния персонал), тъй като тези разходи ще бъдат изцяло финансирани от таксите.

Финансовото и бюджетно отражение на настоящото предложение е подробно изложено в приложената към него законодателна финансова обосновка.

5. ДРУГИ ЕЛЕМЕНТИ

- Планове за изпълнение и механизми за наблюдение, оценка и докладване

Предложението съдържа общ план за наблюдение и оценка на въздействието върху конкретните цели, който изисква от Комисията да извърши преглед най-рано три години след влизането му в сила и да докладва на Европейския парламент и на Съвета за основните си констатации.

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

- Подробно разяснение на отделните разпоредби на предложението

Предложението е структурирано около няколко основни области на политика, които представляват възлови взаимосвързани стълбове, включени по общо съгласие в европейските и международните насоки и най-добри практики, насочени към укрепване на кибернетичната и оперативната устойчивост на финансовия сектор.

Обхват на регламента и съобразено прилагане на необходимите мерки (член 2)

С оглед на съгласуваността на изискванията към финансовия сектор за управление на риска при ИКТ регламентът обхваща следните финансови субекти, уредени на

равнището на Съюза: кредитни институции; платежни институции; институции за електронни пари; инвестиционни посредници; доставчици на услуги за криптоактиви; централни депозитари на ценни книжа; централни контрагенти; места на търговия; регистри на трансакции; лица, управляващи алтернативни инвестиционни фондове и управляващи дружества; доставчици на услуги за докладване на данни; застрахователни и презастрахователни дружества; застрахователни посредници, презастрахователни посредници и посредници, които предлагат застрахователни продукти като допълнителна дейност; институции за професионално пенсионно осигуряване; агенции за кредитен рейтинг; задължителни одитори и одиторски дружества; администратори на критични бенчмаркове и доставчици на услуги за колективно финансиране.

Такъв обхват улеснява едно еднородно и съгласувано прилагане на всички компоненти на управлението на риска при ИКТ, като същевременно осигурява на финансовите субекти равни условия на конкуренция, тъй като ги подчинява на еднакви регулаторни задължения по отношение на риска при ИКТ. Същевременно в регламента се признава, че финансовите субекти се различават значително по размер, профил на стопанска дейност или изложеност на свързаните с цифровите технологии рискове. По-големите финансови субекти разполагат с повече ресурси, поради което само тези, които не са определени като микропредприятия, трябва да бъдат задължени да въведат сложни управленски механизми, да предвидят специални управленски функции, да извършват обстойна оценка след съществени промени в инфраструктурата на мрежите и информационните системи, редовно да проучват риска при използваните традиционни системи на ИКТ, да включат в тестването на непрекъснатостта на дейността и на плановете за ответни действия и възстановяване на информацията сценарии за преминаване от първичната инфраструктура на ИКТ към възпроизвеждащите я системи и т.н. Освен това само финансовите субекти, определени като значими за целите на обстойното тестване на устойчивостта на цифровите технологии, трябва да бъдат задължени да тестват проникването.

Независимо от този широк обхват, той не е изчерпателен. По-специално, настоящият регламент не обхваща системните оператори, както са определени в член 2, буква п) от Директива 98/26/ЕО[22] относно окончателността на сетълмента в платежните системи и в системите за сетълмент на ценни книжа (Директива за окончателността на сетълмента — ДОС), нито системните участници — освен ако не са финансови субекти, уредени на равнището на Съюза и следователно обхванати от настоящия регламент (т.е. кредитни институции, инвестиционни посредници, ЦК). Извън обхвата остава и регистърът на ЕС на квотите за емисии, който по силата на Директива 2003/87/ЕО[23] се администрира под егидата на Европейската комисия.

Тези изключения от ДОС се налагат поради необходимостта от допълнителен преглед на правните и политическите въпроси при системните оператори и системните участници по ДОС, като същевременно надлежно се отчита ефектът на правните

[22] 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).

[23] Директива 2003/87/ЕО на Европейския парламент и на Съвета от 13 октомври 2003 г. за установяване на схема за търговия с квоти за емисии на парникови газове в рамките на Общността и за изменение на Директива 96/61/ЕО на Съвета (ОВ L 275, 25.10.2003 г., стр. 32).

норми, понастоящем приложими за платежните системи[24], управлявани от централните банки. Тези въпроси могат да включват аспекти, които са отвъд въпросите, предмет на настоящия регламент, поради което Комисията ще продължи да оценява доколко е необходимо и какво въздействие би имало едно разширяване на обхвата на настоящия регламент с включването на понастоящем стоящите извън този обхват субекти и инфраструктури на ИКТ.

Изисквания във връзка с управлението (член 4)

Настоящия регламент има за цел да сближи бизнес стратегиите на финансовите субекти с тяхното управление на риска при ИКТ. За тази цел от ръководния орган ще се изиска да има възлова, активна роля в ръководенето на рамката за управление на риска при ИКТ и да се стреми към спазване на строга киберхигиена. Пълната отговорност на ръководния орган за управляването на риска при ИКТ за финансовия субект ще бъде основополагащ принцип, който ще бъде по-нататък претворен в набор от конкретни изисквания — ясно определяне на ролите и отговорности за всички функции, свързани с ИКТ, постоянно участие в текущия контрол на управлението на риска при ИКТ и във всички процеси на одобрение и контрол, както и подходящо разпределяне на инвестициите в ИКТ и на съответните обучения.

Изисквания във връзка с управляването на риска при ИКТ (членове 5—14)

В духа на съвместното техническо становище на ЕНО оперативната устойчивост на цифровите технологии се корени в набор от основополагащи принципи и изисквания за рамката за управление на риска при ИКТ. Тези изисквания, в който са почерпени идеи от съответните международни, национални и секторни стандарти, насоки и препоръки, са структурирани около специфичните функции за управление на риска при ИКТ (установяване, защита и предотвратяване, откриване, ответни действия и възстановяване на информацията, обучение и задълбочаване на познанията, и комуникиране). С цел да разполагат със средства, съобразени с динамичния характер на киберзаплахите, финансовите субекти са задължени да въведат и поддържат надеждни системи и инструменти на ИКТ за свеждане до минимум на въздействието на риска при ИКТ, за постоянно установяване на всички източници на риск за ИКТ, за въвеждане на мерки за превенция и защита, за бързо откриване на необичайните дейности, за въвеждане, като част от политиката си за непрекъснатост на дейността, на специална и всеобхватна политика за непрекъснато функциониране на ИКТ и план за възстановяване на информацията при срив на ИКТ. Последните компоненти са необходими за бързото възстановяване на информацията след инцидент с ИКТ, в частност — кибератака, при ограничаване на щетите и безопасно възобновяване на дейността възможно най-бързо. Регламентът сам по себе си не налага специфична стандартизация, а по-скоро се основава на европейските и международно признатите технически стандарти и на най-добрите секторни практики — доколкото са в пълно съответствие с надзорните инструкции за използването и включването на такива международни стандарти. Настоящият регламент обхваща също целостта, безопасността и устойчивостта на физическите инфраструктури и оборудване, които поддържат съответните технологии и свързаните с ИКТ процеси и човешки ресурси, представлявайки част от цифровия отпечатък на дейността на даден финансов субект.

Уведомяване за инцидентите с ИКТ (членове 15—20)

[24] В частност Регламент (ЕС) № 795/2014 на Европейската централна банка от 3 юли 2014 г. относно надзорните изисквания за системно важните платежни системи.

Хармонизирането и оптимизирането на уведомяването за инцидентите с ИКТ се постига, първо, чрез общо изискване към финансовите субекти за внедряване на управленски процес за наблюдаване и регистриране на инцидентите с ИКТ, и след това — за класифицирането им по изложени в регламента и доусъвършенствани от ЕНО, по силата на мандат, критерии за определяне на праговете на същественост. Второ, компетентните органи биват уведомявани само за инцидентите с ИКТ, които се считат за съществени. Уведомяването следва да се извършва чрез общ образец и по разработена от ЕНО единна процедура. Финансовите субекти следва да подават първоначални уведомления и неокончателни и окончателни доклади, както и да уведомяват ползвателите и клиентите си за дадения инцидент, когато последният засяга или може да засегне финансовите им интереси. Компетентните органи следва да предоставят важните сведения за инцидентите на други институции или органи: на ЕНО, на ЕЦБ и на определените в изпълнение на Директива (ЕС) 2016/1148 единни звена за контакт.

С оглед на установяването на диалог между финансовите субекти и компетентните органи за свеждане до минимум на въздействието и набелязване на подходящите корективни мерки, уведомяването за съществените инциденти с ИКТ следва да бъде допълвано от предоставяни от компетентните органи обратна информация или надзорни насоки.

Накрая, ЕНО, ЕЦБ и ENISA следва да изготвят съвместен доклад за оценка на осъществимостта на централизиране на равнището на Съюза на уведомяването за инциденти чрез създаването на централен портал на ЕС за уведомяване от финансовите субекти за съществените инциденти с ИКТ.

Тестване на оперативната устойчивост на цифровите технологии (членове 21—24)

Степента на подготвеност, от гледна точка на киберсигурността, на оперативния капацитет и функциите, предвидени в рамката за управление на риска при ИКТ, трябва да бъдат периодично тествани, като тестването цели и да се установяват слабостите, недостатъците или пропуските, както и бързината, с която могат да бъдат предприети корективни мерки. Настоящият регламент предвижда изискванията за тестване на оперативната устойчивост на цифровите технологии да се прилагат съобразно размера, профила на стопанска дейност и профила на риска на отделните финансови субекти: въпреки че всички субекти следва да тестват инструментите и системите на ИКТ, обстойно тестване чрез тестване на проникването следва да се изисква само от тези, които компетентните органи (въз основа на изложените в настоящия регламент и доусъвършенствани от ЕНО критерии) са определили като значими и с рутинни ИКТ. С настоящия регламент се въвеждат и изисквания за лицата, провеждащи тестове, и за признаване в целия Съюза на резултатите от проведените тестове на проникването при финансовите субекти с дейност в няколко държави членки.

Риск при ИКТ, пораждан от трета страна (членове 25—39)

С регламента се цели да се установи надеждно наблюдаване на риска при ИКТ, пораждан от трета страна. Тази цел се постига, първо, чрез спазване от страна на финансовите субекти на принципни правила за наблюдаване на рисковете, които крият доставчиците трети страни на ИКТ. На второ място, настоящият регламент уеднаквява възловите елементи на предоставяното от доставчиците трети страни на ИКТ обслужване и на отношенията с тези доставчици. Тези елементи обхващат базовите аспекти, за които се счита, че са от решаващо значение, за да могат финансовите субекти неотклонно да проследяват риска при ИКТ, пораждан от трета страна, на всеки

етап от деловите отношения — сключване на договор, изпълнение на договора, прекратяване на договора и следдоговорни етапи.

По-специално договорите, уреждащи тези отношения, трябва да съдържат пълно описание на услугите, на местата, където ще бъдат обработвани данните, както и на нивото на обслужване; те трябва да съдържат количествени и качествени цели за ефективност, съответни разпоредби относно достъпността, наличността, целостта, сигурността и защитата на личните данни, както и гаранции за достъп, възстановяване и връщане в случай на несъстоятелност на дадения доставчик трета страна на услуги в областта на ИКТ, задължения за доставчиците трети страни на услуги в областта на ИКТ да осведомяват финансовите субекти, както и съответните срокове за това; в договорите трябва също така да е предвидено правото на достъп, проверка и одит от страна на финансовите субекти или от определени трети лица, ясни права за прекратяване на договорните отношения и съответни изходни стратегии. Освен това, поради факта, че някои от тези договорни елементи могат да бъдат стандартизирани, регламентът насърчава, без да задължава, да се използват стандартните договорни клаузи, които Комисията ще разработи за компютърните услуги „в облак“.

Накрая, с настоящия регламент се цели да се насърчи сближаването на надзорните подходи към риска при ИКТ, пораждан от трета страна, във финансовия сектор чрез създаването на съюзна надзорна рамка за възловите доставчици трети страни на услуги в областта на ИКТ. Чрез тази нова единна правна рамка този ЕНО, който бъде определен за водещ надзорник на даден възлов доставчик трета страна на услуги в областта на ИКТ, получава правомощия, благодарение на които доставчиците на технологични услуги с възлова роля за функционирането на финансовия сектор ще са обект на подходящо наблюдение на европейско равнище. Предвидената в настоящия регламент надзорна рамка се основава на съществуващата институционална структура при финансовите услуги, при която съвместният комитет на Европейските надзорни органи осигурява междусекторната координация по всички въпроси на риска при ИКТ в съответствие със задачите си в сферата на киберсигурността, подкрепян от съответния подкомитет (надзорен форум), който извършва подготвителната работа както за целите на решенията, касаещи отделни възлови доставчици трети страни на услуги в областта на ИКТ, така и на препоръките, отправяни към всички такива доставчици.

Обмен на информация (член 40)

С цел да се повиши осведомеността за риска при ИКТ, да се сведе до минимум неговото разпространение, да се засили оперативният капацитет на финансовите субекти за защита и техниките им за откриване на заплахи, регламентът позволява на същите да се договарят да обменят помежду си информация и разузнавателни сведения за киберзаплахи.

2020/0266 (COD)

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

(Текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейската централна банка[25],

като взеха предвид становището на Европейския икономически и социален комитет[26],

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) В цифровата ера информационните и комуникационните технологии (ИКТ) са в основата на сложни системи, използвани в ежедневните дейности на нашето общество. Те движат напред възлови икономически сектори като финансовите услуги и подобряват функционирането на единния пазар. От друга страна засилената цифровизация и взаимообвързаност засилват рисковете при ИКТ, което прави обществото като цяло — и в частност финансовата система — по-уязвимо на киберзаплахи и сривове на ИКТ. Въпреки че днес повсеместната употреба на системите на ИКТ и значителната цифровизация и свързаност са основен белег на всички дейности на финансовите субекти на Съюза, устойчивостта на цифровите технологии все още не е внедрена в достатъчна степен в оперативните им механизми.

(2) През последните десетилетия използването на ИКТ придоби възлова роля във финансовия сектор, като днес то е от решаващо значение за обичайното ежедневно функциониране на всички финансови субекти. Цифровизацията обхваща например плащанията, при които, за сметка на извършването им в брой и с използването на хартиен носител, все повече навлизат цифровите решения, но също и услугите за клиринг и сетълмент на ценни книжа, електронната и алгоритмичната търговия, операциите по кредитиране и финансиране, партньорското финансиране, присъждането на кредитен рейтинг, подписваческата застрахователна дейност, уреждането на застрахователни

[25] [*да се добави препратка*] ОВ C [...], [...] г., стр. [...].

[26] [*да се добави препратка*] ОВ C [...], [...] г., стр. [...].

претенции и вътрешните за дружествата операции. Цифровите технологии не само вече обслужват в значителна степен финансовия сектор; те доведоха до задълбочаване на взаимните връзки и зависимости както в рамките на самия сектор, така и с доставчици трети страни на инфраструктура и услуги.

(3) В доклада си от 2020 г. за системния киберриск[27] Европейският съвет за системен риск (ЕССР) отново подчерта, че наблюдаваната тясна взаимосвързаност между финансовите субекти, финансовите пазари и инфраструктурите на финансовите пазари, и в частност — взаимозависимостта на техните системи на ИКТ, може потенциално да представлява системна уязвимост, тъй като локализираните инциденти с ИКТ биха могли бързо, невъзпрепятствани от географските граници, да се разпространят от всеки от приблизително 22 000-те финансови субекта в Съюза[28] в цялата финансова система. Сериозните пробиви в използваните от финансовия сектор ИКТ са проблематични не само за самите финансови субекти. Те улесняват разпространяването по финансовите свързващи канали на локализирани уязвими места и потенциално са източник на неблагоприятни последици за стабилността на финансовата система на Съюза, като генерират загуба на ликвидност и общо недоверие във финансовите пазари.

(4) През последните години отговорните за политиките кадри на национално, европейско и международно равнище, регулаторните органи и органите по стандартизация се заеха с рисковете при ИКТ в опит да се повиши устойчивостта, да се установят стандарти и да се координира нормотворческата или надзорната дейност. На международно равнище Базелският комитет по банков надзор, Комитетът по плащанията и пазарните инфраструктури, Съветът за финансова стабилност, Институтът за финансова стабилност и съставляващите Г-7 и Г-20 държави се стремят да предоставят на компетентните органи и пазарните участници от различни юрисдикции инструменти за засилване на устойчивостта на техните финансови системи.

(5) Въпреки националните и европейските целеви политики и законодателни инициативи, рисковете при ИКТ продължават да са предизвикателство пред оперативната устойчивост, функционирането и стабилността на финансовата система на Съюза. Основната цел на реформата, последвала финансовата криза от 2008 г., бе да се засили финансовата устойчивост на финансовия сектор на Съюза и защити конкурентоспособността и стабилността на Съюза от икономическа, пруденциална и пазарна гледна точка. Въпреки че сигурността на ИКТ и устойчивостта на цифровите технологии са част от операционния риск, те останаха извън приоритетите на следкризисната нормотворческа програма, като

---

27 ESRB report Systemic Cyber Risk [Доклад на ЕССР за системния киберриск], февруари 2020 г., https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Според оценката на въздействието, придружаваща прегледа на европейските надзорни органи (SWD(2017) 308), съществуват около 5 665 кредитни институции, 5 934 инвестиционни посредници, 2 666 застрахователни предприятия, 1 573 институции за професионално пенсионно осигуряване, 2 500 дружества за управление на инвестиции, 350 пазарни инфраструктури (централни контрагенти, фондови борси, систематични участници, регистри на трансакции и многостранни системи за търговия), 45 агенции за кредитен рейтинг и 2 500 лицензирани платежни институции и институции за електронни пари. Това са общо около 21 233 субекта, като тук не се включват дружествата за колективно финансиране, регистрираните одитори и одиторските дружества, доставчиците на услуги за криптоактиви, нито администраторите на бенчмаркове.

бяха обхванати само в някои части на политиката на Съюза за регламентиране на финансовите услуги или само в няколко държави членки.

(6) В своя изготвен през 2018 г. План за действие в областта на финансовите технологии[29] Комисията подчерта, че финансовият сектор на Съюза трябва непременно да повиши устойчивостта си и в оперативен аспект, за да може да функционира добре, използваните от него технологии да бъдат сигурни, а пробивите в ИКТ и инцидентите с ИКТ да бъдат бързо преодолявани, така че да се постигне в целия Съюз ефективно и безпрепятствено предоставяне на финансови услуги, в т.ч. при напрегнати ситуации, без при това да се уронва доверието на потребителите и на пазара.

(7) През април 2019 г. Европейският банков орган (ЕБО), Европейският орган за ценни книжа и пазари (ЕОЦКП) и Европейският орган за застраховане и професионално пенсионно осигуряване (ЕОЗППО) (общо наричани „Европейските надзорни органи“ — „ЕНО“) съвместно публикуваха две технически становища, в които се призовава за съгласуван подход към риска при използваните във финансовия сектор ИКТ и се препоръчва да се засили оперативната устойчивост на цифровите технологии при финансовите услуги чрез секторно насочена инициатива на Съюза, която да е съизмерима с целта.

(8) Финансовият сектор на Съюза е обхванат от единна нормативна уредба и се управлява от европейска система за финансов надзор. Въпреки това разпоредбите относно оперативната устойчивост на цифровите технологии и сигурността на ИКТ все още не са напълно или хомогенно хармонизирани, въпреки че оперативната устойчивост на цифровите технологии е от основно значение за финансовата стабилност и целостта на пазара в цифровата ера, като е не по-малко важна от общите пруденциални или етични стандарти например. Поради това, при разработването на единната нормативна уредба и надзорната система следва да се предвиди и този компонент — като се разширят мандатите на финансовите надзорни органи, които имат за задача да наблюдават и защитават финансовата стабилност и целостта на пазара.

(9) Нормативните несъответствия и различията в строгостта на националните нормативни или надзорни подходи към риска при ИКТ пречат на единния пазар на финансови услуги, като затрудняват финансовите субекти с трансгранично присъствие безпрепятствено да упражняват свободата на установяване и на предоставяне на услуги. Това може да доведе и до нарушаване на конкуренцията между един и същ вид финансови субекти с дейност в различни държави членки. В частност в области като тестването на оперативната устойчивост на цифровите технологии — където хармонизацията на равнище Съюза е ограничена, или наблюдаването на риска при ИКТ, пораждан от трети страни — където такава изобщо няма, различията в резултат на планираните национални мерки биха могли допълнително да затруднят функционирането на единния пазар в ущърб на пазарните участници и финансовата стабилност.

[29] Съобщение на Комисията до Европейския парламент, Европейския съвет, Съвета, Европейската централна банка, Европейския икономически и социален комитет и Комитета на регионите „План за действие в областта на финансовите технологии — за по-конкурентоспособен и иновативен европейски финансов сектор, COM/2018/0109 final, https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A52018DC0109&qid=1604942964842

(10) Частичният подход на равнище Съюза към риска при ИКТ е източник на нормативни пропуски или препокривания във важни аспекти като уведомяването за инцидентите с ИКТ и тестването на оперативната устойчивост на цифровите технологии, както и на различия — вследствие на въвеждането на разнопосочни национални разпоредби или неефективното прилагане на припокриващи се изисквания. От това особено страдат интензивно ползващите ИКТ като финансовия сектор, тъй като технологичните рискове нямат граници, а финансовите услуги са в значителна степен трансгранични — в рамките на Съюза и извън него.

Финансовите субекти с трансгранична дейност или с няколко лицензa (например даден финансов субект може да има лиценз за банка, за инвестиционен посредник и за платежна институция, като всеки от тях е издаден от различен надзорен орган в една или няколко държави членки) се сблъскват с оперативни предизвикателства, когато желаят самостоятелно и по разходо-ефективен начин да управляват рисковете при ИКТ и да ограничават неблагоприятното въздействие на инцидентите с ИКТ.

(11) Единната нормативна уредба не е придружена от обща уредба на риска при ИКТ или на операционния риск, поради което фундаменталните изисквания за всички финансови субекти във връзка с оперативната устойчивост на цифровите технологии трябва да бъдат допълнително хармонизирани. Оперативният капацитет и общата устойчивост, които финансовите субекти ще изградят въз основа на тези фундаментални изисквания, за да преодоляват оперативните неизправности, ще допринесат за запазването на стабилността и целостта на финансовите пазари на Съюза и оттам — за осигуряването на висока степен на защита на инвеститорите и потребителите в Съюза. Предвид целта на настоящия регламент — да допринесе за гладкото функциониране на вътрешния пазар, той следва да се основава на член 114 от ДФЕС — както този член се тълкува в юриспруденцията на Съда на Европейския съюз.

(12) Стремежът при настоящия регламент е първо да се консолидират и подобрят изискванията за риска при ИКТ, които понастоящем са разпръснати в различни регламенти и директиви. Макар че тези правни актове на Съюза обхванаха основните категории финансов риск (кредитен риск, пазарен риск, кредитен риск от контрагента, риск във връзка с ликвидността, риск във връзка с етичните принципи на дейност), към момента на приемането им не бе възможно да се проучат всички компоненти на оперативната устойчивост. Когато изискванията във връзка с операционния риск се доразвиваха в тези правни актове на Съюза, за проучването на риска се предпочиташе често традиционен количествен подход (определяне на капиталово изискване за покриване на рисковете при ИКТ), вместо с оглед на повишаване на функционалната устойчивост да се предвидят специални качествени изисквания за оперативния капацитет с цел защита, установяване и ограничаване на инцидентите с ИКТ, възстановяване на информацията и възобновяване на обичайното функциониране — или да се създаде оперативен капацитет за уведомяване за тези инциденти или за тестване на цифровите технологии. С тези директиви и регламенти се целеше най-вече да се въведат базовите норми за пруденциалния надзор, целостта на пазара или етичните принципи.

От своя страна настоящата инициатива консолидира и актуализира нормите за риска при ИКТ, като за първи път всички разпоредби относно цифровия риск във финансовия сектор ще бъдат обединени в единен законодателен акт. Така тя

би следвало да запълни пропуските или да отстрани несъответствията в някои от тези правни актове, в т.ч. по отношение на използваната в тях терминология, и изрично да въведе риска при ИКТ чрез специални норми за оперативния капацитет за управление на риска при ИКТ, за уведомяването и тестването, както и за наблюдаването на риска, пораждан от трета страна.

(13) В мерките си във връзка с риска при ИКТ финансовите субекти следва да спазват един и същ подход и принципни правила. Със съгласуваността се засилва доверието във финансовата система и се съхранява нейната стабилност, особено във времена на прекомерна употреба на системите, платформите и инфраструктурите на ИКТ, която повишава риска при цифровите технологии.

Освен това спазването на базови правила за киберсигурност следва да сведе до минимум сривовете на ИКТ и свързаните с тях разходи и оттам — да спести на икономиката значителни средства.

(14) Правният акт под формата на регламент спомага за намаляване на нормативната сложност, насърчава сближаването на надзорните практики, повишава правната сигурност, а и допринася за намаляване на разходите за съблюдаване на изискванията — особено за финансовите субекти с трансгранична дейност, и за ограничаване на изкривяванията на конкуренцията. Ето защо изборът на регламент за създаване на обща уредба на оперативната устойчивост на цифровите технологии, използвани от финансовите субекти, е най-добрият начин за осигуряване на еднообразно и съгласувано прилагане от страна на финансовия сектор на Съюза на всички компоненти на управлението на риска при ИКТ.

(15) Освен финансовото законодателство, настоящата обща съюзна уредба на киберсигурността е Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета[30]. Сред седемте критични сектора, посочената директива се прилага и към три вида финансови субекти — кредитните институции, местата на търговия и централните контрагенти. В Директива (ЕС) 2016/1148 обаче е предвиден механизъм за установяване на национално равнище на операторите на основни услуги, поради което тя на практика обхваща само някои определени от държавите членки кредитни институции, места на търговия и централни контрагенти, които подлежат на нейните изисквания за сигурност на ИКТ и за уведомяване за инцидентите с ИКТ.

(16) Тъй като с настоящия регламент се засилва хармонизацията на аспектите, свързани с устойчивостта на цифровите технологии, като се въвеждат по-строги от предвидените в действащото финансово законодателство на Съюза изисквания за управление на риска при ИКТ и за уведомяване за инцидентите с ИКТ, това представлява и по-тясна хармонизация в сравнение с изискванията на Директива (ЕС) 2016/1148. Следователно настоящият регламент представлява *lex specialis* по отношение на Директива (ЕС) 2016/1148.

От решаващо значение е да се запази силната връзка между финансовия сектор и хоризонталната съюзна уредба на киберсигурността, за да се осигури съгласуваност с вече приетите от държавите членки стратегии за

[30] 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).

киберсигурност и да се позволи на надзорните органи на финансовия сектор да бъдат уведомявани за инцидентите с киберсигурността, засягащи другите обхванати от Директива (ЕС) 2016/1148 сектори.

(17) Финансовите субекти, посочени в Директива (ЕС) 2016/1148, следва да останат част от „екосистемата“ на тази директива (напр. групата за сътрудничество за МИС и екипите за реагиране при инциденти с киберсигурността — ЕРИКС), така че натрупаният от едни сектори опит в преодоляването на киберзаплахи да може ефективно да бъде внедряван и прилаган в други.

ЕНО и националните компетентни органи следва да могат да участват в обсъжданията на стратегическите цели и на техническите аспекти на работата на групата за сътрудничество за МИС, съответно да обменят информация и да продължават да сътрудничат с определените в изпълнение на Директива (ЕС) 2016/1148 единни звена за контакт. Компетентните органи по настоящия регламент следва също така да се допитват до определените в изпълнение на член 9 от Директива (ЕС) 2016/1148 национални ЕРИКС и да сътрудничат с тях.

(18) Важно е да се осигури съгласуваност и с Директивата за европейските критични инфраструктури (ЕКИ)[31], която понастоящем се преразглежда с цел да се подобри защитата и устойчивостта на критичните инфраструктури срещу заплахи, различни от киберзаплахите, като този преглед може потенциално да е от значение за финансовия сектор.

(19) Доставчиците на компютърни услуги „в облак“ са сред категориите доставчици на цифрови услуги, обхванати от Директива (ЕС) 2016/1148. Като такива те подлежат на последващ надзор от определените в изпълнение на посочената директива национални органи, като този надзор е ограничен до предвидените в посочения акт изисквания за сигурност на ИКТ и за уведомяване за инцидентите с ИКТ. Тъй като създадената с настоящия регламент надзорна рамка се прилага спрямо всички възлови доставчици трети страни на услуги в областта на ИКТ, в т.ч. спрямо доставчиците на компютърни услуги „в облак“, които предоставят услуги в областта на ИКТ на финансови субекти, тя следва да се приеме за допълваща надзора по Директива (ЕС) 2016/1148. Създадената с настоящия регламент надзорна рамка следва да обхваща и доставчиците на компютърни услуги „в облак“, докато няма хоризонтална неспецифична за конкретен сектор рамка на Съюза, с която се създава орган за надзор на цифровите услуги.

(20) С оглед на пълния контрол на риска при ИКТ финансовите субекти трябва да разполагат с мащабен функционален капацитет за стабилно и ефективно управление на този риск, както и със специални механизми и практики за уведомяване за инцидентите с ИКТ, за тестване на системите на ИКТ, контролите и процесите, както и за управление на риска при ИКТ, пораждан от трета страна. Стандартите за оперативната устойчивост на цифровите технологии във финансовата система следва да се повишат, като същевременно се предвиди съизмеримо прилагане на изискванията спрямо финансовите

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

субекти, които са микропредприятия по смисъла на Препоръка 2003/361/ЕО на Комисията[32].

(21) Националните таксономии и прагове за уведомяване за инцидентите с ИКТ варират значително. Макар постигането на общо разбиране въз основа на съответната работа на Агенцията на Европейския съюз за киберсигурност (ENISA)[33] и групата за сътрудничество за МИС за финансовите субекти по Директива (ЕС) 2016/1148 да не е невъзможно, по отношение на останалите финансови субекти все още има или могат да възникнат различни подходи към праговете и таксономиите. Това предполага наличието на множество изисквания, които финансовите субекти трябва да спазват, особено когато извършват дейност в няколко юрисдикции на Съюза или са част от финансова група. Освен това тези различия могат да попречат на създаването на допълнителни единни или централизирани съюзни механизми за ускоряване на уведомяването и за подпомагане на бързия и безпрепятствен обмен на информация между компетентните органи, което е от решаващо значение за противодействие на рисковете при ИКТ при мащабни атаки с потенциално системни последствия.

(22) С цел да се позволи на компетентните органи да изпълняват надзорните си функции, разполагайки с обстойна картина на естеството, честотата, значимостта и ефекта на инцидентите с ИКТ, както и за да се подобри обменът на информация между съответните публични органи, в т.ч. правоприлагащите органи и органите за преструктуриране, е необходимо да се въведат правни норми, така че изискванията за уведомяване за инцидентите с ИКТ да бъдат допълнени с изисквания, които понастоящем липсват в уредбата на финансовия подсектор, и да се премахнат, за да се намалят разходите, всички съществуващи припокривания и дублирания. Поради това изискванията за уведомяване за инцидентите с ИКТ трябва непременно да бъдат уеднаквени, като се изиска финансовите субекти да уведомяват само компетентните си органи. Освен това ЕНО следва да бъдат оправомощени да доопределят елементите, свързани с уведомяването за инцидентите с ИКТ: таксономия, времеви рамки, набори от данни, образци и приложими прагове.

(23) Изисквания за тестване на оперативната устойчивост на цифровите технологии има в някои финансови подсектори, но те са въведени в няколко национални уредби, които не са координирани помежду си, поради което третират различно едни и същи проблеми. Това води до дублиране на разходите за трансграничните финансови субекти и затруднява взаимното признаване на резултатите. Некоординираното тестване може следователно да разпокъса единния пазар.

(24) Освен това, когато не се изисква тестване, уязвимите места при даден финансов субект остават неразкрити, което повишава риска за него и оттам — за стабилността и целостта на целия финансов сектор. Без намеса от страна на Съюза, тестването на оперативната устойчивост на цифровите технологии ще продължи да бъде разпокъсано и без взаимно признаване на тестовите резултати

---

32 Препоръка на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

33 Вж. Таксономия на ENISA за класифициране на инцидентите, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

в отделните юрисдикции. Освен това, предвид слабата вероятност другите финансови подсектори да възприемат такива мерки в значим мащаб, те биха пропуснали потенциалната полза от разкриване на уязвимите места и рисковете, тестване на оперативния капацитет за защита и за непрекъснатост на дейността и повишено доверие от клиентите, доставчиците и търговските партньори. С цел да се отстранят подобни припокривания, различия и пропуски е необходимо да се установят изисквания с оглед на едно координирано тестване от финансовите субекти и компетентните органи, с което ще се улесни взаимното признаване на обстойните тестове, провеждани от значимите финансови субекти.

(25) Широкото използване от финансовите субекти на услугите в областта на ИКТ се дължи отчасти на необходимостта да се адаптират към нововъзникващата конкурентна цифрова световна икономика, да повишат ефективността на дейността си и да удовлетворят потребителското търсене. В последните години естеството и обхватът на това широко използване не спряха да се развиват и доведоха до намаляване на разходите за финансово посредничество, позволиха разширяването и разрастването на финансовите дейности и същевременно предложиха богат инструментариум, основан на ИКТ, за управление на сложните вътрешни процеси.

(26) Това широко използване на услугите в областта на ИКТ се вижда от сложните договорни условия, където договарянето на клаузите във връзка с пруденциалните стандарти или управляващите ги други регулаторни изисквания, или с ефективното упражняване на дадени договорени права, като например за достъп или за извършване на одити, често е проблематично за финансовите субекти. Освен това редица такива договори не предвиждат достатъчно гаранции с оглед на цялостното наблюдение на възложените на доставчик трета страна процеси и така не позволяват на финансовите субекти да оценяват рисковете при тези процеси. Също така, поради факта, че доставчиците трети страни на услуги в областта на ИКТ често предоставят стандартизирани услуги на различни видове клиенти, тези договори не винаги са съобразени с индивидуалните или специфичните нужди на даден представител на финансовия сектор.

(27) Въпреки наличието в някои законодателни актове на Съюза в областта на финансовите услуги на някои общи правила относно възлагането на дейности на външен изпълнител, проследяването на изпълнението на договорите не е залегнало в пълен вид в законодателството на Съюза. Докато няма ясни специални съюзни стандарти за договорите с доставчиците трети страни на услуги в областта на ИКТ, противодействието на външния източник на риска при ИКТ ще остане непълно. Това налага да се определят някои основни принципи, които да ръководят финансовите субекти при управлението на риска при ИКТ, пораждан от трета страна, както и набор от основни договорни права по отношение на няколко елемента на изпълнението и прекратяването на договорите с оглед на включването на някои минимални гаранции, благодарение на които финансовите субекти да могат ефективно да следят всички пораждани от трета страна рискове при ИКТ.

(28) Въпросите с риска при ИКТ, пораждан от трета страна, и зависимостта от доставчик трета страна на услуги в областта на ИКТ са третирани разнородно. Въпреки някои усилия по един специфичен въпрос — възлагането на дейности

на доставчик трета страна, като например препоръките от 2017 г. относно възлагането на дейности на доставчици на компютърни услуги „в облак“[34], системният риск, който може да възникне от експозицията на финансовия сектор към ограничен брой възлови доставчици трети страни на услуги в областта на ИКТ, почти не е разглеждан в законодателството на Съюза. Този пропуск на съюзно равнище се утежнява от липсата на специални мандати и инструменти, с които да се позволи на националните надзорни органи да придобият ясна представа за зависимостта от даден доставчик трета страна на услуги в областта на ИКТ и адекватно да следят рисковете, произтичащи от концентрацията на подобна зависимост.

(29) Предвид потенциалните системни рискове от разрастващата се практика на възлагане на дейности на доставчици трети страни на услуги в областта на ИКТ и от концентрацията на зависимостта от такива доставчици, както и недостатъчните национални механизми, позволяващи на надзорните органи на финансовия сектор да определят количествено и качествено последиците от рисковете при ИКТ, материализирали се при възлови доставчици трети страни на услуги в областта на ИКТ, и да противодействат на тези рискове, е необходимо да се създаде подходяща надзорна рамка на равнището на Съюза, с помощта на която дейностите на възловите за финансовите субекти доставчици трети страни на услуги в областта на ИКТ да бъдат неотклонно наблюдавани.

(30) Заплахите, свързани с ИКТ, се усъвършенстват и стават все по-сложни, поради което успехът на мерките за откриване и предотвратяване зависи до голяма степен от редовния обмен между финансовите субекти на разузнавателни сведения за заплахите и уязвимите места. Обменът на информация допринася за повишаване на осведомеността относно киберзаплахите, което от своя страна увеличава капацитета на финансовите субекти да не допускат превръщането на заплахите в реални инциденти и им позволява да овладяват по-добре последиците от инцидентите с ИКТ и да се възстановят от тях по-ефективно. При отсъствието на насоки на равнището на Съюза няколко фактора изглежда възпрепятстват обмена на разузнавателни сведения, сред които по-специално е несигурността доколко това е съвместимо със защитата на данните, антитръстовите норми и правилата за отговорността.

(31) Колебанията по въпроса за вида информация, която може да се обменя с останалите пазарни участници или с органите, които не са надзорни органи (например с ENISA — за аналитични цели, или с Европол — за целите на правоприлагането), водят до задържането на полезна информация. Обхватът и качеството на обмена на информация остават ограничени, фрагментарни — като полезни сведения се обменят предимно на местно равнище (чрез национални инициативи), и без съобразени с потребностите на интегрирания финансов сектор съгласувани механизми на равнището на Съюза за обмен на информация.

(32) Поради това финансовите субекти следва да се насърчават да използват колективно индивидуалните си знания и практически опит на стратегическо, тактическо и оперативно ниво, за да повишат оперативния си капацитет за адекватно оценяване, следене, защита и реагиране на киберзаплахите.

[34] Препоръки относно възлагането на дейности на доставчици на компютърни услуги „в облак“ (EBA/REC/2017/03), понастоящем отменени с Насоки на ЕБО относно споразуменията за възлагане на дейности на външен изпълнител (EBA/GL/2019/02).

Следователно е необходимо да се позволи на равнище Съюза да се въведат механизми, които позволяват да се договаря доброволен обмен на информация, който, когато се провежда в защитена среда, ще помага на финансовата общност да предотвратява и колективно да реагира на заплахи чрез бързо ограничаване на разпространението на рисковете при ИКТ и възпрепятстване на потенциалното разпространение на проблемите по финансовите канали. Тези механизми следва да се използват при пълно съблюдаване на приложимите правни норми на Съюза в областта на конкуренцията[35], както и по начин, който гарантира пълното спазване на нормите на Съюза относно защитата на данните и най-вече Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[36] — в частност при обработването на лични данни, необходимо с оглед на легитимния интерес на администратора или на трета страна — както е посочено в член 6, параграф 1, буква е) от същия регламент.

(33) Независимо от предвидения широк обхват на настоящия регламент, при прилагането на нормите относно оперативната устойчивост на цифровите технологии следва да се имат предвид значителните разлики между финансовите субекти по отношение на размера, профила на стопанска дейност или степента на изложеност на рисковете при цифровите технологии. Като общ принцип, когато отделят ресурси и оперативен капацитет за прилагане на нормите относно управлението на риска при ИКТ, финансовите субекти следва надлежно да съобразяват потребностите си, свързани с ИКТ, със своя размер и профил на стопанска дейност, а компетентните органи — постоянно да оценяват и преразглеждат подхода към такова разпределяне.

(34) По-големите финансови субекти потенциално разполагат с повече ресурси и могат бързо да мобилизират средства за създаването на управленски структури и провеждането на различни корпоративни стратегии, поради което по-сложни управленски механизми следва да се изискват само от финансовите субекти, които не са микропредприятия по смисъла на настоящия регламент. Такива субекти могат по-лесно да създадат специални управленски функции за надзор на споразуменията с доставчиците трети страни на услуги в областта на ИКТ или за управление на кризи, да организират управлението на риска при ИКТ според модела на трите защитни слоя или да приемат документ за човешките ресурси, в който изчерпателно се обяснява политиката относно правата на достъп.

По същата причина само от такива финансови субекти следва да се изисква след съществени инфраструктурни и процесуални промени в мрежите и информационните системи да извършват обстойни оценки, редовно да анализират риска при традиционните системи на ИКТ или да включат в тестването на непрекъснатостта на дейността и на плановете за ответни действия и възстановяване на информацията сценарии за преминаване от първичната инфраструктура на ИКТ към възпроизвеждащите я системи.

---

35 Съобщение на Комисията — Насоки относно приложимостта на член 101 от Договора за функционирането на Европейския съюз по отношение на споразуменията за хоризонтално сътрудничество (ОВ C 11, 14.1.2011 г., стр. 1).

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

(35) Освен това, предвид факта, че изискването за тестване на проникването следва да се отнася само за посочените финансови субекти, определени като значими за целите на обстойното тестване на оперативната устойчивост, едва малък процент от финансовите субекти следва да разполагат с административни процеси и да поемат финансови разходи във връзка с провеждането на такива тестове. Накрая, с цел да се намалят нормативните изисквания, само финансовите субекти, които не са микропредприятия, следва да са задължени редовно да уведомяват компетентните органи за разходите и загубите в резултат на неизправности на ИКТ, както и за резултатите от анализа на възникналите инциденти, довели до съществена неизправност на ИКТ.

(36) С оглед, от една страна, на постигането на пълно съответствие и обща съгласуваност на стратегиите на финансовите субекти за стопанската им дейност, а от друга — управляването на риска при ИКТ, от ръководния орган следва да се изиска да има водеща и активна роля в управлението и адаптирането на рамката за управление на риска при ИКТ и на цялостната стратегия за устойчивост на цифровите технологии. Подходът, който трябва да бъде възприет от ръководния орган, следва да бъде съсредоточен не само върху средствата за осигуряване на устойчивост на системите на ИКТ, а да обхваща и хората и процесите чрез набор от политики, които при всеки корпоративен слой, а и за целия персонал изграждат добра осведоменост за киберрисковете и стремеж за стриктно спазване във всички дейности на правилата за киберсигурност.

Крайната отговорност на ръководния орган за управлението на рисковете при ИКТ на финансовия субект следва да бъде основополагащ принцип на този цялостен подход и допълнително да се изразява в постоянния контрол върху управлението на риска при ИКТ.

(37) Пълната отчетност на ръководния орган върви ръка за ръка и с осигуряването на такива инвестиции в ИКТ и общ бюджет на финансовия субект, които са съобразени с базовата за него цел за оперативна устойчивост.

(38) С настоящия регламент, в който са почерпени идеи от съответните международни, национални и секторни стандарти, насоки, препоръки или подходи за управление на киберриска[37], се насърчава набор от функции, които улесняват цялостното структуриране на управлението на риска при ИКТ. Докато финансовите субекти поддържат основен оперативен капацитет, съобразен със заложените в настоящия регламент цели на функциите (установяване, защита и предотвратяване, откриване, ответни действия и възстановяване на информацията, обучение и задълбочаване на познанията, и комуникиране), структурирането или категоризирането на използваните от тях модели за управление на риска при ИКТ остават техен прерогатив.

(39) С цел да разполагат със средства, съобразени с динамичния характер на киберзаплахите, финансовите субекти следва да поддържат актуални и

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; NIST Cybersecurity Framework, https://www.nist.gov/cyberframework; FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

надеждни системи на ИКТ, които не само разполагат с достатъчен капацитет за обработване на данните — което е необходимо за предоставяните от тези субекти услуги, а и са технически устойчиви, така че да могат адекватно да удовлетворяват необходимостта за финансовите субекти от обработване на допълнителна информация при неблагоприятни пазарни условия или други проблематични ситуации. В настоящият регламент не е предвидено да се стандартизират специфични системи, инструменти или технологии на ИКТ, тъй като се разчита, че финансовите субекти ще използват подходящо европейските и международно признатите технически стандарти (напр. ISO) или най-добрите секторни практики, доколкото такова използване е напълно съобразено със специалните надзорни инструкции за използване и въвеждане на международни стандарти.

(40) Финансовите субекти трябва да разполагат с ефективни планове за непрекъснатост на дейността и за възстановяване на информацията, така че да могат бързо да реагират на инцидентите с ИКТ, и в частност на кибератаките, и да ги разрешават, ограничавайки щетите и давайки приоритет на възобновяването на дейностите и мерките за възстановяване на информацията. Въпреки че системите за съхраняване на резервни копия на данните следва да се задействат без неоправдано забавяне, това не следва по никакъв начин да застрашава целостта и сигурността на мрежите и информационните системи, нито поверителността на данните.

(41) Настоящият регламент оставя на финансовите субекти да определят гъвкаво целевите си срокове за възстановяване на информацията, с което им позволява да определят целите си, съобразявайки се изцяло с естеството и значението на съответната функция, както и с евентуалните специфични потребности на стопанската дейност, като обаче при определянето на тези цели следва да се изисква оценка на потенциалното общо въздействие върху пазарната ефективност.

(42) Последиците от кибератаките са по-съществени във финансовия сектор — област, която е застрашена в много по-голяма степен от злонамерени разпространители, които преследват финансова изгода пряко от източника. С цел да се ограничат тези рискове и да не се допусне да се загуби целостта на системите на ИКТ или достъпът до тях, да се откраднат поверителни данни или да се нанесе повреда на физическата инфраструктура на ИКТ, уведомяването от финансовите субекти за инцидентите с ИКТ следва да се подобри значително.

Уведомяването за инцидентите с ИКТ следва да бъде хармонизирано за всички финансови субекти, като от тях се изиска да уведомяват само компетентните си органи. Въпреки че задължението за уведомяване ще обхваща всички финансови субекти, то не следва да се прилага еднакво към всички: следва да бъдат предвидени съответни прагове на същественост и срокове, така че да се обхванат само съществените инциденти с ИКТ. Прякото уведомяване ще осигури на надзорните органи достъп до информацията за инцидентите с ИКТ. Въпреки това надзорните органи на финансовия сектор следва да предават тази информация на публичните органи извън тази област (компетентните органи за МИС, националните органи за защита на данните, както и правоприлагащите органи — за инцидентите с престъпен характер). Сведенията за инцидентите с ИКТ следва да бъдат предавани по веригата: надзорните органи на финансовия сектор следва да предоставят цялата необходима обратна информация или насоки на финансовия субект, а ЕНО следва да споделят анонимни данни за

заплахите и слабите места, свързани с дадено събитие, с цел да се подпомогне по-широко колективно противодействие.

(43) Следва допълнително да се проучи възможността за централизиране на уведомяването за инцидентите с ИКТ чрез централен портал на ЕС, който пряко да получава съответните уведомления и автоматично да уведомява националните компетентни органи или да изпълнява координационни функции, като само централизира уведомленията, изпращани от националните компетентни органи. От ЕНО следва да се изиска до дадена дата да изготвят, като се допитат до ЕЦБ и ENISA, съвместен доклад за осъществимостта на създаването на такъв централен портал на ЕС.

(44) С цел да се постигне стабилна оперативна устойчивост и в съответствие с международните стандарти (напр. изложените от Г-7 базови елементи на тестването на проникването — ТП), финансовите субекти следва редовно да тестват доколко ефективно системите им на ИКТ и персоналът им са способни да предотвратяват, откриват и реагират на инциденти с ИКТ, а и да възстановяват информацията, както и да установяват и премахват потенциалните уязвими места на ИКТ. Предвид различната степен на подготвеност по отношение на киберсигурността на финансовите субекти — в различните финансови подсектори, а и в рамките на един и същ подсектор, тестването следва да съдържа широк набор от аспекти и действия, вариращи от оценяване на базовите изисквания (оценка и сканиране на уязвимите места, анализ на източниците с отворен достъп, оценка на сигурността на мрежата, анализ на пропуските, физически преглед на сигурността, анкета и сканиране на програмните продукти, когато е осъществимо — преглед на изходния код, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането или тестване по цялата верига и др.) до обстойно тестване (напр. ТП от финансовите субекти, чиито ИКТ са достатъчно рутинни, за да го позволяват). Поради това тестването на оперативната устойчивост на цифровите технологии следва да бъде по-обстойно при значимите финансови субекти (големи кредитни институции, фондови борси, централни депозитари на ценни книжа, централни контрагенти и др.). От друга страна тестването на оперативната устойчивост на цифровите технологии следва също така да бъде по-наложително за някои подсектори с основна системна роля (плащания, банково дело, клиринг, сетълмент и др.) и по-малко — за други подсектори (управители на активи, агенции за кредитен рейтинг и др.). Финансовите субекти с трансгранична дейност, които упражняват свободата си на установяване или предоставяне на услуги в Съюза, следва да спазват единен набор от изисквания за обстойно тестване (например ТП) в своята държава членка по произход, като на такова тестване следва да подлежат инфраструктурите на ИКТ във всички юрисдикции в Съюза, където трансграничната група извършва дейност, което означава, че тази група ще има разходи за тестване само в една юрисдикция.

(45) С оглед на надеждното наблюдаване на риска при ИКТ, пораждан от трета страна, е необходимо да се установи набор от принципни правила, които да ориентират финансовите субекти при наблюдаването на рисковете, възникващи при възлагането на функции на доставчици трети страни на услуги в областта на ИКТ и в по-общ план — при зависимост от такива доставчици.

(46) Финансовите субекти следва да носят пълната отговорност за спазването на задълженията по настоящия регламент. Рискът при доставчиците трети страни на услуги в областта на ИКТ следва да бъде обект на съобразен с естеството му

анализ, при който надлежно да се прецени степента, комплексният характер и значимостта на зависимостта от такива доставчици, както и значението — възлово или не — на договорените услуги, процеси или функции, а в принципен аспект — като обстойно се проучи потенциалното въздействие върху непрекъснатостта и качеството на финансовите услуги, предоставяни от отделния субект или според случая — групата.

(47) Подходът към риска при доставчиците трети страни на услуги в областта на ИКТ следва да е стратегически и да е залегнал в специална приета от ръководния орган на финансовия субект стратегия за неотклонно проследяване на всяка зависимост от такива доставчици. С цел да повишат осведомеността си за зависимостта от доставчици трети страни на услуги в областта на ИКТ и с оглед на засилването на създадената с настоящия регламент надзорна рамка, надзорните органи на финансовия сектор следва редовно да получават най-важните сведения от регистрите и да могат когато преценят да искат извадки от тях.

(48) Формалното сключване на договор следва да се крепи на предварителен обстоен анализ, а разтрогването — поне на набор от обстоятелства, които са белег на слабости при доставчика трета страна на услуги в областта на ИКТ.

(49) С цел да се противодейства на системния ефект на риска от концентрация, свързан с доставчици трети страни на услуги в областта на ИКТ, следва да се насърчава балансирано решение в резултат на гъвкав и постепенен подход, тъй като строгите тавани или ограничения могат да попречат на стопанската инициатива и свободата на договаряне. Финансовите субекти следва да извършват задълбочена оценка на договорите, за да определят вероятността от възникване на такъв риск, в т.ч. чрез обстойно проучване на споразуменията за възлагане на дейности на подизпълнител, особено когато са сключени с установени в трета държава доставчици трети страни на услуги в областта на ИКТ. На този етап и с оглед на постигането на равновесие между нуждата да се запази свободата на договаряне и тази да се гарантира финансова стабилност, определянето на строги тавани и ограничения на експозициите към доставчици трети страни на услуги в областта на ИКТ не се смята за уместно. ЕНО, определен да надзирава даден възлов доставчик трета страна на услуги в областта на ИКТ („водещ надзорен орган“), следва при изпълнението на надзорните си задачи да обръща особено внимание на задълбоченото познаване на мащаба на взаимозависимостите и да установява конкретните случаи, при които високата концентрация на възлови доставчици трети страни на услуги в областта на ИКТ в Съюза е възможно да окаже натиск върху стабилността и целостта на финансовата система на Съюза, като при установяването на такъв риск започне диалог със съответния възлов доставчик[38].

(50) С цел да се позволи на финансовите субекти редовно да оценяват и наблюдават доколко доставчиците трети страни на услуги в областта на ИКТ са способни да предоставят услуги по сигурен начин и без неблагоприятни последици за тяхната устойчивост, базовите елементи на изпълнение на договорите с такива

[38] Освен това, ако възникне риск от злоупотреба с господстващо положение от страна на възлов доставчик трета страна на услуги в областта на ИКТ, самите финансови субекти следва да могат да подадат официална или неофициална жалба до Европейската комисия или до националните органи за защита на конкуренцията.

доставчици следва да бъдат хармонизирани. Тези елементи се отнасят само до минимален брой договорни аспекти, за които се смята, че са от решаващо значение за осигуряването на финансовия субект на възможност изцяло да наблюдава стабилността и сигурността на предоставяните му услуги в областта на ИКТ, предвид факта, че устойчивостта на използваните от него цифрови технологии зависи от тези параметри.

(51) С цел да се позволи на финансовия субект да наблюдава процеса ефективно, в договорите следва в частност да се описват подробно функциите и услугите, местата, където се предоставят такива функции и се обработват данните, както и нивото на обслужване, заедно с количествени и качествени целеви показатели за ефективност в рамките на това договорено ниво на обслужване. В същия дух, за елементи от решаващо значение за възможността на финансовия субект да наблюдава риска при даден доставчик трета страна на услуги в областта на ИКТ следва да се смятат и клаузите относно достъпността, наличността, целостта, сигурността и защитата на личните данни, както и гаранциите за достъп, възстановяване и връщане при несъстоятелност, преструктуриране или прекратяване на дейността на този доставчик.

(52) С цел да се позволи на финансовите субекти да контролират изцяло всички събития, които могат да накърнят сигурността на техните системи на ИКТ, доставчикът трета страна на услуги в областта на ИКТ следва да бъде задължен да уведомява в съответни срокове за събитията, които потенциално могат съществено да засегнат способността му ефективно да изпълнява възлови или важни функции, в т.ч. да предоставя поддръжка при инцидент с ИКТ, без това да води за финансовия субект до допълнителни — или над предварително определените — разходи.

(53) Правото на финансовия субект или на определена трета страна за достъп, проверка и одит на доставчика трета страна на услуги в областта на ИКТ, както и пълното сътрудничество на последния по време на проверките, са от решаващо значение за текущото наблюдение на ефективността на този доставчик. Компетентният орган на финансовия субект би следвало също да има тези права на проверка и одит на доставчика трета страна на услуги в областта на ИКТ, при съответното уведомяване на този доставчик и спазване на поверителност.

(54) В договорите следва да е ясно предвидено правото на прекратяване и съответни минимални изисквания за известяване, както и специална изходна стратегия, с оглед по-специално на определянето на задължителни преходни периоди, по време на които доставчиците трети страни на услуги в областта на ИКТ следва да продължат да предоставят съответните функции, така че да се ограничи рискът за финансовия субект от нарушаване на обичайното функциониране или да му се позволи безпрепятствено да започне да използва услугите на други такива доставчици или собствени разработени решения — в зависимост от степента на сложност на предоставяната услуга.

(55) Освен това една възможност за прибягване до стандартните договорни клаузи, разработени от Комисията за компютърните услуги „в облак“, може допълнително да успокои финансовите субекти и техните доставчици трети страни на услуги в областта на ИКТ, тъй като ще се повиши правната сигурност относно използването от финансовия сектор на компютърни услуги „в облак“ при пълно съобразяване с изискванията и очакванията, предвидени във финансовото законодателство. Работата по този въпрос се основава на вече

очертаните мерки в Плана за действие в областта на финансовите технологии от 2018 г., в който Комисията обяви намерението си да насърчава и улеснява разработването на стандартни договорни клаузи за целите на използването от финансовите субекти на компютърни услуги „в облак“, предоставяни от доставчик трета страна, въз основа на работата на заинтересованите страни от редица сектори в областта на тези услуги, която Комисията подпомогна, като улесни участието на финансовия сектор.

(56) С цел да се насърчи сближаването на надзорните подходи към пораждания от трета страна риск при ИКТ за финансовия сектор и да се повиши ефективността на тези подходи, да се засили оперативната устойчивост на цифровите технологии при финансовите субекти, които за изпълнението на оперативните си функции се осланят на възлови доставчици трети страни на услуги в областта на ИКТ, и оттам — да се допринесе за съхраняването на стабилността на финансовата система на Съюза и за целостта на единния пазар на финансови услуги, възловите доставчици трети страни на услуги в областта на ИКТ следва да бъдат обект на надзорна рамка на равнището на Съюза.

(57) С оглед на прилагането на тази съюзна надзорна рамка и поради факта, че специално третиране е необходимо само за възловите доставчици трети страни на услуги в областта на ИКТ, следва да се въведе механизъм за определянето им в зависимост от измерението и естеството на зависимостта на финансовия сектор от тях, измерени по набор от количествени и качествени критерии — които ще поставят определящите възловия характер параметри в основата на надзора. Следователно възловите доставчици трети страни на услуги в областта на ИКТ, които не са автоматично определени в резултат на прилагането на горепосочените критерии, следва да могат по своя воля да се включат към надзорната рамка, като съответно от нея бъдат изключени тези, които вече са обект на надзорните механизми, установени на равнището на Евросистемата с оглед на задачите по член 127, параграф 2 от Договора за функционирането на Европейския съюз.

(58) Изискването за определените като възлови доставчици трети страни на услуги в областта на ИКТ да бъдат учредени в Съюза не води до локализиране на данните, тъй като настоящият регламент не изисква допълнително съхраняването или обработването на данните да се извършва в Съюза.

(59) Тази рамка не следва да засяга компетентността на държавите членки да провеждат собствени надзорни мисии на доставчиците трети страни на услуги на ИКТ, които не са определени като възлови съгласно настоящия регламент, но биха могли да се смятат за важни в национален аспект.

(60) За да се използва настоящата многопластова институционална структура в областта на финансовите услуги, съвместният комитет на ЕНО следва, в съответствие със своите задачи в областта на киберсигурността, да продължи да осигурява цялостната междусекторна координация по всички въпроси на риска при ИКТ, като бъде подкрепен от нов подкомитет (Надзорният форум), който да извършва подготвителната работа както за целите на решенията, касаещи отделни възлови доставчици трети страни на услуги в областта на ИКТ, така и на препоръките, отправяни към всички такива доставчици, по-специално във връзка със сравнителния анализ на програмите за надзор на възловите доставчици трети страни на услуги в областта на ИКТ и с определянето на най-добрите практики с оглед на рисковете от концентрация на такива доставчици.

(61) С оглед на адекватния надзор на равнището на Съюза върху възловите за функционирането на финансовия сектор доставчици трети страни на услуги в областта на ИКТ, за всеки такъв доставчик следва да бъде определен водещ надзорник измежду ЕНО.

(62) Водещите надзорници следва да разполагат с необходимите правомощия за разследвания, проверки на място и от разстояние на възловите доставчици трети страни на услуги в областта на ИКТ, както и с достъп до всички съответни помещения и места, както и да получават пълна и актуална информация с цел да имат реална представа за вида, мащаба и въздействието на риска при ИКТ, пораждан от трета страна, за финансовите субекти и в общ план — за финансовата система на Съюза.

Възлагането на ЕНО на водещия надзор е предпоставка за разбирането и анализирането на системното измерение на риска при ИКТ във финансовия сектор. Присъствието, което имат в Съюза възловите доставчици трети страни на услуги в областта на ИКТ, и свързаните с него потенциални рискове от концентрация на такива доставчици налагат общ подход на равнището на Съюза. Множеството одити и права за достъп, прерогатив на множество компетентни органи, работещи малко или повече изолирано един от друг, възпрепятстват обстойното проучване на риска при ИКТ, пораждан от трета страна, а и същевременно създават ненужни дублирания, тежест и сложност за възловите доставчици трети страни на услуги в областта на ИКТ, които са изправени пред подобни многобройни искания.

(63) Освен това водещите надзорници следва да могат да отправят препоръки относно рисковете при ИКТ и подходящите защитни средства, в т.ч. да се противопоставят на определени договори, които като краен резултат влияят върху стабилността на финансовия субект или на финансовата система. Националните компетентни органи следва надлежно да отчитат такива съществени препоръки на водещите надзорници при упражняването на пруденциален надзора върху финансовите субекти.

(64) Надзорната рамка не заменя, нито по някакъв начин премахва необходимостта от управление от страна на финансовите субекти на риска при доставчиците трети страни на услуги в областта на ИКТ — в т.ч. задължението за текущо наблюдение на сключените договори с възлови доставчици трети страни на услуги в областта на ИКТ, нито засяга пълната отговорност на финансовите субекти за спазването на всички изисквания на настоящия регламент и съответното финансово законодателство. С цел да се избегнат дублиранията и припокриванията, компетентните органи следва да не предприемат индивидуални мерки за наблюдаване на риска при доставчиците трети страни на услуги в областта на ИКТ. Такива мерки следва да бъдат предварително съгласувани и възприети при надзорната рамка.

(65) С цел да се насърчи сближаването в международен план на най-добрите практики, които да се използват при прегледа на начина, по който доставчиците трети страни на услуги в областта на ИКТ управляват риска при цифровите технологии, ЕНО следва да бъдат насърчавани да сключват споразумения за сътрудничество със съответните надзорни и регулаторни органи от трети държави, за да се улесни разработването на най-добри практики за противодействие на риска при ИКТ, пораждан от трета страна.

(66) С цел да се използва техническият опит на експертите на компетентните органи в управлението на операционния риск и на риска при ИКТ, водещите надзорници следва да използват националния надзорен опит и да създадат специални анализаторски екипи за всеки възлов доставчик трета страна на услуги в областта на ИКТ, като приобщят екипи от различни области за подпомагане на подготовката и практическото упражняване на надзора, в т.ч. проверки на място на възловите доставчиците трети страни на услуги в областта на ИКТ, както и необходимите последващи действия.

(67) Компетентните органи следва да разполагат с всички необходими правомощия за надзор, разследване и санкциониране с оглед на прилагането на настоящия регламент. Административните санкции следва по принцип да се публикуват. Финансовите субекти и доставчиците трети страни на услуги в областта на ИКТ могат да бъдат установени в различни държави членки и да бъдат поднадзорни на различни секторни компетентни органи, поради което съответните компетентни органи следва тясно да сътрудничат помежду си, а и с ЕЦБ — за възложените ѝ специфични задачи от Регламент (ЕС) № 1024/2013 на Съвета[39], както и да се допитват до ЕНО чрез взаимен обмен на сведения и взаимопомощ при надзорните действия.

(68) С оглед на количественото и качественото уточняване на критериите за определяне на възловите доставчици трети страни на услуги в областта на ИКТ и на хармонизирането на надзорните такси, Комисията следва да бъде оправомощена да приема актове по силата на член 290 от Договора за функционирането на Европейския съюз за доуточняване на следните въпроси: системното въздействие, което срив при доставчик трета страна на услуги в областта на ИКТ може да има върху обслужваните от него финансови субекти; броя на глобалните системно значими институции (Г-СЗИ) или другите системно значими институции (Д-СЗИ), които се осланят на даден доставчик трета страна на услуги в областта на ИКТ; броя на извършващите дейност на даден пазар доставчици трети страни на услуги в областта на ИКТ; разходите за преминаване към друг доставчик трета страна на услуги в областта на ИКТ; броя на държавите членки, в които даден доставчик трета страна на услуги в областта на ИКТ предоставя услуги и в които извършват дейност използващите услугите му финансови субекти; както и размера на надзорните такси и начина на плащането им.

Особено важно е по време на подготвителната си работа Комисията да проведе подходящи консултации, в т.ч. с експерти, и тези консултации да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г.[40] По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът получават всички документи едновременно с експертите от държавите членки, като техните експерти получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

---

[39] 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).

[40] ОВ L 123, 12.5.2016 г., стр. 1.

(69) С настоящия регламент и с Директива (ЕС) 20xx/xx на Европейския парламент и на Съвета[41] се консолидират разпоредбите относно управлението на риска при ИКТ в множество действащи регламенти и директиви в областта на финансовите услуги, в т.ч. регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012 (ЕС) № 600/2014 и (ЕС) № 909/2014, поради което с оглед на пълната съгласуваност посочените регламенти следва да бъдат изменени, за да се поясни, че съответните разпоредби относно риска при ИКТ се съдържат в настоящия регламент.

Техническите стандарти следва да осигурят повсеместно хармонизиране на въведените с настоящия регламент изисквания. ЕНО разполагат с високоспециализиран експертен опит, поради което разработването и последващото предоставяне на Комисията на проекти на регулаторни технически стандарти, при които не се разглежда изборът на дадена политика, следва да бъде възложено на тях. Регулаторни технически стандарти следва да бъдат разработени за управлението на риска при ИКТ, уведомяването, тестването и базовите изисквания за надеждно наблюдаване на риска при ИКТ, пораждан от трета страна.

(70) Особено важно е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително с експерти. Комисията и ЕНО следва да съобразят прилагането на тези стандарти и изисквания с естеството, мащаба и сложността на финансовите субекти и техните дейности.

(71) С цел да се улесни сравнимостта на уведомленията за съществените инциденти с ИКТ и да се осигури прозрачност на договорите за услуги в областта на ИКТ, предоставяни от доставчик трета страна на такива услуги, на ЕНО следва да бъде възложено да разработят проекти на технически стандарти за изпълнение, с които да се установят стандартизираните образци, формуляри и процедури, които финансовите субекти да използват за уведомяване за съществените инциденти с ИКТ, както и стандартизираните образци за информационния регистър. При разработването на тези стандарти ЕНО следва да вземат предвид размера и сложността на финансовите субекти, а така също и естеството на техните дейности и риска, който те крият. В съответствие с член 15 съответно от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010 Комисията следва да бъде оправомощена да приеме въпросните технически стандарти за изпълнение чрез актове за изпълнение по член 291 от ДФЕС. Тъй като допълнителните изисквания вече са заложени в делегираните актове и актовете за изпълнение, основани на техническите регулаторни стандарти и техническите стандарти за изпълнение съответно в регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014 и (ЕС) № 909/2014, на ЕНО е целесъобразно да се възложи, индивидуално или съвместно чрез Съвместния комитет, да представят на Комисията регулаторни технически стандарти и технически стандарти за изпълнение за приемане на делегираните актове и актовете за изпълнение, които внедряват и актуализират съществуващите разпоредби относно управлението на риска при ИКТ.

(72) Това ще доведе до последващо изменение на съществуващите делегирани актове и актове за изпълнение, приети в различни сфери на финансовото законодателството. Обхватът на членовете относно операционния риск, въз основа на които предвидените в посочените актове правомощия обусловиха

[41] [*Да се въведе пълната препратка*]

приемането на делегирани актове и актове за изпълнение, следва да бъде изменен с оглед на внедряването в настоящия регламент на всички разпоредби относно оперативната устойчивост на цифровите технологии, които понастоящем са част от посочените регламенти.

(73) Тъй като целта на настоящия регламент — постигане на значителна оперативна устойчивост на цифровите технологии при всички финансови субекти, не може да бъде постигната в достатъчна степен от държавите членки, тъй като налага да се хармонизират множество разнородни правила в сила в някои актове на Съюза или в правните системи на държавите членки, а поради мащаба и въздействието си може да се постигне по-добре на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

1. С настоящия регламент се установяват единните изисквания за сигурността на мрежите и информационните системи в основата на стопанските процеси на финансовите субекти — необходими за постигането на високо общо равнище на оперативна устойчивост на цифровите технологии, както следва:

а) изисквания към финансовите субекти във връзка със:

– управлението на риска при информационните и комуникационните технологии (ИКТ);

– уведомяването на компетентните органи за съществените инциденти с ИКТ;

– тестването на оперативната устойчивост на цифровите технологии;

– обмена на информация и разузнавателни сведения за киберзаплахите и уязвимите места;

– мерките за стабилно управление от страна на финансовите субекти на риска при ИКТ, пораждан от трети страни;

б) изискванията във връзка с договорите между доставчиците трети страни на услуги в областта на ИКТ и финансовите субекти;

в) надзорната рамка за възловите доставчици трети страни на услуги в областта на ИКТ, предоставящи такива услуги на финансовите субекти;

г) правилата за сътрудничеството между компетентните органи, както и за надзора и правоприлагането от компетентните органи по всички обхванати от настоящия регламент въпроси.

2. По отношение на финансовите субекти, определени като оператори на основни услуги в националните разпоредби, с които се транспонира член 5 от Директива (ЕС) 2016/1148, настоящият регламент се смята, за целите на член 1, параграф 7 от посочената директива, за специален за сектора правен акт на Съюза.

Член 2

Индивидуален обхват

1. Настоящият регламент се прилага спрямо следните субекти:

а) кредитни институции;

б) платежни институции;

в) институции за електронни пари;

г) инвестиционни посредници;

д) доставчици на услуги за криптоактиви, емитенти на криптоактиви, емитенти на токени, обезпечени с активи, и емитенти на значими токени, обезпечени с активи;

е) централни депозитари на ценни книжа;

ж) централни контрагенти;

з) места на търговия;

и) регистри на трансакции;

й) лица, управляващи алтернативни инвестиционни фондове;

к) управляващи дружества;

л) доставчици на услуги за докладване на данни;

м) застрахователни и презастрахователни дружества;

н) застрахователни посредници, презастрахователни посредници и посредници, които предлагат застрахователни продукти като допълнителна дейност;

о) институции за професионално пенсионно осигуряване;

п) агенции за кредитен рейтинг;

р) задължителни одитори и одиторски дружества;

с) администратори на критични бенчмаркове;

т) доставчици на услуги за колективно финансиране;

у) регистри на секюритизации;

ф) доставчици трети страни на услуги в областта на ИКТ.

2. За целите на настоящия регламент субектите по букви а) — у) се наричат общо „финансови субекти“.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) „оперативна устойчивост на цифровите технологии“ означава капацитетът на финансов субект да изгражда, поддържа и изменя технологичните аспекти на оперативната си дейност, като чрез пряко или непряко прибягване до услуги в областта на ИКТ на трети страни доставчици осигурява пълен набор основани на ИКТ процеси с оглед на защитеността на използваните от него мрежи и информационни системи, които подпомагат непрекъснатото предоставяне на финансови услуги и тяхното качество;

(2) „мрежа и информационна система“ означава мрежа и информационна система по смисъла на член 4, точка 1 от Директива (ЕС) 2016/1148;

(3) „сигурност на мрежите и информационните системи“ означава сигурност на мрежите и информационните системи по смисъла на член 4, точка 2 от Директива (ЕС) 2016/1148;

(4) „риск при ИКТ“ означава всяко установимо при обичайни условия обстоятелство във връзка с използването на мрежа и информационни системи — неизправност, превишаване на капацитета, общ или частичен срив, нарушено функциониране, злоупотреба, загуба или друго събитие — в резултат или не на злонамерен акт, което, ако се реализира, може да застраши сигурността на мрежата и информационните системи, на зависим от ИКТ инструмент или процес, на операциите или функционирането на процесите, или на предоставянето на услуги и оттам — целостта или наличността на данните, програмните продукти или който и да е друг компонент на услугите в областта на ИКТ и инфраструктурите на ИКТ, или да доведе до нарушаване на поверителността, увреждане на физическата инфраструктура на ИКТ или до други неблагоприятни последици;

(5) „информационен актив“ означава материална или нематериална съвкупност от информация, която си струва да се защитава;

(6) „инцидент с ИКТ“ означава установено непредвидено събитие в мрежата и информационните системи в резултат или не на злонамерен акт, което застрашава сигурността на мрежите и информационните системи, както и на обработваната, съхраняваната или обменяната от тях информация, или има неблагоприятни последици за наличността, поверителността, непрекъснатостта или автентичността на предоставяните от финансовия субект финансови услуги;

(7) „съществен инцидент с ИКТ“ означава инцидент с ИКТ с потенциално съществени неблагоприятни последици за мрежата и информационните системи в основата на възловите функции на финансовия субект;

(8) „киберзаплаха“ означава киберзаплаха по смисъла на член 2, точка 8 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[42];

(9) „кибератака“ означава инцидент при ИКТ в резултат на злонамерен акт на източник на заплаха с цел унищожаване, разкриване, промяна, деактивиране, откradване или получаване на непозволен достъп или непозволено използване на актив;

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

(10) „разузнавателни сведения за заплахи“ означава сведения, които са събрани, обработени, анализирани, разтълкувани или обогатени с оглед на взимането на решения и които позволяват в подходяща и достатъчна степен да се разбере как да се ограничат последствията от инцидент при ИКТ или киберзаплаха, в т.ч. техническите белези на дадена кибератака, отговорните за нея лица и техният начин на действие и мотивация;

(11) „защита в дълбочина“ означава стратегия в областта на ИКТ за интегриране на хората, процесите и технологиите с цел създаване на различни препятствия в множество слоеве и измерения на дружеството;

(12) „уязвимо място“ означава слабост, тенденция или недостатък на актив, система, процес или контролна функция, които могат да бъдат използвани чрез заплаха;

(13) „тестване на проникването“ означава симулиране на тактиката, техниките и процедурите на реални източници на заплаха, които се възприема, че представляват истинска киберзаплаха; тази симулация представлява контролиран, специално разработен и опиращ се на разузнавателни сведения (червен екип) тест на възловите оперативни производствени системи на дружеството;

(14) „риск при ИКТ, пораждан от трета страна“ означава риск при ИКТ, който възниква за финансов субект, когато използва услуги в областта на ИКТ на доставчик трета страна на такива услуги или на негови поддоставчици;

(15) „доставчик трета страна на услуги в областта на ИКТ“ означава дружество, което предоставя цифрови услуги и услуги за данни, в т.ч. доставчиците на компютърни услуги „в облак“, на програмни продукти, на услуги за анализ на данни, както и на центрове за данни, но без доставчиците на хардуерни компоненти и лицензираните съгласно правото на Съюза дружества, които предоставят електронни съобщителни услуги, както са определени в член 2, точка 4 от Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета[43];

(16) „услуги в областта на ИКТ“ означава цифрови услуги и услуги за данни, предоставяни чрез системите на ИКТ на един или повече вътрешни или външни ползватели, в т.ч. услуги за предоставяне, въвеждане, съхранение, обработка и докладване на данни, както и мониторинг на данни, а така също и услуги за подпомагане, въз основа на обработването на данни, на взимането на решения и на самата стопанска дейност;

(17) „възлова или важна функция“ означава функция, чието прекъсване, неизправност или срив може съществено да намали възможността на даден финансов субект да продължава да изпълнява условията и задълженията на своя лиценз или останалите си задължения съгласно приложимото финансово законодателство, или съществено да се отрази на финансовите му резултати или на стабилността или непрекъснатостта на неговите услуги и дейност;

(18) „възлов доставчик трета страна на услуги в областта на ИКТ“ означава доставчик трета страна на услуги в областта на ИКТ, който е определен в

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

съответствие с член 29 и е обхванат от надзорната рамка, посочена в членове 30—37;

(19) „доставчик трета страна на услуги в областта на ИКТ, установен в трета държава“ означава доставчик трета страна на услуги в областта на ИКТ, който е установено в трета държава юридическо лице, не извършва дейност и няма присъствие в Съюза, но е сключил договор с финансов субект за предоставяне на услуги в областта на ИКТ;

(20) „поддоставчик на ИКТ, установен в трета държава “ означава поддоставчик на ИКТ, който е установено в трета държава юридическо лице, не извършва дейност и няма присъствие в Съюза, но е сключил договор с доставчик трета страна на услуги в областта на ИКТ или с доставчик трета страна на услуги в областта на ИКТ, установен в трета държава;

(21) „риск от концентрация при ИКТ“ означава експозиция към даден възлов доставчик трета страна на услуги в областта на ИКТ или към множество свързани такива доставчици, която поражда известна степен на зависимост от такива доставчици, така че ако един от тях не бъде достъпен, престане да предоставя услугите си или понесе друг вид неизправност, това потенциално може да застраши капацитета на финансовия субект и в крайна сметка — на финансовата система на Съюза като цяло, да изпълнява възлови функции или да понесе друг вид неблагоприятни последици, в т.ч. огромни загуби;

(22) „ръководен орган“ означава ръководен орган по смисъла на член 4, параграф 1, точка 36 от Директива 2014/65/ЕС, член 3, параграф 1, точка 7 от Директива 2013/36/ЕС, член 2, параграф 1, буква т) от Директива 2009/65/ЕО, член 2, параграф 1, точка 45 от Регламент (ЕС) № 909/2014, член 3, параграф 1, точка 20 от Регламент (ЕС) № 2016/1011 на Европейския парламент и на Съвета[44], член 3, параграф 1, буква ф) от Регламент (ЕС) 20xx/xx на Европейския парламент и на Съвета[45] [РПКА] или еквивалентните лица, които действително управляват дружеството или упражняват възлови функции съгласно приложимото законодателство на Съюза или национално законодателство;

(23) „кредитна институция“ означава кредитна институция по смисъла на член 4, параграф 1, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета[46];

(24) „инвестиционен посредник“ означава инвестиционен посредник по смисъла на член 4, параграф 1, точка 1 от Директива 2014/65/ЕС;

(25) „платежна институция“ означава платежна институция по смисъла на член 1, параграф 1, точка 4 от Директива (ЕС) 2015/2366;

---

44 Регламент (ЕС) 2016/1011 на Европейския парламент и на Съвета от 8 юни 2016 г. относно индекси, използвани като бенчмаркове за целите на финансови инструменти и финансови договори или за измерване на резултатите на инвестиционни фондове, и за изменение на директиви 2008/48/ЕО и 2014/17/ЕС и на Регламент (ЕС) № 596/2014 (ОВ L 171, 29.6.2016 г., стр. 1).

45 [*да се въведат пълното заглавие и данните на публикацията в ОВ*]

46 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).

(26) „институция за електронни пари“ означава институция за електронни пари по смисъла на член 2, точка 1 от Директива 2009/110/ЕО на Европейския парламент и на Съвета[47];

(27) „централен контрагент“ означава централен контрагент по смисъла на член 2, точка 1 от Регламент (ЕС) № 648/2012;

(28) „регистър на трансакции“ означава регистър на трансакции по смисъла на член 2, точка 2 от Регламент (ЕС) № 648/2012;

(29) „централен депозитар на ценни книжа“ означава централен депозитар на ценни книжа по смисъла на член 2, параграф 1, точка 1 от Регламент (ЕС) № 909/2014;

(30) „място на търговия“ означава място на търговия по смисъла на член 4, параграф 1, точка 24 от Директива 2014/65/ЕС;

(31) „лице, управляващо алтернативни инвестиционни фондове“ означава лице, управляващо алтернативни инвестиционни фондове, по смисъла на член 4, параграф 1, буква б) от Директива 2011/61/ЕС;

(32) „управляващо дружество“ означава управляващо дружество по смисъла на член 2, параграф 1, буква б) от Директива 2009/65/ЕО;

(33) „доставчик на услуги за докладване на данни“ означава доставчик на услуги за докладване на данни по смисъла на член 4, параграф 1, точка 63 от Директива 2014/65/ЕС;

(34) „застрахователно предприятие“ означава застрахователно предприятие по смисъла на член 13, точка 1 от Директива 2009/138/ЕО;

(35) „презастрахователно предприятие“ означава презастрахователно предприятие по смисъла на член 13, точка 4 от Директива 2009/138/ЕО;

(36) „застрахователен посредник“ означава застрахователен посредник по смисъла на член 2, точка 3 от Директива (ЕС) 2016/97;

(37) „посредник, предлагащ застрахователни продукти като допълнителна дейност“ означава посредник, предлагащ застрахователни продукти като допълнителна дейност, по смисъла на член 2, точка 4 от Директива (ЕС) 2016/97;

(38) „презастрахователен посредник“ означава презастрахователен посредник по смисъла на член 2, точка 5 от Директива (ЕС) 2016/97;

(39) „институция за професионално пенсионно осигуряване“ означава институция за професионално пенсионно осигуряване по смисъла на член 6, точка 1 от Директива (ЕС) 2016/2341;

(40) „агенция за кредитен рейтинг“ означава агенция за кредитен рейтинг по смисъла на член 3, параграф 1, буква б) от Регламент (ЕС) № 1060/2009;

(41) „задължителен одитор“ означава задължителен одитор по смисъла на член 2, точка 2 от Директива 2006/43/ЕО;

---

[47] Директива 2009/110/ЕО на Европейския парламент и на Съвета от 16 септември 2009 г. относно предприемането, упражняването и пруденциалния надзор на дейността на институциите за електронни пари и за изменение на директиви 2005/60/ЕО и 2006/48/ЕО, и за отмяна на Директива 2000/46/ЕО (ОВ L 267, 10.10.2009 г., стр. 7).

(42) „одиторско дружество“ означава одиторско дружество по смисъла на член 2, точка 3 от Директива 2006/43/ЕО;

(43) „доставчик на услуги за криптоактиви“ означава доставчик на услуги за криптоактиви по смисъла на член 3, параграф 1, буква н) от Регламент (ЕС) 202x/xx [*ОВ: да се въведе позоваване на Регламента за криптоактивите*];

(44) „емитент на криптоактиви“ означава емитент на криптоактиви по смисъла на член 3, параграф 1, буква з) от [*ОВ: да се въведе позоваване на Регламента за криптоактивите*];

(45) „емитент на токени, обезпечени с активи“ означава емитент на токени, обезпечени с активи, по смисъла на член 3, параграф 1, буква и) от [*ОВ: да се въведе позоваване на Регламента за криптоактивите*];

(46) „емитент на значими токени, обезпечени с активи“ означава емитент на значими токени, обезпечени с активи, по смисъла на член 3, параграф 1, буква й) от [*ОВ: да се въведе позоваване на Регламента за криптоактивите*];

(47) „администратор на критични бенчмаркове“ означава администратор на критични бенчмаркове по смисъла на член x, точка x) от Регламент xx/202x [*ОВ: да се въведе позоваване на Регламента за бенчмарковете*];

(48) „доставчик на услуги за колективно финансиране“ означава доставчик на услуги за колективно финансиране по смисъла на член x, точка x) от Регламент (ЕС) 202x/xx [*ОВ: да се въведе позоваване на Регламента за колективното финансиране*];

(49) „регистър на секюритизации“ означава регистър на секюритизации по смисъла на член 2, точка 23 от Регламент (ЕС) 2017/2402;

(50) „микропредприятие“ означава финансов субект по смисъла на член 2, параграф 3 от приложението към Препоръка 2003/361/ЕО.

ГЛАВА II

УПРАВЛЕНИЕ НА РИСКА ПРИ ИКТ

РАЗДЕЛ I

Член 4

Управление и организация

1. Финансовите субекти разполагат с вътрешни управленски и контролни механизми с оглед на ефективното и благоразумно управление на всички рискове при ИКТ.

2. Ръководният орган на финансовия субект определя, одобрява, контролира и носи отговорност за изпълнението на всички действия във връзка с посочената в член 5, параграф 1 рамка за управление на риска при ИКТ.

За целите на първа алинея ръководният орган:

а) носи крайната отговорност за управлението на рисковете при ИКТ за финансовия субект;

б) определя ясно ролята и отговорността при всички свързани с ИКТ функции;

в) определя подходящото за финансовия субект равнище на толерантност към риска при ИКТ, както е посочено в член 5, параграф 9, буква б);

г) одобрява, наблюдава и периодично прави преглед на изпълнението на посочените в член 10, съответно параграфи 1 и 3 политика на финансовия субект за непрекъснато функциониране на ИКТ и план за възстановяване на информацията при срив на ИКТ;

д) одобрява и периодично прави преглед на плановете за одит на ИКТ, на одитите на ИКТ и на съществените промени в тях;

е) разпределя и периодично преглежда подходящия бюджет за всички видове ресурси с оглед на потребностите на финансовия субект по отношение на оперативната устойчивост на цифровите технологии, в т.ч. потребностите от обучение за рисковете при ИКТ и уменията в областта на ИКТ за всички съответни служители;

ж) одобрява и периодично преглежда политиката на финансовия субект за използването на услуги в областта на ИКТ, предоставяни от доставчици трети страни на такива услуги;

з) надлежно се осведомява за сключените с доставчици трети страни на услуги в областта на ИКТ договори за използване на услуги в областта на ИКТ, за всякакви съответни планирани съществени промени по отношение на тези доставчици, както и за потенциалното въздействие на такива промени върху възловите или важните функции, предмет на тези договори, в т.ч. като получава обобщен анализ на риска, за да оцени въздействието на тези промени;

и) надлежно се осведомява за инцидентите с ИКТ и за тяхното въздействие, както и за ответните действия, възстановяването на информацията и коригиращите мерки.

3. Финансовите субекти, без микропредприятията, определят функция за наблюдение на сключените с доставчици трети страни на услуги в областта на ИКТ договори за използване на услуги в областта на ИКТ или възлагат на член на висшето ръководство да следи свързания с тези доставчици риск и съответната документация.

4. Членовете на ръководния орган периодично преминават специално обучение, за да придобият и поддържат актуални достатъчно знания и умения, за да разбират и оценяват рисковете при ИКТ и тяхното въздействие върху дейността на финансовия субект.

РАЗДЕЛ II

Член 5

Рамка за управление на риска при ИКТ

1. Финансовите субекти разполагат с надеждна, широкообхватна и добре документирана рамка за управление на риска при ИКТ, която им позволява да се справят бързо, ефикасно и многоаспектно с риска при ИКТ и да поддържат

значителна оперативна устойчивост на цифровите технологии, съобразена с техните стопански нужди, размер и сложност.

2. Посочената в параграф 1 рамка за управление на риска при ИКТ включва стратегии, политики, процедури, протоколи за ИКТ и инструменти, основани на ИКТ, които са необходими за надлежната и ефективна защита на всички съответни физически компоненти и инфраструктури, в т.ч. компютърен хардуер, сървъри, а и всички съответни помещения, центрове за данни и определени чувствителни зони, така че всички тези физически елементи да са подходящо защитени от рискове, в т.ч. увреждане и непозволен достъп или използване.

3. Финансовите субекти свеждат до минимум въздействието на риска при ИКТ, като прилагат заложените в рамката за управление на риска при ИКТ подходящи стратегии, политики, процедури, протоколи и инструменти. Те предоставят пълна и актуална информация за рисковете при ИКТ съобразно изискванията на компетентните органи.

4. Като част от посочената в параграф 1 рамка за управление на риска при ИКТ финансовите субекти, без микропредприятията, въвеждат, като се опират на признатите международни стандарти и се съобразяват с надзорните насоки, система за управление на сигурността на информацията и редовно я преразглеждат.

5. Финансовите субекти, без микропредприятията, подходящо обособяват според модела на трите защитни слоя или свой модел за управление и контрол на риска функциите за управление на ИКТ, контролните функции и функциите за вътрешен одит.

6. Посочената в параграф 1 рамка за управление на риска при ИКТ бива документирана и преразглеждана поне веднъж годишно, както и при съществени инциденти с ИКТ, като това се прави съобразно надзорните инструкции или констатациите от съответните одити или тестове на оперативната устойчивост на цифровите технологии. Рамката се усъвършенства непрекъснато въз основа на натрупания при нейното прилагане и наблюдаване опит.

7. Посочената в параграф 1 рамка за управление на риска при ИКТ е предмет на периодично провеждан одит от страна на одиторите в сферата на ИКТ, които притежават достатъчно знания, умения и опит за риска при ИКТ. Честотата и обхватът на одитите на ИКТ са съобразени с рисковете при използваните от дадения финансов субект ИКТ.

8. Финансовите субекти въвеждат формален процес на последващи мерки във връзка със заключенията на одитните прегледи на ИКТ, който включва правила за своевременно проверяване на съществените констатации на одита на ИКТ и за отстраняване на отбелязаните проблеми при надлежното отчитане на естеството, мащаба и сложността на услугите и дейностите на дружеството.

9. Посочената в параграф 1 рамка за управление на риска включва стратегия за устойчивост на цифровите технологии, в която се описва нейното прилагане. В рамката се посочват методите за противодействие на риска при ИКТ и за постигането на конкретни цели в областта на ИКТ, както следва:

   а) обяснява се как тя подпомага стратегията и целите, които финансовият субект си е поставил за своята стопанска дейност;

б) определя се равнище на толерантност към риска при ИКТ според склонността на финансовия субект за поемане на риск и се проучва допустимата степен на въздействие на неизправност на ИКТ;

в) залагат се ясни цели за сигурност на информацията;

г) описва се архитектурата на ИКТ и всички промени, необходими за постигането на конкретни цели за дейността;

д) очертават се различните механизми за откриване, противодействие и предотвратяване на въздействието на инциденти с ИКТ;

е) посочва се фактическият брой на съществените инциденти с ИКТ, за които е било съобщено, и се демонстрира ефективността на превантивните мерки;

ж) определя се цялостна стратегия на субекта за прибягване до множество доставчици на ИКТ, в която се посочват основните отношения на зависимост от доставчици трети страни на услуги в областта на ИКТ и се обяснява логиката зад избора на съответните доставчици трети страни;

з) въвежда се тестване на оперативната устойчивост на цифровите технологии;

и) очертава се стратегията за уведомяване за инцидентите с ИКТ.

10. След одобрение от компетентните органи финансовите субекти могат да поверят на предприятия от своята група или на външни предприятия задачите по проверка на съблюдаването на изискванията за управление на риска при ИКТ.

Член 6

Системи и протоколи на ИКТ и основани на ИКТ инструменти

1. Финансовите субекти използват и поддържат в актуален вид системи и протоколи на ИКТ и основани на ИКТ инструменти, които удовлетворяват следните условия:

а) системите и инструментите са съобразени с естеството, разнообразието, сложността и мащаба на операциите, посредством които те провеждат дейността си;

б) те са надеждни;

в) капацитетът им е достатъчен за точното обработване на данните, необходими за изпълнението на дейностите и за своевременното предоставяне на услуги, както и за справянето със скокове в обема на поръчките, съобщенията или обемите на операциите според нуждите, в т.ч. при въвеждането на нови технологии;

г) те са технически устойчиви, така че да могат адекватно да удовлетворяват необходимостта от обработване на допълнителна информация при неблагоприятни пазарни условия или други проблематични ситуации.

2. Когато финансовите субекти използват международно признати технически стандарти и водещи секторни практики за сигурност на информацията и за вътрешен контрол на ИКТ, те използват тези стандарти и практики, като при

внедряването им се съобразяват с евентуалните препоръки, отправени им от надзорните органи.

Член 7

Установяване

1. Като част от посочената в член 5, параграф 1 рамка за управление на риска при ИКТ финансовите субекти установяват, класифицират и документират по подходящ начин всички свързани с ИКТ стопански функции, поддържаните от тези функции информационни активи, както и конфигурациите на ИКТ и взаимовръзките с вътрешните и външни системи на ИКТ. Когато е необходимо, но поне веднъж годишно финансовите субекти преценяват адекватността на класификацията на информационните активи и на съответната документация.

2. Финансовите субекти непрекъснато установяват всички източници на риск за ИКТ, по-специално доколко са изложени на риск от други финансови субекти и доколко те самите са рисков фактор за тези други субекти, и оценяват киберзаплахите и уязвимите места при ИКТ, които са съществени за техните стопански функции, свързани с ИКТ, и информационни активи. Периодично, но поне веднъж годишно финансовите субекти правят преглед на рисковите сценарии с въздействие върху тях.

3. Финансовите субекти, без микропредприятията, извършват оценка на риска при всяка съществена промяна в инфраструктурата на мрежите и информационните системи, в процесите или процедурите, засягащи техните функции, в поддържащите процеси или в информационните активи.

4. Финансовите субекти установяват всички заведени системи на ИКТ, в т.ч. в отдалечените обекти, мрежовите ресурси и хардуера, и правят опис на физическото оборудване от възлово значение. Те описват и конфигурацията на активите на ИКТ, както и връзките и взаимозависимостта между тези активи.

5. Финансовите субекти установяват и документират всички процеси, които зависят от доставчици трети страни на услуги в областта на ИКТ, и взаимовръзките с тези доставчици.

6. За целите на параграфи 1, 4 и 5 финансовите субекти поддържат и редовно актуализират съответните описания.

7. Периодично, но поне веднъж годишно финансовите субекти, без микропредприятията, специално оценяват риска при ИКТ при вече използваните системи на ИКТ, особено преди и след свързването на старите и новите технологии, приложения или системи.

Член 8

Защита и предотвратяване

1. С оглед на адекватната защита на системите на ИКТ и организирането на ответни действия финансовите субекти неотклонно наблюдават и контролират функционирането на системите на ИКТ и основаните на ИКТ инструменти, и свеждат до минимум рисковете при ИКТ чрез въвеждането на подходящи инструменти, политики и процедури за сигурност на ИКТ.

2. Финансовите субекти проектират, възлагат и прилагат стратегии, политики, процедури, протоколи и инструменти за сигурност на ИКТ, с които в частност се осигурява устойчивостта, непрекъснатостта и достъпът до системите на ИКТ и се поддържат високи стандарти за сигурност, поверителност и цялост на данните при тяхното съхранение, използване и обменяне.

3. С оглед на посочените в параграф 2 цели финансовите субекти използват съвременни технологии и процеси в областта на ИКТ, които:

   а) гарантират сигурността на средствата за предаване на информацията;

   б) свеждат до минимум риска от увреждане или загуба на данните, непозволен достъп и техническите недостатъци, които могат да попречат на стопанската дейност;

   в) предотвратяват изтичането на информация;

   г) предпазват данните от риск от лошо администриране или във връзка с обработването им, в т.ч. от неподходящо документиране.

4. Като част от посочената в член 5, параграф 1 рамка за управление на риска финансовите субекти:

   а) разработват и документират политика за сигурност на информацията, в която определят правила за защита на поверителността, целостта и наличността на своите и клиентските информационни ресурси, данни и информационни активи;

   б) създават, следвайки подход, при който се отчита рискът, стабилно управление на мрежите и инфраструктурата с помощта на подходящи техники, методи и протоколи, в т.ч. автоматизирани механизми за обособяване на засегнатите при кибератака информационни активи;

   в) прилагат политики, които ограничават физическия и виртуалния достъп до системните ресурси и данните на ИКТ до необходимото с оглед на законните и одобрени функции и дейности, като за тази цел създават набор от политики, процедури и механизми за контрол на правата на достъп, които администрират по подходящ начин;

   г) прилагат политики и протоколи за стабилни механизми за удостоверяване на автентичността, като използват съответните стандарти и системи за специален контрол, с цел да се предотврати достъпът до криптографските ключове, когато данните са криптирани след одобрено тяхно класифициране и извършена оценка на риска;

   д) прилагат политики, процедури и контролни механизми за управление на промените в ИКТ, извършени в резултат на оценка на риска и в рамките на цялостния процес на управление на промените от страна на финансовия субект — в т.ч. на промените в софтуера, хардуера, компонентите на базовото програмно осигуряване, системата или сигурността, с цел да се контролира записването, тестването, оценяването, одобряването и проверяването на всички промени в системите на ИКТ;

   е) разполагат с подходящи и обстойни политики за коригиране и актуализиране.

За целите на буква б) финансовите субекти разработват инфраструктурата за мрежова връзка така, че да бъде възможно моменталното ѝ изваждане от експлоатация, както и обособяване и сегментиране, така че да се сведе до минимум и да се предотврати разпространяването на даден проблем, особено при взаимосвързаните финансови процеси.

За целите на буква д) управлението на промените в ИКТ се одобрява от подходяща йерархична стълбица и разполага със специални протоколи за промени при извънредни обстоятелства.

Член 9

Откриване

1. Както е посочено в член 15, финансовите субекти разполагат с механизми за бързо откриване на необичайните дейности — в т.ч. проблеми с функционирането на мрежата на ИКТ и инциденти с ИКТ, както и за установяване на всички потенциални точки, повредата в които може да доведе до общ срив.

   Механизмите по първа алинея се тестват редовно, както е посочено в член 22.

2. Механизмите по параграф 1 позволяват множество нива на контрол, определят прагове за отправяне на предупреждение и критерии за задействане на процес за откриване на инциденти с ИКТ и за предприемане на ответни действия при такива инциденти, и въвеждат автоматични механизми за предупреждаване на съответните отговорни служители за предприемането на ответни действия при инциденти с ИКТ.

3. Финансовите структури отделят достатъчно ресурси и оперативен капацитет за наблюдение на активността на ползвателите и на възникналите аномалии при ИКТ и инциденти с ИКТ, особено кибератаки; тези ресурси и капацитет са надлежно съобразени с техния размер, профил на стопанска дейност и профил на риска.

4. От своя страна финансовите субекти по член 2, параграф 1, буква л) разполагат и със системи за надеждна проверка на отчетите на сделките, за да се установи дали са пълни, дали има пропуски и явни грешки и при установени недостатъци да се поиска повторното им предоставяне.

Член 10

Ответни действия и възстановяване на информацията

1. Като част от посочената в член 5, параграф 1 рамка за управление на риска при ИКТ и въз основа на посочените в член 7 изисквания за установяване, финансовите субекти въвеждат като част от политиката си за непрекъснатост на дейността специална и всеобхватна политика за непрекъснато функциониране на ИКТ.

2. Финансовите субекти прилагат посочената в параграф 1 политика за непрекъснато функциониране на ИКТ чрез специални, подходящи и документирани правила, планове, процедури и механизми, с помощта на които:

   а) се завеждат всички инциденти с ИКТ;

б) се осигурява непрекъснатостта на възловите функции на финансовия субект;

в) ответните действия на инцидентите с ИКТ — най-вече, но не само, кибератаките, както и възстановяването от тях са бързи и се предприемат по подходящ и ефективен начин, с който се ограничават щетите и се отдава приоритет на възобновяването на функционирането и на възстановяването на информацията;

г) след всеки вид инцидент с ИКТ се задействат незабавно специални планове за прилагане на мерки, процеси и технологии за овладяването му и за предотвратяването на допълнителни щети, както и въведените по силата на член 11 специални процедури за предприемане на ответни действия и за възстановяване на информацията;

д) се прави оценка на предварителното въздействие, щети и загуби;

е) се определят действията за комуникация и за управление на кризи с цел актуализираната информация да се предаде на всички съответни вътрешни служители и външни заинтересовани страни — както е посочено в член 13, и да се уведомят компетентните органи — както е посочено в член 17.

3. Като част от посочената в член 5, параграф 1 рамка за управление на риска при ИКТ финансовите субекти прилагат свързан с нея план за възстановяване на информацията при срив на ИКТ, който при всички финансови субекти освен микропредприятията подлежи на независими одитни прегледи.

4. Финансовите субекти въвеждат, поддържат и периодично тестват подходящи планове за непрекъснато функциониране на ИКТ, по-специално по отношение на възловите или важни функции, възложени с договор или другояче на доставчици трети страни на услуги в областта на ИКТ.

5. Като част от общото си управление на риска при ИКТ финансовите субекти:

а) тестват политиката за непрекъснато функциониране на ИКТ и плана за възстановяване на информацията при срив на ИКТ най-малко веднъж годишно, както и след съществени промени в системите на ИКТ;

б) тестват изготвените по силата на член 13 планове за комуникация при кризи.

За целите на буква а) финансовите субекти, без микропредприятията, предвиждат в тестовите си сценарии за кибератаки и преминаване от първичната инфраструктура на ИКТ към възпроизвеждащите я системи наличието на системи за съхраняване на резервни копия на данните и резервни системи, с оглед на задълженията си по член 11.

Финансовите субекти редовно преразглеждат своята политика за непрекъснато функциониране на ИКТ и план за възстановяване на информацията при срив на ИКТ с оглед на резултатите от проведените по силата на първа алинея тестове и препоръките от одитните проверки или надзорните прегледи.

6. Финансовите субекти, без микропредприятията, разполагат с функция за управление на кризи, която, при задействане на тяхната политика за непрекъснато функциониране на ИКТ или план за възстановяване на

информацията при срив на ИКТ, предвижда ясни процедури за управление на посочената в член 13 вътрешна и външна комуникация при кризи.

7. Ако политиката им за непрекъснато функциониране на ИКТ или планът им за възстановяване на информацията при срив на ИКТ са задействани, финансовите субекти документират действията преди и по време на събитията, нарушили обичайното функциониране. Тези сведения са лесно достъпни.

8. Финансовите субекти по член 2, параграф 1, буква е) предоставят на компетентните органи копия от резултатите на извършените през разглеждания период тестове на непрекъснатостта на функционирането на ИКТ или подобни проверки.

9. Финансовите субекти, без микропредприятията, уведомяват компетентните органи за всички разходи и загуби, причинени от сривове на ИКТ и инциденти с ИКТ.

Член 11

Политика за съхраняване на резервни копия на данните и методи за възстановяване на информацията

1. С цел възстановяването на системите на ИКТ да протече максимално бързо и с минимално отражение върху обичайното функциониране финансовите субекти разработват като част от рамката си за управление на риска при ИКТ следното:

   а) политика за съхраняване на резервни копия на данните, в която с оглед на значимостта или чувствителния характер на информацията се определят данните, на които ще бъдат съхранявани резервни копия, както и минималната честота на това копиране;

   б) методи за възстановяване на информацията.

2. Системите за съхраняване на резервни копия на данните се задействат без неоправдано забавяне, стига това да не застрашава сигурността на мрежите и информационните системи, нито целостта или поверителността на данните.

3. Когато финансовите субекти използват собствени системи за съхраняване на резервни копия на данните, те предвиждат такива системи на ИКТ, чиято операционна среда е различна от основната, не е пряко свързана с нея и е защитена по сигурен начин от непозволен достъп или неизправност на ИКТ.

   При финансовите субекти по член 2, параграф 1, буква ж) плановете за възстановяване на информацията предвиждат възстановяването на всички трансакции към момента на прекъсването, така че ЦДЦК да може да продължи да функционира по надежден начин и да приключи сетълмента на определената дата.

4. Финансовите субекти поддържат допълнителен капацитет в областта на ИКТ, чиито ресурси, оперативен капацитет и възможности са достатъчни и съобразени с потребностите на дейността.

5. Финансовите субекти по член 2, параграф 1, буква е) поддържат — или се уверяват, че техните доставчици трети страни на услуги в областта на ИКТ поддържат — поне един допълнителен обект за обработка, който разполага с ресурси, оперативен капацитет, възможности и договорености за набиране на

персонал, които са достатъчни и подходящи предвид потребностите на дейността.

Допълнителният обработвателен център:

а) се намира на физическо разстояние от основния обект за обработка, така че да има отделен рисков профил и да не бъде засегнат от събитието, засегнало основния обект;

б) притежава капацитет, равен на този на основния обект, за осигуряване на непрекъснатостта на възловите услуги или за предоставяне на такова ниво на обслужване, което позволява на финансовият субект да извършва основните си операции в рамките на заложените цели за възстановяване на информацията;

в) е непосредствено достъпен за персонала на финансовия субект, ако основният обект за обработка не е достъпен, така че да се осигури непрекъснатостта на възловите услуги.

6. Когато определят целевите срокове — като продължителност и момент във времето — за възстановяване на информацията при всяка функция, финансовите субекти взимат предвид потенциалното общо въздействие върху пазарната ефективност. Тези срокове позволяват да се удовлетворяват договорените параметри на обслужване дори при крайно неблагоприятни сценарии.

7. Когато възстановяват информацията след инцидент с ИКТ, финансовите субекти извършват множество проверки, в т.ч. сравняват възстановените с оригиналните данни, за да се осигурят възможно най-пълни данни. Тези проверки се извършват и когато се възстановяват данни на външни заинтересовани страни, така че да се осигури съгласуваност на всички данни между отделните системи.

Член 12

Обучение и задълбочаване на познанията

1. Финансовите субекти разполагат със съобразени с техния размер, профил на стопанска дейност и профил на риска оперативен капацитет и персонал, които да събират информация за уязвимите места, киберзаплахите и инцидентите с ИКТ — особено кибератаките, и да анализират вероятното им въздействие върху оперативната устойчивост на използваните от тези субекти цифрови технологии.

2. След съществена неизправност на ИКТ, засегнала основната им дейност, финансовите субекти извършват прегледи на възникналите инциденти с ИКТ, за да проучат техните причини и да установят какво е необходимо да се подобри в основаните на ИКТ операции или в посочената в член 10 политика за непрекъснато функциониране на ИКТ.

Финансовите субекти, без микропредприятията, уведомяват компетентните органи за всички въведени промени.

С посочените в първа алинея прегледи на възникналите инциденти с ИКТ се установява дали са били спазени въведените процедури и дали са били ефективни предприетите действия, в т.ч. по отношение на:

а) бързината на реагиране на предупредителните сигнали и установяване на въздействието на инцидентите с ИКТ и на тяхната сериозност;

б) бързината, с която е извършена техническата експертиза, и нейното качество;

в) ефективността на процедурата на финансовия субект за управление на инцидентите;

г) ефективността на вътрешната и външната комуникация.

3. В процеса на оценка на риска при ИКТ надлежно и непрекъснато се добавя натрупаният опит от проведените по силата на членове 23 и 24 тестове на оперативната устойчивост на цифровите технологии, от реалните инциденти с ИКТ — особено кибератаките, както и от срещнатите предизвикателства при задействането на плановете за непрекъснато функциониране на ИКТ и за възстановяване на информацията след срив на ИКТ, а така също и съответната информация, обменяна с контрагентите и оценявана при надзорните прегледи. Тези констатации водят до подходящи преразглеждания на съответните компоненти на посочената в член 5, параграф 1 рамка за управление на риска при ИКТ.

4. Финансовите субекти наблюдават доколко ефективно се провежда стратегията им за устойчивост на цифровите технологии, посочена в член 5, параграф 9. С цел да определят степента, в която техните ИКТ са изложени на риск, да задълбочат познанията си за киберсигурността и да усъвършенстват готовността си в тази област финансовите субекти документират тенденцията при рисковете при ИКТ във времето, анализират честотата, видовете и мащаба на инцидентите с ИКТ, както и начина, по който те се променят, особено що се отнася до кибератаките и техните модели.

5. Най-малко веднъж годишно висшите служители, работещи с ИКТ, представят на ръководния орган посочените в параграф 3 констатации и правят препоръки.

6. Финансовите организации разработват и включват като задължителни модули в схемите си за обучение на персонала програми за повишаване на осведомеността за сигурността на ИКТ и обучения по оперативна устойчивост на цифровите технологии. Тези програми се прилагат за всички служители и за висшето ръководство.

Финансовите субекти постоянно следят развитието на съответните технологии, също и с цел да проучат потенциалното въздействие от внедряването на такива нови технологии върху изискванията за сигурност на ИКТ и оперативната устойчивост на цифровите технологии. Те трябва да са запознати с най-новите процеси за управление на риска при ИКТ и да могат ефективно да противодействат на настоящите или новите форми на кибератаки.

Член 13

Комуникиране

1. Като част от посочената в член 5, параграф 1 рамка за управление на риска финансовите субекти разполагат с комуникационни планове за отговорно уведомяване на клиентите и контрагентите, а по необходимост — и на обществеността, за инцидентите с ИКТ или за съществените уязвими места.

2. Като част от посочената в член 5, параграф 1 рамка за управление на риска финансовите субекти въвеждат комуникационна политика за персонала и за външните заинтересовани страни. В комуникационната политика за персонала се прави разлика между персонала, зает с управлението на риска при ИКТ и по-специално — с ответните действия и възстановяването на информацията, и персонала, който трябва да бъде уведомен.

3. За комуникационната стратегия на финансовия субект при инциденти с ИКТ отговаря поне един служител, който в тази връзка изпълнява и ролята на говорител за обществеността и медиите.

Член 14

Допълнително хармонизиране на инструментите, методите, процесите и политиките за управление на риска при ИКТ

Европейският банков орган (ЕБО), Европейският орган за ценни книжа и пазари (ЕОЦКП) и Европейският орган за застраховане и професионално пенсионно осигуряване (ЕОЗППО) разработват, като се консултират с Агенцията на Европейския съюз за киберсигурност (ENISA), проекти на регулаторни технически стандарти с оглед на следното:

а) определяне на допълнителните елементи, които да бъдат включени в посочените в член 8, параграф 2 политики, процедури, протоколи и инструменти за сигурност на ИКТ, така че мрежите да бъдат сигурни, да се създадат подходящи механизми срещу проникване и срещу злоупотреба с данните, да се запази, в т.ч. чрез криптиране, автентичността и целостта на данните, както и да се осигури точното и бързо предаване на данните, без съществени неизправности;

б) определяне на начина, по който в посочените в член 8, параграф 2 политики, процедури, протоколи и инструменти за сигурност на ИКТ се включват контролни механизми още на етапа на проектиране на системите, позволява се адаптиране към динамичната среда на заплахите и се предвижда използването на технологии за защита в дълбочина;

в) доуточняване на посочените в член 8, параграф 4, буква б) подходящи техники, методи и протоколи;

г) разработване на допълнителни компоненти на посочените в член 8, параграф 4, буква в) механизми за контрол на правата на достъп и на свързаната с тях политика за човешките ресурси, в които се определят правата на достъп, процедурите за предоставяне и отнемане на права, както и за наблюдаване на необичайното поведение във връзка с рисковете при ИКТ чрез подходящи показатели за моделите на използване на мрежата, за часовите пояси, за дейността, свързана с информационните технологии, и за неизвестните устройства;

д) доразработване на посочените в член 9, параграф 1 елементи за бързо откриване на аномалии, както и на посочените в член 9, параграф 2 критерии за задействане на процес за откриване на инциденти с ИКТ и за предприемане на ответни действия;

е) доуточняване на компонентите на посочената в член 10, параграф 1 политика за непрекъснато функциониране на ИКТ;

ж) доуточняване на изискванията за тестване на посочената в член 10, параграф 5 политика за непрекъснато функциониране на ИКТ с цел тестването надлежно да обхваща всички сценарии, при които възлова или важна функция се предоставя с неприемливо ниско качество или не се предоставя изобщо, както и надлежно да отчита потенциалното въздействие на изпадането в несъстоятелност или възникването на други проблеми при съответните доставчици трети страни на услуги в областта на ИКТ, а когато е приложимо — и политическия риск в юрисдикциите на съответните доставчици;

з) доуточняване на компонентите на посочения в член 10, параграф 3 план за възстановяване на информацията при срив на ИКТ.

ЕБО, ЕОЦКП и ЕОЗППО предават на Комисията тези проекти на регулаторни технически стандарти до [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да приеме посочените в първа алинея регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010.

ГЛАВА III

ИНЦИДЕНТИ С ИКТ

УПРАВЛЕНИЕ, КЛАСИФИЦИРАНЕ И УВЕДОМЯВАНЕ

Член 15

Процес за управление на инцидентите с ИКТ

1. Финансовите субекти въвеждат и прилагат процес за управление на инцидентите с ИКТ, чрез който да се откриват, управляват и съобщават инцидентите с ИКТ, като също така определят показатели за ранно предупреждение, които да служат за предупредителни сигнали.

2. Финансовите субекти въвеждат подходящи процедури за последователно и интегрирано наблюдаване, преодоляване и проследяване на инцидентите с ИКТ, така че да се установят и отстранят основните причини за тях и да се предотврати появата им.

3. С посочения в параграф 1 процес за управление на инцидентите с ИКТ се постига следното:

   а) въвеждат се процедури за установяване, проследяване, регистриране, категоризиране и класифициране на инцидентите с ИКТ според техния приоритет и според тежестта и значимостта на засегнатите услуги — по критериите в член 16, параграф 1;

   б) определят се ролите и задачите, които трябва да се задействат при отделните видове и сценарии на инциденти с ИКТ;

   в) изготвят се планове за комуникиране, по силата на член 13, за персонала, външните заинтересовани страни и медиите, както и за уведомяване на клиентите, процедурите за управление на инцидентите, в т.ч. на

оплакванията на клиентите във връзка с ИКТ, както и планове за предоставяне на информация на контрагентите финансови субекти, ако това е необходимо;

г) съществените инциденти с ИКТ се докладват на съответното висше ръководство, а се уведомява и ръководният орган, като се обясняват последиците от дадения инцидент и се посочват необходимите в тази връзка ответни действия и допълнителни контролни мерки;

д) въвеждат се процедури за предприемане на ответни действия при инцидент с ИКТ, за да се ограничат последиците и своевременно да се възобнови обичайното и сигурно функциониране на услугите.

Член 16

Класифициране на инцидентите с ИКТ

1. Финансовите субекти класифицират инцидентите с ИКТ и определят въздействието им по следните критерии:

а) брой потребители или финансови контрагенти, засегнати от породената от инцидента с ИКТ неизправност, както и евентуално въздействие на инцидента с ИКТ върху репутацията;

б) продължителност на инцидента с ИКТ, в т.ч. период на прекъсване на услугата;

в) географски обхват, т.е. райони, засегнати от инцидента с ИКТ, особено ако са засегнати над две държави членки;

г) проблеми при данните в резултат на инцидента с ИКТ, като например накърнена цялост, нарушена поверителност или невъзможен достъп;

д) тежест на последиците от инцидента с ИКТ върху системите на ИКТ на финансовия субект;

е) значимост на засегнатите услуги, в т.ч. на сделките и операциите на финансовия субект;

ж) икономически последици от инцидента с ИКТ в абсолютно и в относително изражение.

2. В рамките на съвместния си комитет и след консултация с Европейската централна банка (ЕЦБ) и ENISA ЕНО разработват общи проекти на регулаторни технически стандарти за доуточняване на:

а) критериите по параграф 1, в т.ч. праговете на същественост за определяне на съществените инциденти с ИКТ, които трябва да бъдат съобщавани по силата на член 17, параграф 1;

б) критериите, които компетентните органи трябва да прилагат, когато оценяват значението на съществен инцидент с ИКТ за юрисдикциите на други държави членки, и информацията в докладите за инцидент с ИКТ, която трябва да бъде споделяна с други компетентни органи по силата на член 17, параграфи 5 и 6.

3. При разработването на посочените в параграф 2 общи проекти на регулаторни технически стандарти ЕНО се съобразяват с международните стандарти и

разработените и публикуваните от ENISA спецификации, в т.ч. и за други икономически сектори — когато е целесъобразно.

ЕНО предават на Комисията тези общи проекти на регулаторни технически стандарти до [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените в параграф 2 регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010.

Член 17

Уведомяване за съществените инциденти с ИКТ

1. Финансовите субекти уведомяват съответния компетентен орган по член 41 за съществените инциденти с ИКТ в посочените в параграф 3 срокове.

   За целите на първа алинея финансовите субекти събират и проучват цялата съответна информация, след което по образеца, посочен в член 18, изготвят доклад за инцидента, който предават на компетентния орган.

   Докладът съдържа цялата информация, която е необходима на компетентния орган, за да определи доколко даденият инцидент с ИКТ е съществен и да оцени възможните последици в трансграничен план.

2. Когато съществен инцидент с ИКТ има или може да има последици за финансовите интереси на ползвателите на услугите и на клиентите, финансовите субекти възможно най-бързо ги уведомяват за него и за всички предприети мерки за ограничаване на неблагоприятните последици.

3. Финансовите субекти предоставят на компетентния орган, посочен в член 41:

   а) първоначално уведомление — възможно най-бързо, но не по-късно от края на работния ден, а ако съществен инцидент с ИКТ настъпи по-късно от 2 часа преди края на работния ден — не по-късно от 4 часа от началото на следващия работен ден, а ако няма комуникационни канали за тази цел — веднага след като се появят;

   б) неокончателен доклад — не по-късно от 1 седмица след първоначалното уведомление по буква а), последван, по целесъобразност, от актуализирани уведомления — всеки път, когато съответният статус бъде актуализиран или ако компетентният орган специално поиска такива уведомления;

   в) окончателен доклад — когато първопричината бъде проучена, независимо дали мерките за ограничаване на последиците са били вече предприети или не, и когато са налице действителните стойности на въздействието, с които могат да се заместят прогнозните — но не по-късно от един месец от момента на изпращане на първоначалния доклад.

4. Финансовите субекти могат да прехвърлят на доставчик на услуги трета страна посочените в настоящия член задължения за уведомяване само ако съответният компетентен орган по член 41 одобри това.

5. Когато получи доклада по параграф 1 компетентният орган възможно най-бързо уведомява подробно за инцидента:

а) ЕБО, ЕОЦКП или ЕОЗППО — в зависимост от случая;

б) ЕЦБ, според случая, когато става въпрос за финансовите субекти по член 2, параграф 1, букви а), б) и в); както и

в) единното звено за контакт, определено по силата на член 8 от Директива (ЕС) 2016/1148.

6. ЕБО, ЕОЦКП или ЕОЗППО, както и ЕЦБ оценяват доколко съществените инцидент с ИКТ е от значение за другите съответни публични органи и ги уведомяват възможно най-бързо. ЕЦБ уведомява членовете на Европейската система на централните банки за проблемите, които имат отношение към платежната система. Въз основа на уведомлението компетентните органи предприемат, когато е целесъобразно, всички необходими мерки, за да защитят непосредствената стабилност на финансовата система.

Член 18

Хармонизиране на съдържанието на уведомленията и на образците за уведомяване

1. В рамките на съвместния си комитет и след консултация с ЕЦБ и ENISA ЕНО разработват:

а) общи проекти на регулаторни технически стандарти:

(1) за определяне на съдържанието на уведомленията за съществени инциденти с ИКТ;

(2) за доуточняване на условията, при които финансовите субекти могат след предварително одобрение от компетентния орган да прехвърлят на доставчик на услуги трета страна посочените в настоящата глава задължения за уведомяване;

б) общи проекти на технически стандарти за изпълнение за установяване на стандартните формуляри, образци и процедури за уведомяване за съществените инциденти с ИКТ.

ЕНО предават на Комисията общите проекти на регулаторни технически стандарти по параграф 1, буква а) и общите проекти на технически стандарти за изпълнение по параграф 1, буква б) до хх 202х г. [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените в параграф 1, буква а) общи регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

Комисията се оправомощава да приеме посочените в параграф 1, буква б) общи технически стандарти за изпълнение в съответствие с член 15 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

Член 19

Централизиране на уведомяването за съществените инциденти с ИКТ

1. В рамките на съвместния си комитет и след консултация с ЕЦБ и ENISA ЕНО изготвят съвместен доклад за оценка на осъществимостта на допълнително централизиране на уведомяването за инциденти чрез създаването на централен портал на ЕС за уведомяване от финансовите субекти за съществените инциденти с ИКТ. В доклада се проучват начините за улесняване на уведомяването за инцидентите с ИКТ, за намаляване на свързаните с това разходи и за подпомагане на тематичните проучвания с цел да се засили сближаването на надзорните практики.

2. Докладът по параграф 1 съдържа като минимум следните елементи:

   а) предварителните условия за създаването на такъв централен портал на ЕС;

   б) ползата, ограниченията и възможните рискове;

   в) елементите на оперативното управление;

   г) условията за членство;

   д) условията за достъп на финансовите субекти и националните компетентни органи до централния портал на ЕС;

   е) предварителна оценка на финансовите разходи за създаването на оперативна платформа на централния портал на ЕС, в т.ч. на необходимия експертен опит.

3. ЕНО предават на Комисията, Европейския парламент и Съвета доклада по параграф 1 до хх 202х г. [*СП: да се въведе дата — 3 години след датата на влизане в сила*].

Член 20

Обратна информация от надзорните органи

1. При получаването на доклада по член 17, параграф 1 компетентният орган потвърждава, че е бил уведомен и възможно най-бързо предоставя на финансовия субект всички необходими сведения или указания, по-специално с оглед на корективните мерки, които субектът трябва да предприеме, или на начина за свеждане до минимум на неблагоприятните последици за другите сектори.

2. В рамките на съвместния си комитет ЕНО ежегодно изготвят доклад, в който данните са анонимизирани и обобщени, за получените от компетентните органи уведомления за инцидентите с ИКТ, като посочват като минимум броя на съществените инциденти с ИКТ, техния характер, последиците за операциите на финансовите субекти или на техните клиенти, разходите и предприетите корективни мерки.

   ЕНО отправят предупреждения и изготвят статистически данни на високо равнище в подкрепа на оценяването на заплахите и на уязвимите места при ИКТ.

ГЛАВА IV

ТЕСТВАНЕ НА ОПЕРАТИВНАТА УСТОЙЧИВОСТ НА ЦИФРОВИТЕ ТЕХНОЛОГИИ

Член 21

Общи изисквания за тестването на оперативната устойчивост на цифровите технологии

1. С цел да оценят доколко са подготвени за инциденти с ИКТ, да установят слабостите, недостатъците или пропуските в оперативната устойчивост на цифровите технологии, както и с оглед на бързото прилагане на коригиращи мерки, финансовите субекти въвеждат, поддържат и актуализират стабилна и мащабна програма за тестване на оперативната устойчивост на цифровите технологии, надлежно съобразена с техния размер, профил на стопанска дейност и профил на риска; тази програма е неразделна част от посочената в член 5 рамка за управление на риска при ИКТ.

2. Програмата за тестване на оперативната устойчивост на цифровите технологии съдържа набор от оценки, тестове, методи, практики и инструменти, които се прилагат в съответствие с разпоредбите на членове 22 и 23.

3. Когато изпълняват посочената в параграф 1 програма за тестване на оперативната устойчивост на цифровите технологии, финансовите субекти следват подход, при който се отчита рискът, като взимат предвид променливото естество на рисковете при ИКТ, потенциалните или реални специфични рискове за финансовия субект, значимостта на информационните активи и на предоставяните услуги, както и всеки друг фактор, който преценят за подходящ.

4. Финансовите субекти възлагат тестването на независими страни — вътрешни или външни.

5. Финансовите субекти установяват процедури и политики за подреждане по важност, класифициране и отстраняване на всички открити при тестването проблеми, както и вътрешни методики за валидиране, така че всички установени слабости, недостатъци или пропуски да бъдат изцяло преодолени.

6. Финансовите субекти тестват всички възлови системи и приложения на ИКТ най-малко веднъж годишно.

Член 22

Тестване на инструментите и системите на ИКТ

1. Посочената в член 21 програма за тестване на оперативната устойчивост на цифровите технологии предвижда провеждането на пълен набор от подходящи тестове, в т.ч. оценка и сканиране на уязвимите места, анализ на софтуерните продукти с отворен достъп, оценка на сигурността на мрежата, анализ на пропуските, физически преглед на сигурността, анкета и сканиране на програмните продукти, когато е осъществимо — преглед на изходния код, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането, тестване по цялата верига или тестване на пробива.

2. Финансовите субекти по член 2, параграф 1, букви е) и ж) извършват оценки на уязвимите места преди внедряване или вторично внедряване на нови или съществуващи услуги за техните възлови функции, приложения и инфраструктурни компоненти.

Член 23

Обстойно тестване на инструментите, системите и процесите на ИКТ чрез тестване на проникването

1. Финансовите субекти, определени съгласно параграф 4, провеждат най-малко веднъж на 3 години обстойно тестване, като тестват проникването.

2. Минималният обхват на тестването на проникването включва възловите функции и услуги на финансовия субект, а се тестват оперативните производствени системи, поддържащи тези функции. Точният обхват на тестването на проникването, което се базира на оценката на възловите функции и услуги, се определя от финансовите субекти и се валидира от компетентните органи.

   За целите на първа алинея финансовите субекти установяват всички съответни процеси, системи и технологии на ИКТ, поддържащи възловите функции и услуги, в т.ч. функциите и услугите, възложени с договор или другояче на доставчици трети страни на услуги в областта на ИКТ.

   Когато тестването на проникването обхваща доставчици трети страни на услуги в областта на ИКТ, финансовите субекти предприемат необходимите мерки с оглед на участието на тези доставчици.

   Финансовите субекти въвеждат ефективни контролни функции при управлението на риска, за да се ограничи рискът за самите тях, за техните контрагенти или за финансовия сектор от потенциално отражение върху данните, увреждане на активите и неизправности при възловите услуги или операции.

   Когато тестването приключи и бъдат приети докладите и плановете за корективни мерки, финансовият субект и външните лица, провели тестовете, предоставят на компетентния орган документацията, с която се потвърждава, че тестването на проникването е било проведено в съответствие с изискванията. Компетентните органи валидират документацията и издават удостоверение.

3. С оглед на тестването на проникването финансовите субекти сключват договор с лица, провеждащи такива тестове, като се съобразяват с член 24.

   Когато компетентните органи определят кои финансови субекти трябва да провеждат тестове на проникването, те взимат предвид размера, мащаба, дейността и цялостния рисков профил на дадения финансов субект, които са оценили въз основа на следните елементи:

   а) фактори за отражението, по-специално значимостта на предоставяните услуги и предприетите дейности от финансовия субект;

   б) евентуални опасения за финансовата стабилност предвид системния характер на финансовия субект съответно за дадената държава членка или за Съюза;

в) свойствения за финансовия субект профил на риска, степента на рутинност на неговите ИКТ или съответните технически спецификации.

4. ЕБО, ЕОЦКП и ЕОЗППО, след като се допитат до ЕЦБ и като вземат предвид съответните съюзни правни норми за тестване на проникването въз основа на разузнавателни сведения, разработват проекти на регулаторни технически стандарти за доуточняване на:

а) използваните критерии за целите на прилагането на параграф 3 от настоящия член;

б) изискванията във връзка със:

а) посочения в параграф 2 от настоящия член обхват на тестовете на проникването;

б) тестовата методика и подход за всеки етап от тестването;

в) следните тестови етапи: резултати, приключване на процеса и корективни мерки;

в) вида на необходимото сътрудничество между надзорните органи с оглед на тестването на проникването при финансовите дружества с дейност в повече от една държава членка, така че да се осигури подходяща степен на участие на надзорните органи и гъвкаво прилагане, съобразено със спецификите на финансовите подсектори или на местните финансови пазари.

ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до [*СП: въведете дата — 2 месеца преди датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените във втора алинея регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

Член 24

Изисквания във връзка с лицата, провеждащи тестове

1. За да тестват проникването финансовите дружества прибягват само до лица, провеждащи такива тестове, които:

а) са най-подходящи за целта и са с най-добра репутация;

б) разполагат с необходимия технически и организационен капацитет и притежават специална експертни познания в областта на разследването на заплахи, тестването на проникването или тестването на защитните механизми при симулиране на реални условия (червен екип);

в) са акредитирани от съответния орган на държава членка или се придържат към официални етични кодекси или изисквания;

г) предоставят — когато лицата, провеждащи тестовете, са външни — независима гаранция или одитен доклад за доброто управление на рисковете, свързани с провеждането на тестовете на проникването, в т.ч. подходяща защита на поверителната информация на финансовия субект и средства за правна защита във връзка с рисковете за дейността на финансовия субект;

д) разполагат — когато лицата, провеждащи тестовете, са външни — с надлежно и цялостно застрахователно покритие за професионална отговорност, в т.ч. срещу риска от неправомерно поведение и небрежност.

2. Когато се договарят с външните лица, провеждащи тестове, финансовите субекти изискват резултатите от тестването на проникването да бъдат добре управлявани, както и тяхното обработване, в т.ч. генериране, описване, съхраняване, обобщаване, докладване, съобщаване или унищожаване, да не поражда риск за самите тях.

ГЛАВА V

УПРАВЛЕНИЕ НА РИСКА ПРИ ИКТ, ПОРАЖДАН ОТ ТРЕТА СТРАНА

РАЗДЕЛ I

ОСНОВНИ ПРИНЦИПИ ЗА ДОБРО УПРАВЛЕНИЕ НА РИСКА ПРИ ИКТ, ПОРАЖДАН ОТ ТРЕТА СТРАНА

Член 25

Общи принципи

Финансовите субекти управляват риска при ИКТ, пораждан от трета страна, като неразделна част от компонента „риск при ИКТ“ на своята рамка за управление на риска при ИКТ и съобразно следните принципи:

1. Финансовите субекти, които с оглед на стопанската си дейност са сключили договори за услуги в областта на ИКТ, във всеки един момент са изцяло отговорни за спазването на всички задължения по силата на настоящия регламент и на приложимото финансово законодателство, както и за преценката, че тези задължения са изпълнени.

2. Финансовите субекти управляват риска при ИКТ, пораждан от трета страна, съобразно принципа на пропорционалност, като взимат предвид:

   а) мащаба, сложността и значението на зависимостта от такива доставчици трети страни,

   б) рисковете, свързани с договорите за услуги в областта на ИКТ, сключени с доставчици трети страни на услуги в областта на ИКТ, като отчитат значението — възлово или не — на договорената услуга, процес или функция, както и потенциалното въздействие на тези рискове върху непрекъснатостта и качеството на финансовите услуги и дейности на отделния субект или според случая — на групата.

3. Като част от своята рамка за управление на риска при ИКТ финансовите субекти приемат и подлагат на редовен преглед стратегията за риска при ИКТ, пораждан от трета страна, като взимат предвид посочената в член 5, параграф 9, буква ж) стратегия за прибягване до множество доставчици на ИКТ. Тази стратегия включва политика за използването на услуги в областта на ИКТ,

предоставяни от доставчици трети страни на такива услуги, и се прилага както на индивидуална, така и, според случая, на подконсолидирана и консолидирана основа. Ръководният орган редовно преглежда установените рискове, свързани с възлагането на доставчик трета страна на възлови или важни функции.

4. Като част от своята рамка за управление на риска при ИКТ финансовите субекти поддържат и актуализират на индивидуална, подконсолидирана и консолидирана основа информационен регистър за всички договори за услуги в областта на ИКТ, сключени с доставчици трети страни на такива услуги.

Договорите по първа алинея се документират по подходящ начин, като тези, които се отнасят до възловите или важните функции, се обособяват от останалите.

Поне веднъж годишно финансовите субекти осведомяват компетентните органи за броя нови договори за услуги в областта на ИКТ, за категориите доставчици трети страни на такива услуги, за вида на договорите и за предоставяните услуги и функции.

При поискване от компетентния орган финансовите субекти му предоставят пълния информационен регистър или поисканите части от него, както и всички сведения, които компетентният орган е сметнал за необходими с оглед на упражняването на ефективен надзор върху финансовия субект.

Финансовите субекти своевременно уведомяват компетентния орган за намерението си да възложат с договор на трета страна дадена възлова или важна функция, както и когато дадена функция се е превърнала във възлова или важна.

5. Преди да сключат договор за услуги в областта на ИКТ финансовите субекти:

а) преценяват дали договорът се отнася до възлова или важна функция;

б) оценяват дали са изпълнени надзорните изисквания за договорно възлагане на дадените услуги;

в) установяват и оценяват всички съответни рискове, свързани с договора, в т.ч. вероятността с такива договори да се засили рискът от концентрация на доставчици трети страни на услуги в областта на ИКТ;

г) надлежно проверяват бъдещите доставчици трети страни на услуги в областта на ИКТ и неотклонно по време на процеса на подбор и оценка се уверяват, че даденият доставчик е подходящ;

д) установяват и оценяват конфликтите на интереси, които договорът може да породи.

6. Финансовите субекти могат да сключват договори само с доставчици трети страни на услуги в областта на ИКТ, които удовлетворяват строги, подходящи и най-актуални стандарти за сигурност на информацията.

7. Когато упражняват правата си за достъп, проверка и одит на даден доставчик трета страна на услуги в областта на ИКТ, финансовите субекти предварително определят въз основа на подход, при който е отчетен рискът, честотата на одитите и проверките, както и подлежащите на одит сфери; при това те се придържат към общоприетите одитни стандарти и към съответните указания от надзорните органи за използването и въвеждането на такива одитни стандарти.

При договорите с технически аспекти със значителна сложност финансовите субекти се уверяват, че одиторите — независимо дали са вътрешни одитори, групи от одитори или външни одитори, притежават подходящите знания и умения, за да извършат ефективно съответните одити и оценки.

8. Финансовите субекти прекратяват договорите за услуги в областта на ИКТ най-малко при следните обстоятелства:

а) ако доставчикът трета страна на услуги в областта на ИКТ наруши приложимите законови, подзаконови или договорни условия;

б) ако при наблюдението на риска при ИКТ, пораждан от трета страна, установят обстоятелства, за които смятат, че могат да променят изпълнението на предоставяните по силата на сключения договор функции, в т.ч. съществени промени, които засягат договора или положението на доставчика трета страна на услуги в областта на ИКТ;

в) ако доставчикът трета страна на услуги в областта на ИКТ не управлява задоволително риска при ИКТ, като в частност е неудовлетворителен начинът му на осигуряване на защитата и целостта на поверителните, личните или по друг начин чувствителни данни, или на информацията без личен характер;

г) ако съответният договор доведе до обстоятелства, които не позволяват на компетентния орган да упражнява ефективен надзор върху финансовия субект.

9. Финансовите субекти въвеждат изходни стратегии с оглед на рисковете, които могат да възникнат при даден доставчик трета страна на услуги в областта на ИКТ — прекратяване на дейността, влошаване на качеството на предоставяните функции, прекъсване на дейността на финансовия субект поради неподходящо или неуспешно предоставяне на услуги или възникване на съществен риск, свързан с подходящото и непрекъснатото изпълнение на функцията.

Финансовите субекти се уверяват, че могат да прекратят всеки договор, без това:

а) да наруши стопанската им дейност,

б) да ограничи спазването на регулаторните изисквания;

в) да нанесе ущърб на непрекъснатостта и качеството на предоставяните на клиентите услуги.

Изходните плановете са изчерпателни, документирани и, когато е целесъобразно, достатъчно тествани.

Финансовите субекти подготвят алтернативни решения и преходни планове за оттегляне от доставчика трета страна на услуги в областта на ИКТ на договорно възложените му функции и на съответните данни, както и за сигурното им предаване на алтернативни доставчици или за реинтегрирането им в собствените системи.

Финансовите субекти взимат подходящи извънредни мерки за осигуряване на непрекъснатостта на дейността при всички обстоятелства, посочени в първа алинея.

10. В рамките на съвместния си комитет ЕНО разработват проекти на технически стандарти за изпълнение за определяне на стандартните образци за целите на информационния регистър по параграф 4.

ЕНО предават на Комисията тези проекти на технически стандарти за изпълнение до [*СП: да се въведе дата — 1 година след датата на влизане в сила на настоящия регламент*].

Комисията се оправомощава да приеме посочените в първа алинея технически стандарти за изпълнение в съответствие с член 15 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

11. В рамките на съвместния си комитет ЕНО разработват проекти на регулаторни стандарти:

а) за доуточняване на подробното съдържание на политиката по параграф 3 във връзка с договорите за услуги в областта на ИКТ, предоставяни от доставчици трети страни на такива услуги, чрез определяне на основните етапи, през които преминава изпълнението на съответните договори за услуги в областта на ИКТ;

б) за доуточняване на сведенията, които трябва да съдържа информационният регистър по параграф 4.

ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените във втора алинея регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

Член 26

Предварителна оценка на риска от концентрация на доставчици трети страни на услуги в областта на ИКТ и на споразуменията за вторично възлагане

1. При установяването и оценяването на риска от концентрация на доставчици трети страни на услуги в областта на ИКТ, посочен в член 25, параграф 5, буква в), финансовите субекти преценяват дали даден договор за услуги в областта на ИКТ води при сключването си до следното:

а) договорно обвързване с доставчик трета страна на услуги в областта на ИКТ, което не може да бъде лесно заменено; или

б) множество договори за услуги в областта на ИКТ, сключени с един и същ доставчик трета страна на такива услуги или с тясно взаимосвързани доставчици трети страни на такива услуги.

Финансовите субекти проучват разходите и ползите от алтернативни решения — например прибягване до различни доставчици трети страни на услуги в областта на ИКТ, като преценяват дали и как разглежданите решения съответстват на потребностите и целите на тяхната дейност, както са заложени в тяхната стратегия за устойчивост на цифровите технологии.

2. Когато договорът за услуги в областта на ИКТ позволява на доставчика трета страна на такива услуги да възлага от своя страна възлова или важна функция

на друг доставчик трета страна на такива услуги, финансовите субекти преценяват потенциалната полза и рискове от такова евентуално вторично възлагане, особено когато даденият подизпълнител е установен в трета държава.

Когато договорът за услуги в областта на ИКТ е сключен с доставчик трета страна на такива услуги, установен в трета държава, финансовите субекти проучват най-малко следните фактори:

а) спазването на изискванията за защита на данните;

б) ефективното правоприлагане;

в) приложимите правни норми при несъстоятелност на доставчика трета страна на услуги в областта на ИКТ;

г) евентуалните ограничения, ако спешно им се наложи да получат обратно данните си от въпросния доставчик.

Финансовите субекти преценяват дали и как потенциално дългите или сложни вериги от подизпълнители могат да засегнат способността им да следят изцяло договорно възложените функции, както и способността на компетентния орган да упражнява върху тях ефективен надзор в тази връзка.

Член 27

Основни договорни клаузи

1. Правата и задълженията на финансовия субект и на доставчика трета страна на услуги в областта на ИКТ се определят ясно и се посочват в писмен вид. Пълният текст на договора, който включва клаузи за нивото на обслужване, се оформя в писмен документ, който е на разположение на страните на хартиен носител или в достъпен електронен формат, който може да бъде изтеглен.

2. Договорите за услуги в областта на ИКТ съдържат най-малко следното:

а) ясно и пълно описание на всички функции и услуги, които доставчикът трета страна на услуги в областта на ИКТ ще предоставя, като се посочва дали се позволява вторично възлагане на възлова или важна функция или на съществени части от нея, както и, ако такава възможност е предвидена, приложимите условия при такова вторично възлагане;

б) местата, където трябва да се предоставят договорно възложените или вторично възложените функции и услуги, както и къде трябва да се обработват и на кое място да се съхраняват данните, в т.ч. изискване за доставчика трета страна на услуги в областта на ИКТ да уведоми финансовия субект, ако възнамерява да промени тези места;

в) клаузи за достъпност, наличност, цялост, сигурност и защита на личните данни, както и за осигуряване на достъп до обработваните от финансовия субект лични данни и такива без личен характер, и за възстановяването и връщането им в лесно достъпен формат в случай на несъстоятелност, преструктуриране или прекратяване на стопанската дейност на доставчика трета страна на услуги в областта на ИКТ;

г) обстойно описание на нивото на обслужване, в т.ч. на актуализиране и преглед на предоставяните услуги, както и точни количествени и качествени цели за ефективност в рамките на договореното ниво на

обслужване, така че финансовият субект да може ефективно да следи изпълнението и ако то стане незадоволително — да предприеме възможно най-бързо подходящите коригиращи мерки;

д) задълженията на доставчика трета страна на услуги в областта на ИКТ да осведомява финансовия субект, както и съответните срокове за това, в т.ч. задължението да го уведомява за всяко обстоятелство, което може съществено да засегне способността на този доставчик ефективно да предоставя възлови или важни функции, в съответствие с договореното ниво на обслужване;

е) задължението за доставчика трета страна на услуги в областта на ИКТ да предоставя поддръжка при инцидент с ИКТ, без това да води за финансовия субект до допълнителни — или над предварително определените — разходи;

ж) изискване към доставчиците трети страни на услуги в областта на ИКТ да прилагат и тестват планове за действие при извънредни ситуации, както и да разполагат с мерки, инструменти и политики за сигурност на ИКТ, които адекватно да гарантират сигурното предоставяне на услуги от финансовия субект, както е предвидено в нормативната му уредба;

з) правото на финансовия субект текущо да наблюдава ефективността на доставчика трета страна на услуги в областта на ИКТ, което включва:

i) правото на достъп, проверка и одит от страна на финансовия субект или от определено трето лице, както и правото на копиране на съответните документи — стига други договорки или самото изпълняване на договора да не възпрепятстват или ограничават ефективното упражняване на това право;

ii) правото да се поискат алтернативни нива на сигурност, ако са засегнати права на други клиенти на финансовия субект;

iii) задължение за доставчика трета страна на услуги в областта на ИКТ напълно да сътрудничи на финансовия субект при извършваните от последния проверки на място — като в договора се посочат обхватът, условията и честотата на дистанционните одити;

и) задължението за доставчика трета страна на услуги в областта на ИКТ напълно да сътрудничи на компетентните органи и органите за преструктуриране на финансовия субект, в т.ч. на определените от тях лица;

й) правото на прекратяване на договора и свързаните с него минимални срокове за предизвестие — съобразно очакванията на компетентните органи;

к) изходни стратегии, по-специално определяне на задължителен подходящ преходен период:

а) по време на който доставчикът трета страна на услуги в областта на ИКТ продължава да предоставя съответните функции или услуги с цел да се ограничи рискът за финансовия субекти от нарушаване на дейността;

б) който позволява на финансовия субект да се прехвърли към друг доставчик трета страна на услуги в областта на ИКТ или да внедри собствени решения съобразно сложността на предоставяната услуга.

3. Когато се договарят, финансовите субекти и доставчиците трети страни на услуги в областта на ИКТ обмислят използването на стандартни договорни клаузи, разработени за конкретни услуги.

4. В рамките на съвместния си комитет ЕНО разработват проекти на регулаторни технически стандарти за доуточняване на елементите, които финансовите субекти трябва да определят и оценят при вторично възлагане на възлови или важни функции, така че пълноценно да бъдат спазени разпоредбите на параграф 2, буква а).

ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените в първа алинея регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1095/2010 и Регламент (ЕС) № 1094/2010.

РАЗДЕЛ II

НАДЗОРНА РАМКА ЗА ВЪЗЛОВИТЕ ДОСТАВЧИЦИ ТРЕТИ СТРАНИ НА УСЛУГИ В ОБЛАСТТА НА ИКТ

Член 28

Определяне на възловите доставчици трети страни на услуги в областта на ИКТ

1. В рамките на съвместния си комитет и по препоръка на създадения с член 29, параграф 1 надзорен форум ЕНО:

а) определят по посочените в параграф 2 критерии възловите за финансовите субекти доставчици трети страни на услуги в областта на ИКТ;

б) за всеки възлов доставчик трета страна на услуги в областта на ИКТ определят за водещ надзорник обхванатите съответно от Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 или Регламент (ЕС) № 1095/2010 ЕБО, ЕОЦКП или ЕОЗППО — в зависимост от това дали стойността на съвкупните активи на финансовите субекти, които ползват услугите на този възлов доставчик, е над половината от стойността на съвкупните активи на всички финансови субекти, които ползват услугите на дадения възлов доставчик — като сравнението се прави въз основа на консолидираните счетоводни баланси на тези финансови субекти или на отделните счетоводни баланси, ако балансите не са консолидирани.

2. Определянето по параграф 1, буква а) се извършва по следните критерии:

а) системното въздействие върху стабилността, непрекъснатостта или качеството на предоставяните финансови услуги, в случай че даден доставчик трета страна на услуги в областта на ИКТ бъде изправен пред

мащабна оперативна неспособност да предоставя услугите си — предвид броя финансови субекти, които се ползват от услугите му;

б) системния характер или значение на финансовите субекти, които обслужва даденият доставчик трета страна на услуги в областта на ИКТ — те се оценяват по следните параметри:

i) броя глобални системно значими институции (Г-СЗИ) или други системно значими институции (Д-СЗИ), които обслужва съответният доставчик трета страна на услуги в областта на ИКТ;

ii) взаимозависимостта между посочените в подточка i) Г-СЗИ или Д-СЗИ и други финансови субекти, в т.ч. ситуациите, при които Г-СЗИ или Д-СЗИ предоставят на други финансови субекти услуги, свързани с финансовата инфраструктура;

в) степента, в която възловите или важните функции на даден финансов субект зависят от услугите, предоставяни от един и същ доставчик трета страна на услуги в областта на ИКТ, без значение дали тази зависимост е пряка, непряка или възникнала поради вторично възлагане на вече възложени услуги;

г) степента, в която даден доставчик трета страна на услуги в областта на ИКТ може да бъде заменен — тя се оценява по следните параметри:

i) отсъствие на реална, дори частична, алтернатива поради: ограничения брой присъстващи на съответния пазар доставчици трети страни на услуги в областта на ИКТ; пазарния дял на дадения такъв доставчик; наличието на висока техническа или друга сложност, в т.ч. използването от дадения доставчик на собствена технология; спецификата на организацията или дейността на дадения доставчик;

ii) трудно частично или пълно прехвърляне на съответните данни и работно натоварване от дадения доставчик трета страна на услуги в областта на ИКТ към друг доставчик на такива услуги поради значителния ресурс — финансови разходи, време или друг ресурс, който прехвърлянето може да изиска, или поради увеличаване в резултат на прехвърлянето на рисковете при ИКТ или на други оперативни рискове за финансовия субект;

д) броя държави членки, в които извършва дейност даденият доставчик трета страна на услуги в областта на ИКТ;

е) броя държави членки, в които извършват дейност финансовите субекти, ползващи дадения доставчик трета страна на услуги в областта на ИКТ.

3. Комисията се оправомощава да приема делегирани актове по силата на член 50, за да допълва изискванията в параграф 2.

4. Към определянето по параграф 1, буква а) се пристъпва само след като Комисията приеме делегиран акт по силата на параграф 3.

5. Определянето по параграф 1, буква а) не се прави за доставчиците трети страни на услуги от областта на ИКТ, които са обхванати от надзорни рамки, създадени с оглед на задачите, посочени в член 127, параграф 2 от Договора за функционирането на Европейския съюз.

6. Чрез съвместния си комитет ЕНО съставят, публикуват и годишно актуализират списък на възловите за Съюза доставчици трети страни на услуги в областта на ИКТ.

7. За целите на параграф 1, буква а) компетентните органи ежегодно и в обобщен вид предават на създадения с член 29 надзорен форум информацията, посочена в член 25, параграф 4. Въз основа на получената от компетентните органи информация надзорният форум оценява зависимостта на финансовите субекти от доставчици трети страни на услуги в областта на ИКТ.

8. Доставчиците трети страни на услуги в областта на ИКТ, които не са включени в посочения в параграф 6 списък, могат да поискат да бъдат включени в него.

За целите на първа алинея даденият доставчик трета страна на услуги в областта на ИКТ подава до ЕБО, ЕОЦКП или ЕОЗППО обосновано заявление; посочените органи решават в рамките на съвместния си комитет дали в съответствие с параграф 1, буква а) да го включат в този списък.

Решението, посочено във втора алинея, се приема и съобщава на доставчика трета страна на услуги в областта на ИКТ в 6-месечен срок, считано от получаването на заявлението.

9. Финансовите субекти не използват доставчици трети страни на услуги в областта на ИКТ, установени в трета държава, които, ако бяха установени в Съюза, щяха да бъдат определени по силата на параграф 1, буква а) като възлови.

Член 29

Структура на надзорната рамка

1. По силата на член 57 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010 съвместният комитет създава надзорен форум като свой подкомитет, който да подпомага неговата работа и тази на водещия надзорник, посочен в член 28, параграф 1, буква б), по въпросите на риска при ИКТ, пораждан от трета страна, за финансовите сектори. Надзорният форум подготвя проектите за съвместни позиции и общите актове на съвместния комитет в тази сфера.

В надзорния форум редовно се обсъждат съответните обстоятелства във връзка с рисковете при ИКТ и с уязвимите места на ИКТ, като се насърчава последователен подход за наблюдаване на равнището на Съюза на риска при ИКТ, пораждан от трета страна.

2. Надзорният форум ежегодно прави колективна оценка на резултатите и констатациите от надзорните действия, проведени за всички възлови доставчици трети страни на услуги в областта на ИКТ, и насърчава координационни мерки за подобряване на оперативната устойчивост на цифровите технологии на финансовите субекти, за възприемане на най-добрите практики с оглед на рисковете от концентрация на доставчици трети страни на услуги в областта на ИКТ и за проучване на начините за ограничаване на прехвърлянето на рисковете от един сектор в друг.

3. Надзорният форум представя на съвместния комитет общи референтни показатели за възловите доставчици трети страни на услуги в областта на ИКТ, които показатели съвместният комитет да приеме като съвместни позиции на

ЕНО по силата на член 56, параграф 1 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010.

4. Надзорният форум се състои от председателите на ЕНО и от по един високопоставен представител на настоящия персонал на съответния компетентен орган на всяка държава членка. В надзорния форум като наблюдатели участват изпълнителните директори на всеки ЕНО, както и един представител от Европейската комисия, от ЕССР, от ЕЦБ и от ENISA.

5. По силата на член 16 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010 ЕНО отправят насоки за сътрудничеството си с компетентните органи за целите на настоящия раздел, в които подробно се излагат приложимите за двете страни процедури и условия във връзка с изпълнението на задачите, както и начинът, по който се обменя информацията, нужна за компетентните органи с оглед на съответни действия по препоръките, отправени от водещите надзорници по силата на член 31, параграф 1, буква г) към възловите доставчици трети страни на услуги в областта на ИКТ.

6. Изискванията в настоящия раздел не засягат прилагането на Директива (ЕС) 2016/1148, нито на другите надзорни норми на Съюза, приложими за доставчиците на компютърни услуги „в облак“.

7. Чрез съвместния си комитет и въз основа на подготвителната работа на надзорния форум ЕНО ежегодно представят на Европейския парламент, Съвета и Комисията доклад за прилагането на настоящия раздел.

Член 30

Задачи на водещия надзорник

1. Водещият надзорник оценява дали всеки възлов доставчик трета страна на услуги в областта на ИКТ разполага с подробни, надеждни и ефективни правила, процедури, механизми и договорености за управление на рисковете при ИКТ, които може да породи за финансовите субекти.

2. Оценката по параграф 1 обхваща:

   а) задълженията във връзка с ИКТ с оглед по-специално на сигурността, наличността, непрекъснатостта, капацитета за увеличаване и качеството на предоставяните на финансовите субекти услуги в областта на ИКТ от доставчиците трети страни на такива услуги, както и способността неотклонно да се спазват строги стандарти за сигурност, поверителност и цялост на данните;

   б) сигурността на физическото оборудване (помещения, оборудване, центрове за данни), която подхранва сигурността на ИКТ;

   в) управляването на риска, в т.ч. политиката за управление на риска при ИКТ и плановете за непрекъснато функциониране на ИКТ и за възстановяване на информацията при срив на ИКТ;

   г) управленските механизми за ефективно управляване на риска при ИКТ, в т.ч. организационна структура с ясни, прозрачни и последователни области на отговорност и правила за отчетността;

д) установяването, наблюдаването и своевременното уведомяване на финансовите субекти за инцидентите с ИКТ, управляването и разрешаването на такива инциденти, в частност — на кибератаките;

е) механизмите за преносимост на данните и приложенията и за оперативна съвместимост, с които на финансовите субекти се позволява ефективно да упражняват правото си да прекратят деловите взаимоотношения;

ж) тестването на системите, инфраструктурата и контролните механизми на ИКТ;

з) одитите на ИКТ;

и) използването на съответни национални и международни стандарти за предоставянето на услуги в областта на ИКТ на финансовите субекти.

3. Въз основа на оценката по параграф 1 водещият надзорник приема за всеки възлов доставчик трета страна на услуги в областта на ИКТ ясен, подробен и обоснован индивидуален надзорен план. Този план се съобщава всяка година на възловия доставчик трета страна на услуги в областта на ИКТ.

4. След договарянето на годишните надзорни планове по параграф 3 и съобщаването им на възловите доставчици трети страни на услуги в областта на ИКТ компетентните органи могат да приемат мерки спрямо тези възлови доставчици само в съгласие с водещия надзорник.

Член 31

Правомощия на водещия надзорник

1. За изпълнението на предвидените в настоящия раздел задачи водещият надзорник разполага със следните правомощия:

а) да изисква цялата съответна информация и документация по силата на член 32;

б) да провежда общи разследвания и проверки по силата на членове 33 и 34;

в) да изисква след приключване на надзорните действия доклади, в които да са посочени предприетите от възловите доставчици трети страни на услуги в областта на ИКТ действия или корективни мерки по посочените в буква г) от настоящия параграф препоръки;

г) да отправя препоръки в областите, посочени в член 30, параграф 2, по-специално за следното:

i) използване на специфични изисквания или процеси за сигурност и качество на ИКТ, по-специално за въвеждане на софтуерни пачове, актуализиране, криптиране и други мерки за защита, които водещият надзорник счита за необходими с оглед на сигурността на услугите в областта на ИКТ, предоставяни на финансовите субекти;

ii) използване на условия и изисквания — като се отчита и техническото им изпълнение, които възловите доставчици трети страни на услуги в областта на ИКТ трябва да съблюдават, когато предоставят такива услуги на финансовите субекти, и които водещият надзорник смята, че са необходими, за да се предотврати появата или разрастването на точки, повредата в които може да

доведе до общ срив, или за да се сведе до минимум възможното системно въздействие върху финансовия сектор на Съюза на материализирал се риск от концентрация на доставчици трети страни на услуги в областта на ИКТ;

iii) проучване, в съответствие с членове 32 и 33, на споразуменията за вторично възлагане, в т.ч. на тези, които възловите доставчици трети страни на услуги в областта на ИКТ възнамеряват да сключат с доставчици трети страни на такива услуги или с установени в трета държава поддоставчици на ИКТ, както и на всяко планирано вторично възлагане — с договор или другояче, за което водещият надзорник смята, че може да породи рискове за предоставяните от финансовия субект услуги или за финансовата стабилност;

iv) въздържане от вторично възлагане, ако са изпълнени кумулативно следните условия:

– предвиденият подизпълнител е доставчик трета страна на услуги в областта на ИКТ или установен в трета държава поддоставчик на ИКТ;

– вторичното възлагане се отнася до възлова или важна функция на финансовия субект.

2. Преди да упражни свое посочено в параграф 1 правомощие водещият надзорник се допитва до надзорния форум.

3. Възловите доставчици трети страни на услуги в областта на ИКТ сътрудничат добросъвестно с водещия надзорник и му съдействат в изпълнението на задачите му.

4. Водещият надзорник може да налага периодични наказателни плащания на възловите доставчици трети страни на услуги в областта на ИКТ, които не спазват разпоредбите на параграф 1, букви а), б) и в).

5. Периодичните наказателни плащания по параграф 4 се начисляват ежедневно докато разпоредбите не започнат да се спазват, но не по-дълго от шест месеца, след като даденият възлов доставчик трета страна на услуги в областта на ИКТ е бил уведомен за тях.

6. Размерът на периодичните наказателни плащания се изчислява от датата, посочена в решението за налагането им, и представлява 1 % от средния дневен световен оборот на възловия доставчик трета страна на услуги в областта на ИКТ през предходната финансова година.

7. Наказателните плащания са административна мярка и подлежат на принудително изпълнение. Принудителното изпълнение се урежда от действащите гражданскопроцесуални норми на държавата членка, на чиято територия се извършват проверките и достъпът. Съдилищата на съответната държава членка са компетентни да разглеждат жалбите за неправомерно правоприлагане. Събраните периодични наказателни плащания се внасят в общия бюджет на Европейския съюз.

8. ЕНО оповестяват публично всички периодични наказателни плащания, стига такова оповестяване да не застрашава сериозно финансовите пазари, нито да причинява несъразмерно голяма вреда на засегнатите страни.

9. Преди да наложи периодичните наказателни плащания по параграф 4, водещият надзорник дава възможност на представителите на възловия доставчик трета страна на услуги в областта на ИКТ, срещу когото е възбудено дело, да бъдат изслушани във връзка с констатациите и основава решението си само на тези констатации, които въпросният доставчик е имал възможност да коментира. Правото на защита на страната, срещу която е възбудено дело, се съблюдава строго в хода на производството. Тя има право на достъп до преписката по делото при зачитане на законния интерес на други лица от опазване на търговските им тайни. Правото на достъп до преписката не се отнася до поверителната информация, нито до вътрешните подготвителни документи на водещия надзорник.

Член 32

Искане на информация

1. Водещият надзорник може с обикновено искане или с решение да поиска от възлов доставчик трета страна на услуги в областта на ИКТ да му предостави всички необходими за изпълнението на задълженията му по настоящия регламент сведения, в т.ч. всички съответни делови или оперативни документи, договори, документация за политиките, одиторски доклади за сигурността на ИКТ, доклади за инцидентите с ИКТ, както и всяка информация за лицата, на които даденият възлов доставчик вторично е възложил оперативни функции или дейности.

2. Когато по силата на параграф 1 водещият надзорник изпраща обикновено искане за информация, той:

   а) се позовава на настоящия член като правно основание за искането;

   б) посочва целта на искането;

   в) уточнява каква информация се изисква;

   г) определя срока за предоставяне на информацията;

   д) уведомява представителя на възловия доставчик трета страна на услуги в областта на ИКТ, от когото се иска информация, че не е задължен да я предостави, но че ако доброволно реши да го направи, предоставената информация трябва да бъде точна и неподвеждаща.

3. Когато по силата на параграф 1 водещият надзорник изисква да му се предостави дадена информация, той:

   а) се позовава на настоящия член като правно основание за искането;

   б) посочва целта на искането;

   в) уточнява каква информация се изисква;

   г) определя срока за предоставяне на информацията;

   д) посочва предвидените в член 31, параграф 4 периодични наказателни плащания при предоставяне на непълна информация;

   е) посочва предвиденото в членове 60 и 61 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010 право на обжалване на решението пред апелативния съвет на ЕНО и на оспорването му пред Съда на Европейския съюз („Съда“).

4. Представителите на възловия доставчик трета страна на услуги в областта на ИКТ предоставят исканата информация. Надлежно упълномощени адвокати могат да предоставят информацията от името на своите клиенти. Възловият доставчик трета страна на услуги в областта на ИКТП носи пълната отговорност за предоставена непълна, неточна или подвеждаща информация.

5. Водещият надзорник незабавно изпраща копие от решението, с което се изисква да му се предостави информация, на компетентните органи на финансовите субекти, които ползват услугите на дадения възлов доставчик трета страна на услуги в областта на ИКТ.

Член 33

Общи разследвания

1. С оглед на задачите си по настоящия регламент водещият надзорник, подпомаган от посочения в член 34, параграф 1 разследващ екип, може да извършва необходимите разследвания на доставчиците трети страни на услуги в областта на ИКТ.

2. Водещият надзорник разполага със следните правомощия:

   а) да проверява документи, данни, процедури и други материали с отношение към изпълнението на неговите задачи, независимо от носителя, на който се съхраняват;

   б) да взима или получава заверени копия или извлечения от такива документи, данни, процедури и други материали;

   в) да призовава представителите на възловия доставчик трета страна на услуги в областта на ИКТ да дават устно или писмено обяснение на факти или документи, свързани с предмета и целта на разследването, и да записва отговорите;

   г) да задава въпроси на всяко друго физическо или юридическо лице, което даде съгласие за това, с цел да събере информация, свързана с предмета на разследването;

   д) да изисква записи на телефонни разговори и регистрирани преноси на данни.

3. Служителите и другите лица, оправомощени от водещия надзорник за целите на разследванията по параграф 1, упражняват правомощията си след представяне на писмено разрешение, в което са посочени предметът и целта на даденото разследване.

   В разрешението се посочват и предвидените в член 31, параграф 4 периодични наказателни плащания, в случай че изисканите записи, данни, процедури или други материали, или отговорите на въпросите, поставени на представителите на възловия доставчик трета страна на услуги в областта на ИКТ, не бъдат представени или бъдат непълни.

4. Представителите на възловите доставчици трети страни на услуги в областта на ИКТ са длъжни да се подчинят на всяко разследване, разпоредено с решение на водещия надзорник. В решението се посочват предметът и целта на разследването, предвидените в член 31, параграф 4 периодични наказателни плащания, средствата за правна защита, предвидени в Регламент (ЕС)

№ 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010, както и правото на оспорване на решението пред Съда.

5. В разумен срок преди да започне разследването водещият надзорник съобщава на компетентните органи на финансовите субекти, които ползват услугите на дадения доставчик трета страна на услуги в областта на ИКТ, че такова предстои, както и самоличността на оправомощените лица.

Член 34

Проверки на място

1. С оглед на задачите си по настоящия регламент водещият надзорник, подпомаган от посочения в член 35, параграф 1 разследващ екип, може да влиза и извършва всички необходими проверки на място във всички търговски помещения, терени или имоти на доставчиците трети страни на услуги в областта на ИКТ — седалища, оперативни центрове, допълнителни помещения, както и да извършва проверки извън работното място.

2. Служителите на водещия надзорник и другите оправомощени от него лица да извършват проверки на място могат да влизат във всички търговски помещения, терени или имоти и разполагат с правомощието да запечатват всякакви служебни помещения, счетоводни книги или документи за срока и в степента, необходими за проверката.

   Ако представителите на даден доставчик трета страна на услуги в областта на ИКТ не се подчинят на дадена проверка, тези лица упражняват правомощията си след представяне на писмено разрешение, в което са посочени предметът и целта на проверката, както и предвидените в член 31, параграф 4 периодични наказателни плащания.

3. В разумен срок преди да започне проверката водещият надзорник уведомява компетентните органи на финансовите субекти, които ползват услугите на дадения доставчик трета страна на услуги в областта на ИКТ.

4. Проверките обхващат изцяло съответните системи на ИКТ, мрежи, устройства, информация и данни, използвани или подпомагащи предоставянето на услуги на финансовите субекти.

5. Преди всяко планирано посещение на място водещият надзорник предизвестява в разумен срок дадения възлов доставчик трета страна на услуги в областта на ИКТ, освен ако такова предизвестие не е възможно поради извънредна или кризисна ситуация или ако с това би се накърнила ефективността на проверката или одита.

6. Възловият доставчик трета страна на услуги в областта на ИКТ се подчинява на всяка проверка на място, разпоредена с решение на водещия надзорник. В решението се посочват предметът и целта на проверката, датата, на която тя ще започне, предвидените в член 31, параграф 4 периодични наказателни плащания, средствата за правна защита, предвидени в Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010, както и правото на оспорване на решението пред Съда.

7. Ако служителите на водещия надзорник и другите оправомощени от него лица установят, че даден възлов доставчик трета страна на услуги в областта на ИКТ се противопоставя на проверка, разпоредена по реда на настоящия член,

водещият надзорник уведомява този доставчик за последиците от такова противопоставяне, в т.ч. за възможността компетентните органи на съответните финансови субекти да прекратят сключените с него договори.

Член 35

Текущ надзор

1. При извършването на общи разследвания или проверки на място водещите надзорници се подпомагат от съвместен разследващ екип, който се сформира за всеки възлов доставчик трета страна на услуги в областта на ИКТ.

2. Съвместният разследващ екип по параграф 1 наброява максимум 10 души и се състои от служители на водещия надзорник и на съответните компетентни органи, които упражняват надзор върху ползващите услугите на този възлов доставчик финансови субекти; членовете на екипа участват в подготовката и провеждането на надзорните действия. Всички членове на съвместния разследващ екип трябва да притежават експертен опит в сферата на ИКТ и операционния риск. Работата на съвместния разследващ екип се координира от определен за целта служител на ЕНО („координатор на водещия надзорник“).

3. В рамките на съвместния си комитет ЕНО разработват проекти на регулаторни технически стандарти за доуточняване на начина на определяне на членовете на съвместния разследващ екип, които са служители на съответните компетентни органи, както и на задачите и реда и условията на работа на разследващия екип. ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

   Комисията се оправомощава да приеме посочените в първа алинея регулаторни технически стандарти в съответствие с членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010.

4. В рамките на 3 месеца след като приключи дадено разследване или проверка на място и след като се допита до надзорния форум водещият надзорник приема в упражняване на правомощията си по силата на член 31 препоръки, които отправя към възловия доставчик трета страна на услуги в областта на ИКТ.

5. Препоръките по параграф 4 се съобщават незабавно на възловия доставчик трета страна на услуги в областта на ИКТ и на компетентните органи на ползващите услугите му финансови субекти.

   С оглед на надзорните си действия водещият надзорник може да взима под внимание съответни издадени от трети страни удостоверения и вътрешни или външни одиторски доклади за ИКТ, предоставени от възловия доставчик трета страна на услуги в областта на ИКТ.

Член 36

Хармонизиране на условията за упражняване на надзора

1. В рамките на съвместния си комитет ЕНО разработват проекти на регулаторни технически стандарти за:

а) информацията, която възлов доставчик трета страна на услуги в областта на ИКТ, който желае да се възползва от предвидената в член 28, параграф 8 възможност, трябва да предостави в заявлението си;

б) съдържанието и формàта на докладите, които могат да бъдат поискани за целите на член 31, параграф 1, буква в);

в) начина на представяне на информацията — в т.ч. структура, формати и методи, която възловите доставчици трети страни на услуги в областта на ИКТ трябва по силата на член 31, параграф 1 да подават, оповестяват или докладват;

г) оценяването, което по силата на член 37, параграф 2 компетентните органи извършват на мерките, предприети от възловите доставчици трети страни на услуги в областта на ИКТ вследствие на препоръките на водещия надзорник.

2. ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до 1 януари 20xx г. [*СП: да се въведе дата — 1 година след датата на влизане в сила*].

Комисията се оправомощава да допълни настоящия регламент, като приеме посочените в първа алинея регулаторни технически стандарти по процедурата, посочена в членове 10—14 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010.

Член 37

Последващи действия на компетентните органи

1. В рамките на 30 календарни дни от получаването на отправените от водещия надзорник по силата на член 31, параграф 1, буква г) препоръки възловите доставчици трети страни на услуги в областта на ИКТ го уведомяват дали възнамеряват да ги следват. Водещият надзорник незабавно предава тази информация на компетентните органи.

2. Компетентните органи следят дали финансовите субекти взимат предвид рисковете, установени в отправените от водещия надзорник по силата на член 31, параграф 1, буква г) препоръки към възловите доставчици трети страни на услуги в областта на ИКТ.

3. Компетентен орган може по силата на член 44 да изиска от финансов субект временно да престане, частично или изцяло, да използва или да внедрява услуга, предоставяна от даден възлов доставчик трета страна на услуги в областта на ИКТ, докато не бъдат отстранени рисковете, установени в отправените към същия доставчик препоръки. Когато е необходимо, той може да изиска от финансовия субект да прекрати, частично или изцяло, съответните договори, сключени с възловия доставчик трета страна на услуги в областта на ИКТ.

4. Когато взима решенията, посочени в параграф 3, компетентният орган отчита вида и размера на риска, на който възловият доставчик трета страна на услуги в областта на ИКТ не е обърнал внимание, както и доколко сериозно е неспазването, като взима предвид следните критерии:

а) тежестта и продължителността на неспазването;

б) дали неспазването е разкрило сериозни слабости в процедурите, системите за управление, управлението на риска и вътрешния контрол на възловия доставчик трета страна на услуги в областта на ИКТ;

в) дали неспазването е благоприятствало, предизвикало или по друг начин довело до финансово престъпление;

г) дали неспазването е било умишлено или поради небрежност.

5. Компетентните органи редовно осведомяват водещите надзорници за предприетите в хода на надзора върху финансовите субекти подходи и мерки, както и за договорните стъпки, предприети от тези финансови субекти в случай на частично или цялостно пренебрегване от страна на възловите доставчици трети страни на услуги в областта на ИКТ на отправените от водещите надзорници препоръки.

Член 38

Надзорни такси

1. ЕНО начисляват на възловите доставчици трети страни на услуги в областта на ИКТ такси, които изцяло покриват надзорните разходи при изпълнението на предвидените в настоящия регламент задачи, в т.ч. възстановяване на разходите, които могат да възникнат в резултат на работата на компетентните органи, които участват в надзорните действия по силата на член 35.

Таксата, която се начислява на възлов доставчик трета страна на услуги в областта на ИКТ, покрива всички административни разходи и е съобразена с неговия оборот.

2. Комисията се оправомощава да приема по силата на член 50 делегирани актове за допълнение на настоящия регламент, с които да определя размера на таксите и начина на плащането им.

Член 39

Международно сътрудничество

1. По силата на член 33 от, съответно, Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010 ЕБО, ЕОЦКП и ЕОЗППО могат да сключват административни споразумения с регулаторните и надзорните органи на трети държави за насърчаване на международното сътрудничество във връзка с риска при ИКТ, пораждан от трета страна, в различните финансови сектори, в частност чрез разработването на най-добри практики за преглед на практиките и контролните механизми за управление на риска при ИКТ, мерки за ограничаване на риска и ответни действия при инциденти.

2. Всеки пет години ЕНО чрез съвместния си комитет представят на Европейския парламент, Съвета и Комисията съвместен поверителен доклад, в който се обобщават резултатите от съответните обсъждания с посочените в параграф 1 органи на трети държави с акцент върху развитието на риска при ИКТ, пораждан от трета страна, и последиците за финансовата стабилност, целостта на пазара, защитата на инвеститорите или функционирането на единния пазар.

ГЛАВА VI

СПОРАЗУМЕНИЯ ЗА ОБМЕН НА ИНФОРМАЦИЯ

Член 40

Споразумения за обмен на информация и разузнавателни сведения за киберзаплахи

1. Финансовите субекти могат да обменят помежду си информация и разузнавателни сведения за киберзаплахи, в т.ч. показатели за застрашена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране, доколкото този обмен на информация и разузнавателни сведения:

   а) има за цел да подобри оперативната устойчивост на цифровите технологии на финансовите субекти, по-специално чрез повишаване на осведомеността за киберзаплахите, ограничаване или възпрепятстване на способността на киберзаплахите да се разпространяват, подпомагане на аспекти на защитния капацитет на финансовите субекти, на техниките за откриване на заплахи, на стратегиите за ограничаване на риска или на етапите на ответни действия и на възстановяване на информацията;

   б) се извършва в ползващи се с доверие общности от финансови субекти;

   в) се извършва чрез споразумения за обмен на информация, които защитават потенциално чувствителния характер на споделената информация и се подчиняват на етични правила при пълно зачитане на търговската тайна, защитата на личните данни[48] и насоките за политиката в областта на конкуренцията[49].

2. За целите на параграф 1, буква в), в споразуменията за обмен на информация се определят условията за участие, а когато е целесъобразно — условията за участието на публични органи и качеството, в което те могат да бъдат приобщени към споразуменията за споделяне на информация, както и оперативните елементи, в т.ч. използването на специални информационни платформи.

3. Финансовите субекти уведомяват компетентните си органи при потвърждаване на членството им в споразумение за обмен на информация по параграф 1 или съответно — при ефективното му прекратяване.

ГЛАВА VII

КОМПЕТЕНТНИ ОРГАНИ

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

[49] Съобщение на Комисията — Насоки относно приложимостта на член 101 от Договора за функционирането на Европейския съюз по отношение на споразуменията за хоризонтално сътрудничество (ОВ C 11, 14.1.2011 г., стр. 1).

Член 41

Компетентни органи

Без да се засягат разпоредбите, отнасящи се до посочената в глава V, раздел II от настоящия регламент надзорна рамка за възловите доставчици трети страни на услуги в областта на ИКТ, спазването на задълженията, въведени с настоящия регламент, се осигурява от следните компетентни органи, оправомощени със съответните правни актове:

а) за кредитните институции — от компетентния орган, определен в изпълнение на член 4 от Директива 2013/36/ЕС, без да се засягат специфичните задачи, възложени на ЕЦБ с Регламент (ЕС) № 1024/2013;

б) за доставчиците на платежни услуги — от компетентния орган, определен в изпълнение на член 22 от Директива (ЕС) 2015/2366;

в) за институциите за електронни пари — от компетентния орган, определен в изпълнение на член 37 от Директива 2009/110/ЕО;

г) за инвестиционните посредници — от компетентния орган, определен в изпълнение на член 4 от Директива (ЕС) 2019/2034;

д) за доставчиците на услуги за криптоактиви, емитентите на криптоактиви, емитентите на токени, обезпечени с активи, и емитентите на значими токени, обезпечени с активи — от компетентния орган, определен съгласно член 3, параграф 1, буква дд), първо тире от [*Регламент (ЕС) 20xx — Регламент относно пазарите на криптоактиви*];

е) за централните депозитари на ценни книжа — от компетентния орган, определен в изпълнение на член 11 от Регламент (ЕС) № 909/2014;

ж) за централните контрагенти — от компетентния орган, определен в изпълнение на член 22 от Регламент (ЕС) № 648/2012;

з) за местата на търговия и доставчиците на услуги за докладване на данни — от компетентния орган, определен в изпълнение на член 67 от Директива 2014/65/ЕС;

и) за регистрите на трансакции — от компетентния орган, определен в изпълнение на член 55 от Регламент (ЕС) № 648/2012;

й) за лицата, управляващи алтернативни инвестиционни фондове — от компетентния орган, определен в изпълнение на член 44 от Директива 2011/61/ЕС;

к) за управляващите дружества — от компетентния орган, определен в изпълнение на член 97 от Директива 2009/65/ЕО;

л) за застрахователните и презастрахователните дружества — от компетентния орган, определен в изпълнение на член 30 от Директива 2009/138/ЕО;

м) за застрахователните посредници, презастрахователните посредници и посредниците, които предлагат застрахователни продукти като допълнителна дейност — от компетентния орган, определен в изпълнение на член 12 от Директива (ЕС) 2016/97;

н) за институциите за професионално пенсионно осигуряване — от компетентния орган, определен в изпълнение на член 47 от Директива (ЕС) 2016/2341;

о) за агенциите за кредитен рейтинг — от компетентния орган, определен в изпълнение на член 21 от Регламент (ЕО) № 1060/2009;

п) за задължителните одитори и одиторските дружества — от компетентния орган, определен в изпълнение на член 3, параграф 2 и член 32 от Директива 2006/43/ЕО;

р) за администраторите на критични бенчмаркове — кот компетентния орган, определен в изпълнение на членове 40 и 41 от *Регламент xx/202x*;

с) за доставчиците на услуги за колективно финансиране — от компетентния орган, определен в изпълнение на *член x от Регламент xx/202x*;

т) за регистрите на секюритизации — от компетентния орган, определен в изпълнение на член 10 и член 14, параграф 1 от Регламент (ЕС) 2017/2402.

Член 42

Сътрудничество със структурите и органите, създадени по силата на Директива (ЕС) 2016/1148

1. С оглед на по-тясното сътрудничество и обмена на надзорни данни между определените по силата на настоящия регламент компетентни органи и групата за сътрудничество, създадена по силата на член 11 от Директива (ЕС) 2016/1148, ЕНО и компетентните органи могат да поискат да участват в работата на групата за сътрудничество.

2. При необходимост компетентните органи могат да провеждат консултации с посочените съответно в членове 8 и 9 от Директива (ЕС) 2016/1148 единни звена за контакт и национални екипи за реагиране при инциденти с компютърната сигурност.

Член 43

Симулации, комуникация и сътрудничество сред финансовите сектори

1. ЕНО, чрез съвместния комитет и в сътрудничество с компетентните органи, ЕЦБ и ЕССР, могат да създадат механизми за споделяне на ефективните практики сред финансовите сектори, за да се повишава осведомеността за възникващите ситуации и да се установят общите за секторите уязвими места и рискове, свързани с кибернетичното пространство.

Те могат да разработят симулационни сценарии за управление на кризи и действие при извънредни ситуации в резултат на кибератаки, с цел да се изградят комуникационни канали и постепенно да се създадат условия за ефективни координирани ответни действия на равнище ЕС при мащабен трансграничен инцидент с ИКТ или свързана с него заплаха, които имат системно въздействие върху целия финансов сектор на Съюза.

При необходимост при тези симулации може да се тества и зависимостта на финансовия сектор от други икономически сектори.

2. Компетентните органи, ЕБО, ЕОЦКП или ЕОЗППО и ЕЦБ си сътрудничат тясно и обменят информация с оглед на задълженията си по членове 42—48. Те координират тясно надзорните си дейности, за да установяват и отстраняват нарушения на настоящия регламент, разработват и насърчават добри практики, улесняват сътрудничеството, стимулират последователност при тълкуването и предоставят валидни за различните юрисдикции оценки в случай на несъгласие.

Член 44

Административни санкции и корективни мерки

1. Компетентните органи разполагат с всички необходими правомощия за надзор, разследване и санкциониране с оглед на възложените им с настоящия регламент задачи.

2. Правомощията по параграф 1 включват най-малко:

   а) правото на достъп до всякакви документи или съхранявани под каквато и да е форма данни, които компетентният орган смята за важни за изпълнението на задълженията си, и на получаване на копие от тях или на копирането им;

   б) правото да извършват проверки на място или разследвания;

   в) правото да изискват корективни мерки за отстраняване на нарушение на изискванията на настоящия регламент и за недопускане в бъдеще на такова нарушение.

3. Без да се засяга правото им да налагат наказателноправни санкции, предвидено в член 46, държавите членки въвеждат при нарушение на настоящия регламент подходящи административни санкции и корективни мерки и осигуряват ефективното им правоприлагане.

   Тези санкции и мерки са ефективни, съразмерни и възпиращи.

4. Държавите членки оправомощават компетентните органи да налагат най-малко следните административни санкции или корективни мерки при нарушение на настоящия регламент:

   а) разпореждане, с което от физическото или юридическото лице се изисква да престане да нарушава настоящия регламент и да не започва отново;

   б) изискване за временно или постоянно прекратяване на практиките или поведението, които компетентният орган смята, че са в нарушение на разпоредбите на настоящия регламент, и за недопускането им в бъдеще;

   в) приемане на всякакви мерки, в т.ч. с парично измерение, за да се осигури неотклонното спазване на правните изисквания от финансовите субекти;

   г) при сериозно подозрение за нарушение на настоящия регламент и доколкото позволява националното право — изискване за предоставяне на съхраняваните от телекомуникационен оператор записи на потоците от данни, които могат да са от значение за разследването на такова нарушение; както и

д) публикуване на известия, в т.ч. на публични изявления, в които се посочва самоличността — при физически лица или наименованието — при юридически лица, както и естеството на нарушението.

5. Когато разпоредбите по параграф 2, буква в) и параграф 4 се прилагат спрямо юридически лица, държавите членки оправомощават компетентните органи да прилагат административните санкции и корективните мерки, при спазване на определените в националното право условия, спрямо членовете на ръководния орган и другите физически лица, които съгласно националното право носят отговорност за нарушението.

6. Държавите членки предвиждат всяко решение за налагане на посочените в параграф 2, буква в) административни санкции или корективни мерки да бъде надлежно мотивирано и да подлежи на обжалване.

Член 45

Упражняване на правомощията за налагане на административни санкции и корективни мерки

1. Компетентните органи упражняват съгласно националната си правна уредба предвидените в член 44 правомощия за налагане на административни санкции и коригиращи мерки, както следва:

а) пряко;

б) в сътрудничество с други органи;

в) на своя отговорност, като оправомощават други органи;

г) като отнасят въпросите пред компетентните съдебни органи.

2. Когато определят вида и размера на налаганите по силата на член 44 административни санкции или корективни мерки компетентните органи се съобразяват с това доколко нарушението е умишлено или произтича от небрежност, както и с всички други съответни обстоятелства, в т.ч., според случая, със следното:

а) съществеността, тежестта и продължителността на нарушението;

б) степента на отговорност на физическото или юридическото лице нарушител;

в) финансовите възможности на отговорното физическо или юридическо лице;

г) размера на реализираната печалба или избегнатата загуба от отговорното физическо или юридическо лице, доколкото може да бъде определен;

д) загубите за трети страни в резултат на нарушението, доколкото могат да бъдат определени;

е) доколко отговорното физическо или юридическо лице съдейства на компетентния орган, без това да засяга принудителното връщане от това лице на реализираната печалба или избегнатата загуба;

ж) предишните нарушения на отговорното физическо или юридическо лице.

Член 46

Наказателноправни санкции

1. Държавите членки могат да решат да не въвеждат административни санкции или корективни мерки за нарушенията, за които в националното им право са предвидени наказателноправни санкции.

2. Ако изберат да предвидят наказателноправни санкции за нарушения на настоящия регламент, държавите членки, в изпълнение на задължението си за сътрудничество за целите на настоящия регламент, въвеждат подходящи мерки, така че компетентните органи да разполагат с всички необходими правомощия, за да осъществят връзка с техните съдебни органи, органи за наказателно преследване или органи на наказателното правосъдие с цел получаване на специфични сведения за предприетите наказателни разследвания или производства за нарушения на настоящия регламент, и за да предоставят тези сведения на другите компетентни органи и на ЕОЦКП, ЕБО и ЕОЗППО.

Член 47

Задължения за уведомяване

Не по-късно от [*СП: да се въведе дата: 1 година след влизането в сила на настоящия регламент*] държавите членки уведомяват Комисията, ЕОЦКП, ЕБО и ЕОЗППО за законовите, подзаконовите и административните разпоредби, с които се прилага настоящата глава, в т.ч. за евентуалните съответни наказателноправни разпоредби. При всяко последващо изменение на тези разпоредби държавите членки своевременно уведомяват Комисията, ЕОЦКП, ЕБО и ЕОЗППО.

Член 48

Публикуване на административните санкции

1. Компетентните органи своевременно публикуват на своите официални уебсайтове всяко необжалвано решение за налагане на административна санкция, след като адресатът на санкцията е бил уведомен за него.

2. В публикацията по параграф 1 се посочват видът и естеството на нарушението, самоличността или съответно наименованието на отговорните лица, както и наложените санкции.

3. Ако компетентният орган прецени за даден случай, че публикуването на наименованието — при юридически лица, или на самоличността и лични данни — при физически лица, би било прекомерна мярка, която би застрашила стабилността на финансовите пазари или провеждането на текущо наказателно разследване, или би причинила несъразмерни вреди на засегнатото лице — доколкото могат да бъдат определени, той приема едно от следните решения по отношение на решението за налагане на административна санкция:

   а) отлага публикуването му, докато не изчезнат всички причини за това то да не бъде публикувано;

   б) публикува го анонимно, съблюдавайки националното право; или

   в) въздържа се от публикуването му, ако сметне, че вариантите по букви а) и б) не са достатъчни, за да се премахне всяка опасност за стабилността на

финансовите пазари, или че такова публикуване, ако наложената санкция е била намалена, би било прекомерно.

4. При решение за анонимно публикуване по силата на параграф 3, буква б) на административна санкция, публикуването на съответните данни може да бъде отложено.

5. Когато компетентен орган публикува решение за налагане на административна санкция, срещу което е подадена жалба пред съответните съдебни органи, компетентните органи незабавно добавят на своите официални уебсайтове тази информация, както и всяка следваща съответна информация за резултата от това обжалване. Публикува се и всяко съдебно решение, с което се отменя решението за налагане на административна санкция.

6. Компетентните органи оставят на официалните си уебсайтове публикациите по параграфи 1—4 най-малко пет години след публикуването им. Личните данни, които се съдържат в публикацията, се оставят на официалния уебсайт на компетентния орган само за необходимия срок, предписан от приложимите норми за защита на данните.

Член 49

Служебна тайна

1. Всяка поверителна информация, получена, обменена или предадена по силата на настоящия регламент, подлежи на посочените в параграф 2 изисквания за опазване на служебната тайна.

2. Задължението за опазване на служебната тайна се прилага спрямо всички лица, които работят или са работили за компетентните органи по настоящия регламент или за друг орган, предприятие на пазара, физическо или юридическо лице, на което компетентният орган е делегирал правомощията си, в т.ч. одитори и експерти, наети от компетентния орган.

3. Информацията, която представлява служебна тайна, не може да бъде оповестявана на никое друго лице или орган, освен по силата на разпоредбите, предвидени в правото на Съюза или в националното право.

4. Цялата обменяна между компетентните органи по силата на настоящия регламент информация, която се отнася до общите или оперативни параметри на стопанската дейност и до други икономически или лични въпроси, се счита за поверителна и за нея се прилагат изискванията за опазване на служебната тайна, освен ако компетентният орган в момента на предаването ѝ не посочи, че тя може да бъде разкрита, или когато разкриването ѝ се налага за процесуални цели.

ГЛАВА VIII

ДЕЛЕГИРАНИ АКТОВЕ

Член 50

Упражняване на делегирането

1. Комисията се оправомощава да приема делегирани актове при спазване на условията в настоящия член.

2. Посоченото в член 28, параграф 3 и член 38, параграф 2 правомощие да приема делегирани актове се предоставя на Комисията за срок от пет години, считано от [СП: да се въведе дата — 5 години след датата на влизане в сила на настоящия регламент].

3. Посоченото в член 28, параграф 3 и член 38, параграф 2 оправомощаване може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него оправомощаване. То поражда действие в деня след публикуването му в Официален вестник на Европейския съюз или на посочената в него по-късна дата. То не засяга действителността на делегираните актове, които вече са в сила.

4. В съответствие с принципите, залегнали в Междуинституционалното споразумение за по-добро законотворчество от 13 април 2016 г., преди да приеме делегиран акт, Комисията се допитва до определени от всяка държава членка експерти.

5. Веднага след като приеме делегиран акт, Комисията уведомява за него едновременно Европейския парламент и Съвета.

6. Делегиран акт, приет по силата на член 28, параграф 3 и член 38, параграф 2, влиза в сила единствено ако нито Европейският парламент, нито Съветът възразят в срок от два месеца след като са били уведомени за него или ако преди изтичането на този срок и Европейският парламент, и Съветът уведомят Комисията, че няма да възразят. Посоченият срок може да се удължи с два месеца по инициатива на Европейския парламент или на Съвета.

ГЛАВА IX

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

РАЗДЕЛ I

Член 51

Преглед

До [*СП: да се въведе дата: 5 години след датата на влизане в сила на настоящия регламент*], след като се допита, по целесъобразност, до ЕБО, ЕОЦКП, ЕОЗППО и ЕССР, Комисията извършва преглед на критериите по член 28, параграф 2 за определяне на възловите доставчици трети страни на услуги в областта на ИКТ и

представя доклад на Европейския парламент и на Съвета, придружен, ако е целесъобразно, от законодателно предложение.

РАЗДЕЛ II

ИЗМЕНЕНИЯ

Член 52

Изменения на Регламент (ЕО) № 1060/2009

В раздел А, точка 4 от приложение I към Регламент (ЕО) № 1060/2009 първа алинея се заменя със следното:

„Агенциите за кредитен рейтинг разполагат с надеждни административни и счетоводни процедури, механизми за вътрешен контрол, ефективни процедури за оценка на риска и ефективни контролни и защитни механизми за управление на системите на ИКТ, както се изисква от Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета*.

* Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета от […], ОВ L XX, [...] г., стр. [...].“.

Член 53

Изменения на Регламент (ЕС) № 648/2012

Регламент (ЕО) № 648/2012 се изменя, както следва:

(1) Член 26 се изменя, както следва:

а) параграф 3 се заменя със следното:

„3. ЦК поддържа и прилага организационна структура, която осигурява непрекъснатост и подходящо функциониране на неговите услуги и дейности. Той използва подходящи и адекватни системи, ресурси и процедури, в т.ч. системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета*.

* Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета от […] (ОВ L XX, [...] г., стр. [...]).“;

б) параграф 6 се заличава;

(2) Член 34 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1. С оглед на запазването на функциите си, своевременното възобновяване на операциите си и изпълнението на задълженията си ЦК създава, прилага и поддържа адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофа, в който се съдържат изготвените в изпълнение на Регламент (ЕС) 2021/xx планове за непрекъснато функциониране на ИКТ и за възстановяване на информацията при срив на ИКТ.“;

б) в параграф 3 първата алинея се заменя със следното:

„С оглед на еднообразното прилагане на настоящия член ЕОЦКП, след консултации с членовете на ЕСЦБ, разработва проект на регулаторни технически стандарти за определяне на минималните елементи и изисквания на политиката за непрекъснатост на дейността и на плана за възстановяване от катастрофа, без плановете за непрекъснато функциониране на ИКТ и за възстановяване на информацията при срив на ИКТ.“;

(3) В член 56, параграф 3 първата алинея се заменя със следното:

„3. С оглед на еднообразното прилагане на настоящия член ЕОЦКП разработва проект на регулаторни технически стандарти за определяне на техническите детайли на посоченото в параграф 1 заявление за регистрация, като тези технически детайли не съдържат изисквания относно управлението на риска при ИКТ.“;

(4) В член 79 параграфи 1 и 2 се заменят със следното:

„1. Регистърът на трансакции идентифицира източниците на операционен риск и ги свежда до минимум също и чрез разработването на подходящи системи, механизми за контрол и процедури, в т.ч. системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2021/xx.

2. С оглед на поддържането на функциите си, своевременното възобновяване на операциите си и изпълнението на задълженията си регистърът на трансакции създава, прилага и поддържа адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофа, в който се съдържат изготвените в изпълнение на Регламент (ЕС) 2021/xx планове за непрекъснато функциониране на ИКТ и за възстановяване на информацията при срив на ИКТ.“;

(5) В член 80 параграф 1 се заличава.

Член 54

Изменения на Регламент (ЕС) № 909/2014

Член 45 от Регламент (ЕС) № 909/2014 се изменя, както следва:

(1) Параграф 1 се заменя със следното:

„1. ЦДЦК установява източниците на операционен риск — както вътрешни, така и външни — и свежда до минимум тяхното въздействие също и чрез внедряването на подходящи основани на ИКТ инструменти, процеси и политики за ИКТ, създадени и управлявани в съответствие с Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета*, както и чрез всякакви други подходящи инструменти, механизми за контрол и процедури, отнасящи се до другите видове операционен риск, в т.ч. до управляваните от него системи за сетълмент на ценни книжа.

* Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета от […], ОВ L XX, [...] г., стр. [...].“;

(2) Параграф 2 се заличава;

(3) Параграфи 3 и 4 се заменят със следното:

„3. С оглед на запазването на функциите си, своевременното възобновяване на операциите си и изпълнението на задълженията си при събития, които крият значителен риск от прекъсване на операциите, ЦДЦК създава, прилага и поддържа, за услугите, които предоставя, както и за всяка управлявана от него система за сетълмент на ценни книжа, подходяща политика за непрекъснатост на дейността и план за възстановяване от катастрофа, в т.ч. изготвени в изпълнение на Регламент (ЕС) 2021/xx планове за непрекъснато функциониране на ИКТ и за възстановяване на информацията при срив на ИКТ.

4. В посочения в параграф 3 план се очертава как се възстановяват всички трансакции и позиции на участниците към момента на прекъсването, така че участниците в ЦДЦК да могат по надежден начин да продължат дейността си и да приключат сетълмента на определената дата; както и как след прекъсването се възобновява функционирането на възловите информационни системи — както е посочено в член 11, параграфи 5 и 7 от Регламент (ЕС) 2012/xx.“;

(4) В параграф 6 първата алинея се заменя със следното:

ЦДЦК установява, наблюдава и управлява рисковете, които пораждат за операциите му възловите участници в управляваните от него системи за сетълмент на ценни книжа, доставчиците на услуги и на комунални услуги, другите ЦДЦК или другите пазарни инфраструктури. При поискване от компетентните и съответните органи той им предоставя информация за всички установени рискове. ЦДЦК също така уведомява незабавно компетентния орган и съответните органи за всички оперативни инциденти, произтичащи от такива рискове, без тук да се включват рисковете при ИКТ.“;

(5) В параграф 7 първата алинея се заменя със следното:

„ЕОЦКП разработва в тясно сътрудничество с членовете на ЕСЦБ проект на регулаторни технически стандарти за определяне на посочените в параграфи 1 и 6 операционни рискове — без тук да се включват рисковете при ИКТ, и методите за тестване на тези рискове, както и за тяхното преодоляване или свеждане до минимум, в т.ч. политиките за непрекъснатост на дейността и плановете за възстановяване от катастрофа, посочени в параграфи 3 и 4, както и методите за тяхната оценка.“.

Член 55

Изменения на Регламент (ЕС) № 600/2014

Регламент (ЕО) № 600/2014 се изменя, както следва:

(1) Член 27ж се изменя, както следва:

а) параграф 4 се заличава;

б) в параграф 8 буква в) се заменя със следното:

в) „в) конкретните организационни изисквания, посочени в параграфи 3 и 5.“;

(2) Член 27з се изменя, както следва:

а) параграф 5 се заличава;

б) в параграф 8 буква д) се заменя със следното:

„д) конкретните организационни изисквания, посочени в параграф 4.“;

(3) Член 27и се изменя, както следва:

а) параграф 3 се заличава;

б) в параграф 5 буква б) се заменя със следното:

„б) конкретните организационни изисквания, посочени в параграфи 2 и 4.“.

Член 56

Влизане в сила и прилагане

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Той се прилага от [*СП: въведете дата — 12 месеца след датата на влизане в сила*].

Членове 23 и 24 обаче се прилагат от [*СП: въведете дата — 36 месеца след датата на влизане в сила на настоящия регламент*].

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

1.2. Съответни области на политиката

1.3. Естество на предложението/инициативата

1.4. Цел(и)

1.5. Мотиви за предложението/инициативата

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

1.7. Планирани методи на управление

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

2.2. Системи за управление и контрол

2.3. Мерки за предотвратяване на измами и нередности

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

3.2. Очаквано отражение върху разходите

3.2.1. Обобщение на очакваното отражение върху разходите

3.2.2. Очаквано отражение върху бюджетните кредити

3.2.3. Очаквано отражение върху човешките ресурси

3.2.4. Съвместимост с настоящата многогодишна финансова рамка

3.2.5. Финансово участие на трети страни

3.3. Очаквано отражение върху приходите

Приложение

Общи допускания

Надзорни правомощия

ЗАКОНОДАТЕЛНА ФИНАНСОВА ОБОСНОВКА — „АГЕНЦИИ“

1. РАМКА НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

1.1. Наименование на предложението/инициативата

Предложение за Регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор.

1.2. Съответни области на политиката

Област на политиката: Финансова стабилност, финансови услуги и съюз на капиталовите пазари

Дейност: Оперативна устойчивост на цифровите технологии

1.3. Предложението е във връзка с:

☑ **ново действие**

☐ **ново действие след пилотен проект/подготвително действие**[50]

☐ **продължаване на съществуващо действие**

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

1.4. Цел(и)

1.4.1. Общи цели

Общата цел на инициативата е да се укрепи оперативната устойчивост на цифровите технологии, използвани от субектите от финансовия сектор на ЕС, като се рационализират и актуализират съществуващите правни норми и се въведат нови изисквания там, където има пропуски. С нея ще се усъвършенства и цифровото измерение на единната нормативна уредба.

Общата цел може да бъде разбита на три съставни цели: 1) редуциране на риска от финансови трусове и нестабилност; 2) намаляване на административното бреме и увеличаване на ефективността на надзора; както и 3) увеличаване на защитата на потребителите и инвеститорите.

1.4.2. Конкретни цели

Предложението има следните конкретни цели:

по-обстойно обхващане на рисковете при информационните и комуникационните технологии („ИКТ“) и засилване на общата устойчивост на цифровите технологии във финансовия сектор;

оптимизиране на уведомяването за инцидентите с ИКТ и премахване на припокриващите се изисквания за уведомяване;

осигуряване на надзорните органи на достъп до информацията за инцидентите с ИКТ;

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

изискване от финансовите субекти, обхванати от настоящото предложение, да оценяват ефективността на своите превантивни мерки и мерки за устойчивост, както и да идентифицират уязвимите места на ИКТ;

намаляване на разпокъсаността на единния пазар и създаване на условия за трансгранично признаване на резултатите от тестовете;

засилване на договорните гаранции за финансовите субекти при използването на услуги в областта на ИКТ, в т.ч. на разпоредбите относно възлагането на дейности на доставчик трета страна и по-специално относно надзора на доставчиците трети страни (ДТС) на ИКТ;

възможност за надзор на дейността на възловите ДТС на ИКТ;

насърчаване на обмена във финансовия сектор на разузнавателни данни за заплахи.

1.4.3. Очаквани резултати и отражение

Да се посочи очакваното отражение на предложението/инициативата върху бенефициерите/целевите групи.

Един законодателен акт относно оперативната устойчивост на цифровите технологии във финансовия сектор ще уреди всички аспекти на оперативната устойчивост на обхванатите цифрови технологии, с което ще се подобри общата оперативна устойчивост на финансовия сектор. Така ще се осигури яснота и съгласуваност в рамките на единна нормативна уредба.

Освен това ще се подобри и изясни взаимодействието с Директивата за МИС и нейното преразглеждане. От своя страна финансовите субекти и в частност тези, които притежават няколко лиценза и извършват дейност на няколко пазара в ЕС, ще получат яснота относно различните разпоредби, които трябва да спазват, отнасящи се до оперативната устойчивост на финансовите технологии.

1.4.4. Показатели за изпълнението

Да се посочат показателите за проследяване на напредъка и постиженията.

Възможни показатели:

Брой на инцидентите с ИКТ във финансовия сектор на ЕС и тяхното въздействие

Брой на съществените инциденти с ИКТ инциденти, за които са уведомени органите за пруденциален надзор

Брой на финансовите субекти, които ще бъдат задължени да провеждат тестове на проникването („ТП“)

Брой на финансовите субекти, които използват стандартни клаузи, когато сключват договори с ДТС на ИКТ

Брой на възловите ДТС на ИКТ, поднадзорни на ЕНО / органите за пруденциален надзор

Брой на финансовите субекти, участващи в технологични решения за обмен на разузнавателни сведения

Брой на органите, които са уведомени за един и същ инцидент с ИКТ

Брой на трансграничните ТП

1.5. Мотиви за предложението/инициативата

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

Финансовият сектор силно разчита на информационните и комуникационните технологии (ИКТ). Въпреки постигнатия значителен напредък благодарение на националните и европейските целеви политики и законодателни инициативи, рисковете при ИКТ продължават да са предизвикателство пред оперативната устойчивост, функционирането и стабилността на финансовата система на ЕС. Основната цел на реформата, последвала финансовата криза от 2008 г., бе да се засили финансовата устойчивост на финансовия сектор на ЕС и защити конкурентоспособността и стабилността на ЕС от икономическа, пруденциална и пазарна гледна точка. Въпреки че сигурността на ИКТ и общата устойчивост на цифровите технологии са част от операционния риск, те останаха извън приоритетите на следкризисната нормотворческа

програма, като бяха обхванати само в някои части на политиката на ЕС за регламентиране на финансовите пазари или само в няколко държави членки. Това поражда следните предизвикателства, които следва да бъдат разгледани в предложението:

Нормативната уредба на ЕС на риска при ИКТ и на оперативната устойчивост във финансовия сектор е разпокъсана и не напълно съгласувана.

Липсата на съгласувани изисквания за уведомяване за инцидентите с ИКТ не позволява да се оформи обстойна картина на естеството, честотата, значимостта и ефекта на инцидентите с ИКТ.

Изискванията към някои финансови субекти за уведомяване за един и същ инцидент с ИКТ са сложни, припокриващи се и потенциално несъгласувани.

Недостатъчният обмен на информация и сътрудничество при стратегическото, тактическото и оперативното разследване на киберзаплахите пречи на отделните финансови субекти адекватно да ги оценяват, наблюдават, предотвратяват и реагират на тях.

В някои финансови подсектори е вероятно да има множество и некоординирани изисквания за тестване на пробива и на устойчивостта, като освен това резултатите не се признават в трансграничен план, а в други изобщо да няма подобни изисквания.

Липсата на надзорна информация за дейността на финансовите субекти, които се обслужват от ДТС на ИКТ, излага на операционен риск всяко едно от тях и финансовата система като цяло.

Надзорните органи на финансовия сектор не разполагат с достатъчен мандат, нито с инструменти, за да наблюдават и управляват риска от концентрация и системните рискове, които крие зависимостта на финансовите субекти от ДТС на ИКТ.

1.5.2. Добавена стойност от участието на Съюза (може да е в резултат от различни фактори (по-добра координация, правна сигурност, по-добра ефективност или взаимно допълване). За целите на тази точка „добавена стойност от участието на Съюза“ е стойността, която намесата на ЕС добавя към самостоятелно създадената от отделните държави членки.

Основания за действие на европейско равнище (ex-ante):

Оперативната устойчивост на цифровите технологии е въпрос от общ интерес за финансовите пазари на ЕС. Едно действие на равнище ЕС ще породи повече предимства и по-голяма стойност от изолирано предприетите на национално равнище действия. Ако в единната нормативна уредба не бъдат добавени оперативните разпоредби относно риска при ИКТ, тя ще предостави инструментариум за противодействие на европейско равнище на другите видове риск, но няма да засегне аспектите на оперативната устойчивост на цифровите технологии или ще ги остави подвластни на разпокъсани и некоординирани национални инициативи. С предложението ще се внесе правна яснота за това дали и как се прилагат разпоредбите относно оперативната устойчивост на цифровите технологии, особено спрямо трансграничните финансови субекти, и ще се премахне необходимостта държавите членки индивидуално да подобряват правните норми, стандартите и очакванията по отношение на оперативната устойчивост и киберсигурността в отговор на настоящия ограничен обхват на нормите на ЕС и на общия характер на Директивата за МИС.

Очаквана генерирана добавена стойност от ЕС (ex-post): Намесата на Съюза ще повиши значително ефективността на политиката, а освен това ще намали сложността и финансовото и административното бреме върху всички финансови субекти. Тя ще внесе хармонизация в една силно взаимосвързана и интегрирана икономическа област, която вече разполага с единна уредба и надзор. Що се отнася до уведомяването за инцидентите с ИКТ, предложението ще намали тежестта и имплицитните разходи, свързани с уведомяването на различни съюзни и/или национални органи за един и същ инцидент с ИКТ. То също така ще улесни взаимното признаване/приемане от страна на държавите членки на резултатите от тестовете на субектите с трансгранична дейност, които субекти понастоящем се подчиняват на множество национални изисквания за провеждане на тестове.

1.5.3. Изводи от подобен опит в миналото

Нова инициатива

1.5.4. Съвместимост с многогодишната финансова рамка и евентуални синергии с други подходящи инструменти

Целта на настоящото предложение е в синхрон с редица други политики и текущи инициативи на ЕС, по-специално Директивата за сигурността на мрежите и информационните системи (МИС) и Директивата за европейската критична инфраструктура (ЕКИ). Предложението ще запази ползата от хоризонталната уредба на киберсигурността, като остави финансовия сектор в обхвата на Директивата за МИС. Така надзорните органи на финансовия сектор ще продължат да бъдат свързани с екосистемата на МИС и ще могат да обменят съответната информация с органите за МИС и да участват в групата за сътрудничество за МИС. Предложението няма да засегне Директивата за МИС, а по-скоро ще се основава на нея и ще отстрани евентуалните припокривания, като въведе освобождаване по силата на „lex specialis“. Взаимодействието между уредбата на финансовите услуги и Директивата за МИС ще продължи да се ръководи от клауза за „lex specialis“, с която финансовите субекти се освобождават от съществените изисквания в Директивата за МИС и се избягват припокриванията между двата акта. Предложението е в съответствие и с Директивата за европейските критични инфраструктури (ЕКИ), която понастоящем се преразглежда с цел да се подобри защитата и устойчивостта на критичните инфраструктури срещу заплахи, различни от киберзаплахите.

Настоящото предложение няма да има отражение върху Многогодишната финансова рамка (МФР). На първо място, надзорната рамка за възловите доставчици трети страни на ИКТ ще бъде изцяло финансирана от такси, събирани от тези доставчици; на второ място, допълнителните възложени на ЕНО регулаторни задачи във връзка с оперативната устойчивост на цифровите технологии ще бъдат изпълнявани, като наличният персонал бъде преразпределен.

Това при бъдещата годишна бюджетна процедура ще доведе до предложение за увеличаване на броя на оправомощените служители на агенцията. Агенцията ще продължи да работи за постигането на оптимална синергия и повишаване на ефективността (в т.ч. чрез информационни системи) и ще наблюдава внимателно допълнителното работно натоварване, свързано с настоящото предложение, което ще бъде отразено в броя на оправомощените служители, които тя ще поиска в рамките на годишната бюджетна процедура.

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

Бяха разгледани няколко варианта за финансиране:

На първо място, допълнителните разходи могат да бъдат финансирани по обичайния механизъм за финансиране на ЕНО. Това обаче значително би увеличило вноската на ЕС във финансовите ресурси на ЕНО.

Този вариант се избира заради разходите, свързани с регулаторните задачи съгласно настоящото предложение. В действителност от ЕНО ще бъде поискано да пренасочат наличния персонал с оглед на разработването на редица технически стандарти. От друга страна, допълнителните разходи, свързани с надзора на възловите ДТС, няма да могат да бъдат покрити чрез вътрешно преразпределяне на ресурсите на ЕНО, на които, в допълнение към предвидените в настоящото предложение задачи, други законодателни актове на Съюза възлагат и други отговорности. Освен това надзорните задачи във връзка с оперативната устойчивост на цифровите технологии изискват специфични

технически познания и експертен опит. В тази връзка понастоящем наличните ресурси на ЕНО са недостатъчни, поради което са необходими допълнителни ресурси.

На последно място, предложението предвижда на поднадзорните възлови ДТС на ИКТ да се начисляват такси. Таксите са предназначени да покриват разходите за всички допълнителни ресурси, необходими на ЕНО за изпълнението на новите им задачи и правомощия.

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

☐ **ограничен срок на действие**

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

☐ Финансово отражение от ГГГГ до ГГГГ

☑ **неограничен срок на действие**

Първоначално прилагане от 2021 г. с постепенно увеличаване,

последвано от пълно действие.

1.7. Планирани методи на управление[51]

Пряко управление от Комисията чрез

☐ изпълнителни агенции

☐ **Споделено управление** с държавите членки

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

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

☐ ЕИБ и Европейския инвестиционен фонд;

☑ органите по членове 70 и 71;

☐ публичноправни органи;

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

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

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

Забележки

N/A

[51] Подробна информация за методите на управление и позоваванията на Финансовия регламент има на уебсайта BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. МЕРКИ ЗА УПРАВЛЕНИЕ

2.1. Правила за мониторинг и докладване

Да се посочат честотата и условията.

В съответствие с вече съществуващите договорености ЕНО изготвят редовни доклади за дейността си (включително вътрешни доклади пред висшето ръководство, доклади пред Управителния съвет, доклади за дейността на всеки шест месеца пред Надзорния съвет и изготвяне на годишния доклад) и подлежат на одити от страна на Сметната палата и службата за вътрешен одит на Комисията във връзка с използването на ресурси от тяхна страна. Мониторингът и докладването на действията, включени в предложението, ще съответстват на вече съществуващите изисквания, както и на новите изисквания, произтичащи от настоящото предложение.

2.2. Системи за управление и контрол

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

Управлението ще бъде непряко чрез ЕНО. Механизмът за финансиране ще включва такси, събирани от съответните възлови ДТС на ИКТ.

2.2.2. Информация за установените рискове и за създадените за ограничаването им системи за вътрешен контрол

По отношение на правните и икономическите аспекти на ефективното и ефикасно използване на произтичащите от предложението бюджетни кредити може да се отбележи, че не се очаква предложението да породи нови значителни рискове, които не са покрити от действащ механизъм за вътрешен контрол. Ново предизвикателство обаче може да представлява осигуряването на своевременно събиране на таксите от съответните ДТС на ИКТ.

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

Системите за управление и контрол, предвидени в регламентите за ЕНО, вече са въведени. ЕНО работи в тясно сътрудничество със Службата за вътрешен одит на Комисията, за да се осигури съблюдаването на съответните стандарти във всички сфери на вътрешния контрол. Тези мерки ще се прилагат и по отношение на ролята на ЕНО, предвидена в настоящото предложение. Освен това всяка финансова година Европейският парламент, по препоръка на Съвета, ще освобождава всеки ЕНО от отговорност във връзка с изпълнението на своя бюджет.

2.3. Мерки за предотвратяване на измами и нередности

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

Разпоредбите на Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 г. относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), се прилагат спрямо ЕНО без никакви ограничения за целите на борбата с измамите, корупцията и други незаконни дейности.

ЕНО имат специална стратегия за борба с измамите, конкретизирана в план за действие. Засилените действия на ЕНО за борба с измамите ще са съобразени с разпоредбите и насоките, предвидени във Финансовия регламент (мерки за борба с измамите като част от доброто финансово управление), политиката на OLAF за предотвратяване на измамите и разпоредбите, предвидени от Стратегията на Комисията за борба с измамите (COM(2011) 376) и от общия подход за децентрализираните агенции на ЕС (юли 2012 г.) и неговата пътна карта.

Освен това в регламентите за създаване на ЕНО и във финансовите регламенти на ЕНО се съдържат разпоредбите относно изпълнението и контрола на бюджета на ЕНО и приложимите финансови правила, в т.ч. насочените към предотвратяване на измамите и нередностите.

3. ОЧАКВАНО ФИНАНСОВО ОТРАЖЕНИЕ НА ПРЕДЛОЖЕНИЕТО/ИНИЦИАТИВАТА

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

Съществуващи бюджетни редове

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

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансово участие			
	Номер	Многогод./едногод[52].	от държавите от ЕАСТ[53]	от държавите кандидатки[54]	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия регламент

Поискани нови бюджетни редове

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

Функция от многогодишната финансова рамка	Бюджетен ред	Вид разход	Финансово участие			
	Номер	Многогод./едногод.	от държавите от ЕАСТ	от държавите кандидатки	от трети държави	по смисъла на член 21, параграф 2, буква б) от Финансовия

[52] Многогод. = многогодишни бюджетни кредити; едногод. = едногодишни бюджетни кредити.

[53] ЕАСТ: Европейска асоциация за свободна търговия.

[54] Държавите кандидатки и ако е приложимо — потенциалните кандидатки от Западните Балкани.

						регламент

3.2. Очаквано отражение върху разходите

3.3. Обобщение на очакваното отражение върху разходите

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

Функция от многогодишната финансова рамка	Номер	Бюджетен ред

ГД: <..>			2020 г.	2021 г.	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
	Поети задължения	(1)									
	Плащания	(2)									
ОБЩО бюджетни кредити за ГД <>	Поети задължения										
	Плащания										

Функция от многогодишната финансова рамка		

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

		2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
ГД:								
• Човешки ресурси								
• Други административни разходи <>								
ОБЩО ГД	Бюджетни кредити							

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

в млн. EUR (до третия знак след десетичната запетая) по постоянни цени

		2022 г.	**2023 г.**	**2024 г.**	**2025 г.**	**2026 г.**	**2027 г.**	**ОБЩО**
ОБЩО бюджетни кредити по ФУНКЦИЯ 1 от многогодишната финансова рамка	Поети задължения							
	Плащания							

3.3.1. Очаквано отражение върху бюджетните кредити

☑ Предложението/инициативата не налага използване на бюджетни кредити за оперативни разходи

☐ Предложението/инициативата налага използване на бюджетни кредити за оперативни разходи, както следва:

Бюджетни кредити за поети задължения в млн. EUR (до третия знак след десетичната запетая) по постоянни цени

Да се посочат целите и резултатите ⇩			2022 г.		2023 г.		2024 г.		2025 г.		2026 г.		2027 г.		**ОБЩО**	
	РЕЗУЛТАТИ															
	Вид[55]	Средни разходи	№	Разход	№	Разходи	№	Разход	№	Разход	№	Разход	№	Разход	Общо брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[56] …																
- Резултат																
Междинен сбор за конкретна цел № 1																
КОНКРЕТНА ЦЕЛ № 2…																
- Резултат																
Междинен сбор за конкретна цел № 2																
ОБЩО РАЗХОДИ																

[55] Резултатите са продуктите и услугите, които ще бъдат доставени (напр.: брой финансирани обмени на учащи се, дължина на построените пътища в километри и т.н.).

[56] Съгласно описанието в точка 1.4.2. „Конкретни цели...“

3.3.2. Очаквано отражение върху човешките ресурси

3.3.2.1. Резюме

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

☑ Предложението/инициативата налага използване на бюджетни кредити за административни разходи, както следва:

в млн. EUR (до третия знак след десетичната запетая) по постоянни цени

ЕБО, ЕОЗППО, ЕОЦКП	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
Временно наети лица (степени AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Временно наети служители (ниво AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Договорно нает персонал							
Командировани национални експерти							
ОБЩО	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Изисквания по отношение на персонала (ЕПРВ):

ЕБО, ЕОЗППО, ЕОЦКП и ЕАОС	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
Временно наети лица (степени AD) ЕБО =5, ЕОЗППО =5, ЕОЦКП =5	15	15	15	15	15	15	15
Временно наети служители (ниво AST) ЕБО = 1, ЕОЗППО = 1, ЕАОС = 1	3	3	3	3	3	3	3
Договорно нает персонал							
Командировани национални експерти							

ОБЩО	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Очаквани нужди от човешки ресурси за (отговарящата) ГД

☑ Предложението/инициативата не налага използване на човешки ресурси

☐ Предложението/инициативата налага използване на човешки ресурси, както следва:

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

		2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.
• **Длъжности в щатното разписание (длъжностни лица и срочно наети служители)**							
• **Външен персонал (в еквивалент на пълно работно време — ЕПРВ)**[57]							
XX 01 02 01 (ДНП, КНЕ, ПНА от общия финансов пакет)							
XX 01 02 02 (ДНП, МП, КНЕ, ПНА и МЕД в делегациите)							
XX 01 04 ***yy***[58]	- в централата[59]						
	- в делегациите						
XX 01 05 02 (ДНП, КНЕ и ПНА – непреки научни изследвания)							
10 01 05 02 (ДНП, КНЕ и ПНА — преки научни изследвания)							
Други бюджетни редове (да се посочат)							
ОБЩО							

XX е съответната област на политиката или съответният бюджетен дял.

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

Описание на задачите, които трябва да се изпълнят:

Длъжностни лица и срочно наети служители	
Външен персонал	

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

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

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

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

3.3.3. Съвместимост с настоящата многогодишна финансова рамка

☑ Предложението/инициативата е съвместимо(а) с настоящата многогодишна финансова рамка.

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

☐ Предложението/инициативата налага да се използва Инструментът за гъвкавост или да се преразгледа многогодишната финансова рамка[60].

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

3.3.4. Финансово участие на трети страни

☐ Предложението/инициативата не предвижда съфинансиране от трети страни.

☑ Предложението/инициативата предвижда съфинансиране съгласно следния разчет:

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

ЕБО

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ОБЩО съфинансирани бюджетни кредити	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ЕОЗППО

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
ОБЩО съфинансирани бюджетни кредити	1,305	1,811	1,611	1,611	1,611	1,611	9,560

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

61 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

62 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

ЕОЦКП

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ОБЩО съфинансирани бюджетни кредити	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Очаквано отражение върху приходите

☑ Предложението/инициативата няма финансово отражение върху приходите

☐ Предложението/инициативата има следното финансово отражение:

☐ върху собствените ресурси

☐ върху разните приходи

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

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

Приходен бюджетен ред:	Налични бюджетни кредити за текущата финансова година	Отражение на предложението/инициативата[64]						
		Година **N**	Година **N+1**	Година **N+2**	Година **N+3**	Добавят се толкова години, колкото е необходимо, за да се обхване продължителността на отражението (вж. точка 1.6)		
Статия ….								

За разните целеви приходи се посочват съответните разходни бюджетни редове.

[...]

Посочва се методът за изчисляване на отражението върху приходите.

[...]

63 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

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

ПРИЛОЖЕНИЕ

Общи допускания

Дял I — Разходи за персонал

При изчисляването на разходите за персонал са използвани следните специфични допускания, основани на посочените по-долу установени потребности от персонал:

- Разходите за допълнителния персонал, нает през 2022 г., са изчислени за 6 месеца, като се има предвид предполагаемото време, необходимо за наемане на допълнителен персонал;
- Средните годишни разходи за срочно нает служител възлизат на 150 000 евро, като тук се включват 25 000 евро за т.нар. „habillage“ (пропорционални разходи за ползването на сградите, информационните технологии и др.);
- Корекционните коефициенти, приложими към възнагражденията на персонала в Париж (ЕБО и ЕОЦКП) и Франкфурт (ЕОЗППО), са съответно 117,7 и 99,4;
- Плащаните от работодателя пенсионни вноски за срочно наетите служители са изчислени въз основа на стандартните основни заплати, включени в стандартните средни годишни разходи, т.е. 95 660 евро;
- Допълнителните срочно наети служители са в степен AD5 и AST.

Дял II — Инфраструктурни и оперативни разходи

Разходите се изчисляват като броят на служителите се умножи по частта от годината на работа по стандартните разходи за „habillage“, т.е. 25 000 евро.

Дял III — Оперативни разходи

Разчетните разходи са предмет на следните допускания:

- Разходите за писмен превод възлизат на 350 000 евро годишно за всеки ЕНО.
- Допуска се, че еднократните разходи за информационни технологии в размер на 500 000 евро за ЕБО ще бъдат извършени през двете години — 2022 г. и 2023 г., разпределени 50 % / 50 %; Годишните разходи за поддръжка, считано от 2024 г., се оценяват на 50 000 евро за всеки ЕНО;
- Годишните разходи за надзор на място се оценяват на 200 000 евро за всеки ЕНО.

Приблизителните оценки, представени по-горе, водят до следните годишни разходи:

Функция от многогодишната финансова рамка	Номер	

Постоянни цени

ЕБО:			2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
Дял 1:	Поети задължения	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Плащания	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Дял 2:	Поети задължения	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Плащания	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Дял 3:	Поети задължения	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Плащания	(3б)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ОБЩО бюджетни кредити за ЕБО	Поети задължения	= 1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Плащания	= 2+2a +3б	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ЕОЗППО:			2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
Дял 1:	Поети задължения	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Плащания	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Дял 2:	Поети задължения	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Плащания	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Дял 3:	Поети задължения	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

	Плащания	(3б)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ОБЩО бюджетни кредити за ЕОЗППО	Поети задължения	= 1+1a+3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Плащания	= 2+2a +3б	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ЕОЦКП:			2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	**ОБЩО**
Дял 1:	Поети задължения	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Плащания	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Дял 2:	Поети задължения	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Плащания	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Дял 3:	Поети задължения	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Плащания	(3б)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ОБЩО бюджетни кредити за ЕОЦКП	Поети задължения	= 1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Плащания	= 2+2a +3б	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Предложението налага използване на бюджетни кредити за оперативни разходи съгласно обяснението по-долу:

Бюджетни кредити за поети задължения в млн. EUR (до третия знак след десетичната запетая) по постоянни цени

ЕБО

Да се посочат целите и резултатите ⇩			2022 г.		2023 г.		2024 г.		2025 г.		2026 г.		2027 г.			
	РЕЗУЛТАТИ															
	Вид[65]	Средни разходи	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	Общо брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[66] Пряк надзор на възловите ДТС на ИКТ																
- Резултат				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Междинен сбор за конкретна цел № 1																
КОНКРЕТНА ЦЕЛ № 2…																
- Резултат																
Междинен сбор за конкретна цел № 2																
ОБЩО РАЗХОДИ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ЕОЗППО

Да се посочат целите и резултатите ⇩			2022 г.		2023 г.		2024 г.		2025 г.		2026 г.		2027 г.			
	РЕЗУЛТАТИ															
	Вид[67]	Средни разходи	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	Общо брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[68] Пряк надзор на възловите ДТС на ИКТ																
- Резултат				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] Резултатите са продуктите и услугите, които ще бъдат доставени (напр.: брой финансирани обмени на учащи се, дължина на построените пътища в километри и т.н.).

[66] Съгласно описанието в точка 1.4.2. „Конкретни цели...“

[67] Резултатите са продуктите и услугите, които ще бъдат доставени (напр.: брой финансирани обмени на учащи се, дължина на построените пътища в километри и т.н.).

[68] Съгласно описанието в точка 1.4.2. „Конкретни цели...“

Междинен сбор за конкретна цел № 1															
КОНКРЕТНА ЦЕЛ № 2…															
- Резултат															
Междинен сбор за конкретна цел № 2															
ОБЩО РАЗХОДИ		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**	

ЕОЦКП

Да се посочат целите и резултатите ⇩			2022 г.		2023 г.		2024 г.		2025 г.		2026 г.		2027 г.			
	РЕЗУЛТАТИ															
	Вид[69]	Средни разходи	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	№	Разход	Общо брой	Общо разходи
КОНКРЕТНА ЦЕЛ № 1[70] Пряк надзор на възловите ДТС на ИКТ																
- Резултат				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Междинен сбор за конкретна цел № 1																
КОНКРЕТНА ЦЕЛ № 2…																
- Резултат																
Междинен сбор за конкретна цел № 2																
ОБЩО РАЗХОДИ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Резултатите са продуктите и услугите, които ще бъдат доставени (напр.: брой финансирани обмени на учащи се, дължина на построените пътища в километри и т.н.).

[70] Съгласно описанието в точка 1.4.2. „Конкретни цели...“

Надзорните дейности се финансират изцяло с таксите, събирани от поднадзорните субекти, както следва:

ЕБО

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ОБЩО съфинансирани бюджетни кредити	1,373	1,948	1,748	1,748	1,748	1,748	10,313

ЕОЗППО

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
ОБЩО съфинансирани бюджетни кредити	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ЕОЦКП

	2022 г.	2023 г.	2024 г.	2025 г.	2026 г.	2027 г.	Общо
Разходите се покриват 100 % от таксите, събирани от поднадзорните субекти[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
ОБЩО съфинансирани бюджетни кредити	1,373	1,948	1,748	1,748	1,748	1,748	10,313

СПЕЦИАЛНА ИНФОРМАЦИЯ

Преки надзорни правомощия

[71] 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

[72] 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

[73] 100 % от общите разчетни разходи плюс пълния размер на пенсионните вноски, плащани от работодателя

Като начало следва да се припомни, че субектите, които подлежат на пряк надзор от ЕОЦКП, следва да заплащат такси на органа (еднократна регистрационна такса и периодични такси за разходите по текущия надзор). Такъв е случаят с агенциите за кредитен рейтинг (вж. Делегиран регламент (ЕС) № 272/2012 на Комисията) и регистрите на трансакции (Делегиран регламент (ЕС) № 1003/2013 на Комисията).

С настоящото законодателно предложение на ЕНО ще бъдат възложени нови задачи за насърчаване на сближаването на надзорните подходи към риска при ИКТ, пораждан от трета страна, във финансовия сектор чрез създаването на съюзна надзорна рамка за възловите доставчици трети страни на услуги в областта на ИКТ.

Надзорната рамка, предвидена в настоящото предложение, се основава на съществуващата институционална структура при финансовите услуги, при която съвместният комитет на Европейските надзорни органи осигурява междусекторната координация по всички въпроси на риска при ИКТ в съответствие със задачите си в сферата на киберсигурността, подкрепян от съответния подкомитет (надзорен форум), който извършва подготвителната работа както за целите на решенията, касаещи отделни възлови доставчици трети страни на услуги в областта на ИКТ, така и на препоръките, отправяни към всички такива доставчици.

По силата на тази рамка този ЕНО, който бъде определен за водещ надзорник на дадения възлов доставчик трета страна на услуги в областта на ИКТ, получава правомощия, благодарение на които доставчиците на технологични услуги с възлова роля за функционирането на финансовия сектор ще са обект на подходящо наблюдение на европейско равнище. Задълженията във връзка с надзора са посочени в предложението и са пояснени допълнително в обяснителния меморандум. Сред тези права са правото да изискват цялата съответна информация и документация за целите на свои общи разследвания и проверки, както и правото да отправят препоръки и впоследствие да представят доклади за предприетите действия или приложените корективни мерки във връзка с тях.

С оглед на новите си задачи, предвидени в настоящото предложение, ЕНО ще наемат допълнителен персонал със специализация в областта на риска при ИКТ, който ще работи по оценяването на зависимостта от доставчиците трети страни.

Нуждите от човешки ресурси могат да бъдат оценени на 6 ЕПРВ за всеки орган (5 AD и 1 AST за подпомагане на AD). Освен това ЕНО ще имат допълнителни разходи за информационни технологии, които се оценяват на 500 000 евро еднократни разходи плюс 50 000 евро разходи за поддръжка, които са на година за всеки от трите ЕНО. Важен елемент за изпълнението на новите задачи са мисиите за проверки и одити на място, които се оценяват на 200 000 евро годишно за всеки ЕНО. Разходите за превод на различните документи, които ЕНО ще получават от възлови доставчици трети страни на услуги в областта на ИКТ, също са част от оперативните разходи и възлизат на 350 000 евро годишно.

Всички горепосочени административни разходи ще бъдат изцяло финансирани от годишните такси, събирани от ЕНО от възловите доставчици трети страни на услуги в областта на ИКТ (без отражение върху бюджета на ЕС).