I

(Законодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ (ЕС) 2022/2554 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 14 декември 2022 година

относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

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

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

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

като имат предвид, че:

(1) В цифровата ера информационните и комуникационните технологии (ИКТ) са в основата на сложни системи, използвани в ежедневните дейности. ИКТ поддържат работата на икономиките ни в ключови сектори, включително финансовия сектор, и подобряват функционирането на вътрешния пазар. От друга страна, засилената цифровизация и взаимосвързаност засилват риска в областта на ИКТ, което прави обществото като цяло и финансовата система по-специално по-уязвими на киберзаплахи или смущения на ИКТ. Въпреки че повсеместното използване на системите на ИКТ и високата степен на цифровизация и свързаност са днес основни характеристики на дейностите на финансовите субекти на Съюза, предприемането на мерки по отношение на устойчивостта на използваните от тях цифрови технологии и интегрирането на тази устойчивост в по-широките им оперативни рамки все още предстои.

(2) През изминалите десетилетия използването на ИКТ придоби до такава степен ключова роля в предоставянето на финансови услуги, че днес се е превърнало в критично важен елемент за осъществяването на обичайните ежедневни функции на всички финансови субекти. Цифровизацията понастоящем обхваща например плащанията, които все повече преминават от методи, базирани на плащане в брой и използване на хартиен носител, към използването на цифрови решения, както и клиринг и сетълмент на ценни книжа, електронна и алгоритмична търговия, операции по кредитиране и финансиране, партньорско финансиране, присъждане на кредитен рейтинг, уреждане на застрахователни претенции и вътрешни за дружествата операции. Застрахователният сектор също претърпя сериозни

([1]) ОВ C 343, 26.8.2021 г., стр. 1.
([2]) ОВ C 155, 30.4.2021 г., стр. 38.
([3]) Позиция на Европейския парламент от 10 ноември 2022 г. (все още непубликувана в Официален вестник) и решение на Съвета от 28 ноември 2022 г.

промени вследствие на използването на ИКТ — от появата на застрахователни посредници, които предлагат своите услуги онлайн като работят със застрахователни технологии (InsurTech), до извършването на цифрова застрахователна дейност. Целият финансов сектор не само се цифровизира в голяма степен, но цифровизацията доведе и до задълбочаване на взаимните връзки и зависимости както в рамките на самия финансов сектор, така и с доставчици на инфраструктура и услуги, които са трети страни.

(3) В свой доклад от 2020 г., посветен на системния киберриск 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, би могла да представлява системна уязвимост, тъй като локализираните киберинциденти биха могли бързо, невъзпрепятствани от географските граници, да се разпространят от всеки от приблизително 22 000-те финансови субекта в Съюза в цялата финансова система. Сериозните пробиви в ИКТ във финансовия сектор не засягат само финансови субекти, взети изолирано едни от други. Те също така улесняват разпространението на локализирани уязвимости по финансовите трансмисионни канали и потенциално са източник на неблагоприятни последици за стабилността на финансовата система на Съюза, например генериране на загуби на ликвидност и общо намаляване на доверието и увереността във финансовите пазари.

(4) През последните години отговорните за политиките кадри, регулаторните органи и органите по стандартизация на международно, съюзно и национално равнище се заеха с риска в областта на ИКТ в опит да се повиши устойчивостта на цифровите технологии, да се установят стандарти и да се координира регулаторната 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 Г-7 и Г-20 се стремят да предоставят на компетентните органи и пазарните участници от различни юрисдикции инструменти за засилване на устойчивостта на техните финансови системи. Работата в тази насока се ръководи също от необходимостта за надлежно отчитане на риска в областта на ИКТ в контекста на една силно взаимосвързана глобална финансова система и за стремеж към по-голяма съгласуваност на съответните най-добри практики.

(5) Въпреки целевите политики и законодателни инициативи на национално равнище и на равнището на Съюза, рискът в областта на ИКТ продължава да поражда предизвикателства за оперативната устойчивост, функционирането и стабилността на финансовата система на Съюза. Реформите, последвали финансовата криза от 2008 г., най-вече засилиха финансовата устойчивост на финансовия сектор на Съюза и бяха насочени към запазване на конкурентоспособността и стабилността на Съюза от икономическа и пруденциална гледна точка и от гледна точка на поведението на пазара. Въпреки че сигурността на ИКТ и устойчивостта на цифровите технологии са част от операционния риск, в следкризисната регулаторна програма им беше обърнато по-малко внимание и те претърпяха развитие само в някои области на политиката и регулаторната среда на финансовите услуги на Съюза или само в няколко държави членки.

(6) В своето съобщение от 8 март 2018 г., озаглавено „План за действие в областта на финансовите технологии — за по-конкурентоспособен и иновативен европейски финансов сектор“ Комисията подчерта, че осигуряването на по-голяма устойчивост на финансовия сектор на Съюза е от първостепенно значение, включително в оперативен аспект, за да се гарантират технологичната му сигурност и доброто функциониране, бързото му възстановяване след пробиви и инциденти с ИКТ, което в крайна сметка да позволи ефективно и безпрепятствено предоставяне на финансови услуги в целия Съюз, включително в ситуации на стрес, като същевременно се запазят доверието и увереността на потребителите и пазара.

(7) През април 2019 г. Европейският надзорен орган (Европейски банков орган — ЕБО), създаден с Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([4]), Европейският надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване — ЕОЗППО), създаден с Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета ([5]), и Европейският надзорен орган (Европейски орган за ценни книжа и

([4]) Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12).

([5]) Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/79/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 48).

пазари — ЕОЦКП), създаден с Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета ([6]) (заедно известни като „Европейски надзорни органи“ или „ЕНО“), съвместно публикуваха техническо становище, в което призоваха за възприемането на съгласуван подход към риска в областта на ИКТ във финансовия сектор и препоръчаха да се засили по пропорционален начин оперативната устойчивост на цифровите технологии в сектора на финансовите услуги чрез секторно насочена инициатива на Съюза.

(8) Финансовият сектор на Съюза се регулира 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 хармонизирани изцяло или последователно, независимо от факта, че оперативната устойчивост на цифровите технологии е от ключово значение за гарантиране на финансовата стабилност и интегритета на пазара в цифровата ера, като е не по-малко важна например от общите пруденциални стандарти или стандартите за пазарно поведение. Поради това единната нормативна уредба и надзорната система следва да бъдат развити така, че да обхванат и оперативната устойчивост на цифровите технологии чрез укрепване на мандатите на компетентните органи, което да им позволи да упражняват надзор върху управлението на риска в областта на ИКТ във финансовия сектор с цел да се защитят интегритетът и ефикасността на вътрешния пазар и да се подпомогне безпроблемното му функциониране.

(9) Нормативните несъответствия и различията в националните регулаторни или надзорни подходи по отношение на риска в областта на ИКТ създават пречки за функционирането на вътрешния пазар на финансови услуги, като възпрепятстват безпроблемното упражняване на свободата на установяване и предоставянето на услуги от финансовите субекти с трансгранична дейност. Конкуренцията между един и същ вид финансови субекти с дейност в различни държави членки би могла също да бъде нарушена. Това важи по-специално за области, в които хармонизацията на равнището на Съюза е съвсем ограничена, например тестване на оперативната устойчивост на цифровите технологии, или в които хармонизация изобщо не съществува, например наблюдението на риска в областта на ИКТ, пораждан от трета страна. Различията в резултат на планирани национални мерки биха могли допълнително да затруднят функционирането на вътрешния пазар в ущърб на пазарните участници и финансовата стабилност.

(10) Към настоящия момент, поради частичния подход на равнището на Съюза по отношение на разпоредбите, свързани с риска в областта на ИКТ, има празноти или препокривания във важни области, например при докладването на инциденти с ИКТ и тестването на оперативната устойчивост на цифровите технологии, както и непоследователност, която се дължи на въвеждане на разнопосочни национални правила или икономически неефективно прилагане на припокриващи се правила. Особено потърпевши от това са интензивно ползващите ИКТ, например финансовият сектор, тъй като технологичните рискове нямат граници, а финансовият сектор разгръща услугите си в широк международен мащаб в рамките на Съюза и извън него. Отделните финансови 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 компетентен орган в една или няколко държави членки) се сблъскват с оперативни предизвикателства, когато желаят самостоятелно и по последователен икономически ефективен начин да управляват риска в областта на ИКТ и да ограничават неблагоприятното въздействие на инцидентите с ИКТ.

(11) Единната нормативна уредба не е придружена от всеобхватна уредба на риска в областта на ИКТ или на операционния риск, поради което е необходимо допълнително хармонизиране на ключовите изисквания за всички финансови субекти във връзка с оперативната устойчивост на цифровите технологии. Развиването на капацитета на ИКТ и на общата устойчивост от финансовите субекти въз основа на тези ключови изисквания с цел да се преодоляват оперативните неизправности, ще допринесе за запазването на стабилността и интегритета на финансовите пазари на Съюза и оттам — за осигуряването на висока степен на защита на инвеститорите и потребителите в Съюза. Тъй като целта на настоящия регламент е да допринесе за гладкото функциониране на вътрешния пазар, той следва да се основава на разпоредбите на член 114 от Договора за функционирането на Европейския съюз (ДФЕС) съгласно тълкуването на този член в съдебната практика на Съда на Европейския съюз (наричан по-нататък „Съда“).

(12) Целта на настоящия регламент е да се консолидират и подобрят изискванията във връзка с риска в областта на ИКТ като част от изискванията за операционния риск, които към настоящия момент се разглеждат отделно в различни правни актове на Съюза. Макар че тези актове обхващат основните категории финансов риск (напр. кредитен риск, пазарен риск, кредитен риск и ликвиден риск от контрагента, риск във връзка с пазарното поведение), към момента на приемането им в тях не са включени всеобхватно всички компоненти на оперативната устойчивост. При доразвиването на нормите за операционния риск в правните актове на Съюза често беше предпочитан традиционният количествен подход по отношение на риска (а именно определяне на капиталово изискване за покриване на риска в областта на ИКТ) вместо целенасочени норми за качество във връзка с капацитета за защита,

([6]) Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за създаване на Европейски надзорен орган (Европейски орган за ценни книжа и пазари), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/77/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 84).

установяване, ограничаване, възстановяване на информацията и възобновяване на обичайното функциониране при инциденти, засягащи ИКТ, или за капацитета за докладване и цифрово тестване. С тези актове се целеше най-вече включване и актуализиране на основните правила за пруденциален надзор, интегритет на пазара или пазарно поведение. Посредством консолидирането и актуализирането на различните правила за риска в областта на ИКТ, всички разпоредби, посветени на цифровия риск във финансовия сектор, следва за първи път да бъдат последователно обединени в един единствен законодателен акт. Следователно с настоящия регламент се запълват празнотите или се отстраняват несъответствията в някои от предходните правни актове, включително по отношение на използваната в тях терминология, и изрично се прави позоваване на риска в областта на ИКТ чрез целенасочени правила за капацитета за управление на риска в областта на ИКТ, докладването на инциденти, тестването на оперативната устойчивост и наблюдението на риска в областта на ИКТ, пораждан от трети лица. Настоящият регламент следва също да повиши осведомеността относно риска в областта на ИКТ и да отчита факта, че инцидентите с ИКТ и липсата на оперативна устойчивост могат да застрашат стабилността на финансовите субекти.

(13) В мерките си във връзка с риска в областта на ИКТ финансовите субекти следва да спазват един и същ подход и принципни правила, като отчитат размера и цялостния си рисков профил, както и естеството, мащабите и сложността на своите услуги, дейности и операции. Съгласуваността допринася за засилване на доверието във финансовата система и за съхраняване на нейната стабилност, особено във времена на голяма зависимост от системите, платформите и инфраструктурите на ИКТ, която повишава риска при цифровите технологии. Спазването на елементарна киберхигиена би следвало също така да спести необходимостта от налагане на значителни разходи върху икономиката посредством свеждане до минимум на въздействието на смущенията на ИКТ и свързаните с тях разходи.

(14) Приемането на регламент спомага за намаляване на нормативната сложност, насърчава сближаването на надзорните практики, повишава правната сигурност, като освен това допринася за ограничаване на разходите за спазване на изискванията — особено за финансовите субекти с трансгранична дейност, и за намаляване на нарушаването на конкуренцията. Ето защо изборът на регламент за създаване на обща рамка за оперативната устойчивост на цифровите технологии при 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 в областта на ИКТ.

(15) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([7]) беше първата хоризонтална рамка в областта на киберсигурността, приета на равнището на Съюза, която се прилага освен това към три вида финансови субекти, а именно кредитни институции, места за търговия и централни контрагенти. Въпреки това, тъй като в Директива (ЕС) 2016/1148 е предвиден механизъм за определяне на национално равнище на операторите на основни услуги, само конкретни кредитни институции, места за търговия и централни контрагенти, които са били определени от държавите членки, са били включени на практика в нейния обхват и съответно подлежат на предвидените в нея изисквания за сигурност на ИКТ и за уведомяване за инцидентите с ИКТ. С Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([8]) се установява единен критерий за определяне на субектите, попадащи в нейния обхват (правило за размера на предприятието), като същевременно трите вида финансови субекти остават в приложното ѝ поле.

(16) Въпреки това, тъй като с настоящия регламент се повишава нивото на хармонизация на различните аспекти, свързани с устойчивостта на цифровите технологии, като се въвеждат изисквания относно управлението на риска в областта на ИКТ и докладването на инциденти с ИКТ, които са по-строги от предвидените в действащото право на Съюза в областта на финансовите услуги, това по-високо ниво представлява по-тясна хармонизация и в сравнение с изискванията, предвидени в Директива (ЕС) 2022/2555. Следователно настоящият регламент представлява *lex specialis* по отношение на Директива (ЕС) 2022/2555. Същевременно е изключително важно да се запази силна връзка между финансовия сектор и хоризонталната рамка на Съюза в областта на киберсигурността, установена понастоящем в Директива (ЕС) 2022/2555, за да се осигури съгласуваност с приетите от държавите членки стратегии за киберсигурност и да се даде възможност органите за финансов надзор да бъдат информирани за инциденти с киберсигурността, засягащи други сектори, попадащи в обхвата на посочената директива.

([7]) 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).

([8]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (вж. страница 80 от настоящия брой на Официален вестник).

(17) В съответствие с член 4, параграф 2 от Договора за Европейския съюз и без да се засяга съдебният контрол, упражняван от Съда, настоящият регламент не следва да засяга отговорността на държавите членки по отношение на основните държавни функции, свързани с обществената сигурност, отбраната и гарантирането на националната сигурност, например по отношение на предоставянето на информация, което би било в противоречие с гарантирането на националната сигурност.

(18) За да се осигури възможност за междусекторно прехвърляне на знанията и ефективно използване на придобития в други сектори опит при преодоляването на киберзаплахи, финансовите субекти, посочени в Директива (ЕС) 2022/2555, следва да останат част от „екосистемата“ на посочената директива (напр. групата за сътрудничество и екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС). ЕНО и националните компетентни органи следва да могат да участват в обсъжданията на стратегическата политика и в техническата работа на групата за сътрудничество съгласно посочената директива, както и да обменят информация и да поддържат по-тясно сътрудничество с единните звена за контакт, определени или установени в съответствие с посочената директива. Компетентните органи съгласно настоящия регламент следва също така да провеждат консултации и да си сътрудничат с ЕРИКС. Наред с това, компетентните органи следва да могат да искат технически становища от компетентните органи, определени или установени в съответствие с Директива (ЕС) 2022/2555, и да установяват договорености за сътрудничество с оглед на осигуряването на ефективни и гарантиращи бърза реакция координационни механизми.

(19) Като се имат предвид силните взаимовръзки между устойчивостта на цифровите технологии и физическата устойчивост на финансовите субекти, е необходимо в настоящия регламент и в Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета ([9]) да се възприеме съгласуван подход по отношение на устойчивостта на критичните субекти. Като се има предвид, че физическата устойчивост на финансовите субекти е изчерпателно регламентирана чрез задълженията за управление и докладване на риска в областта на ИКТ, предвидени в настоящия регламент, задълженията, установени в глави III и IV от Директива (ЕС) 2022/2557, не следва да се прилагат за финансовите субекти, попадащи в обхвата на посочената директива.

(20) Доставчиците на компютърни услуги „в облак“ са сред категориите цифрови инфраструктури, обхванати от Директива (ЕС) 2022/2555. Създадената с настоящия регламент надзорна рамка на Съюза (наричана по-нататък „надзорната рамка“) се прилага спрямо всички трети страни критични доставчици на услуги в областта на ИКТ включително доставчиците на компютърни услуги „в облак“, които предоставят услуги в областта на ИКТ на финансови субекти, и следва да се счита за допълваща надзора, осъществяван съгласно Директива (ЕС) 2022/2555. Наред с това, надзорната рамка, създадена с настоящия регламент, следва да обхваща доставчиците на компютърни услуги „в облак“, докато няма хоризонтална рамка на Съюза, с която се създава орган за надзор на цифровите услуги.

(21) С цел да се поддържа пълен контрол върху риска в областта на ИКТ, финансовите субекти трябва да разполагат с всеобхватен капацитет, който да позволява стабилно и ефективно управление на риска в областта на ИКТ, както и със специални механизми и политики за справяне с всички инциденти с ИКТ и за докладване на съществените инциденти с ИКТ. Аналогично, финансовите субекти следва да разполагат с политики за тестване на системите, контролите и процесите на ИКТ, както и за управление на риска в областта на ИКТ, пораждан от трета страна. Базовите стандарти за оперативната устойчивост на цифровите технологии на финансовите субекти следва да бъдат повишени, като същевременно се осигури възможност за съизмеримо прилагане на изискванията спрямо определени финансови субекти, по-специално микропредприятия, както и спрямо финансови субекти, за които се прилага опростена рамка за управление на риска в областта на ИКТ. За да се улесни упражняването на ефикасен надзор над институциите за професионално пенсионно осигуряване, който е пропорционален и отразява необходимостта от намаляване на административната тежест за компетентните органи, съответните национални надзорни договорености по отношение на такива финансови субекти следва да отчитат техния размер и цялостен рисков профил, както и естеството, мащаба и сложността на техните услуги, дейности и операции, дори когато са превишени съответните прагове, установени в член 5 от Директива (ЕС) 2016/2341 на Европейския парламент и на Съвета ([10]). По-специално, надзорните дейности следва да се съсредоточат главно върху необходимостта от преодоляване на сериозните рискове, свързани с управлението на риска в областта на ИКТ на конкретен субект.

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

([10]) Директива (ЕС) 2016/2341 на Европейския парламент и на Съвета от 14 декември 2016 г. относно дейностите и надзора на институциите за професионално пенсионно осигуряване (ИППО) (ОВ L 354, 23.12.2016 г., стр. 37).

Компетентните органи следва също да поддържат строг, но пропорционален подход по отношение на надзора над институциите за професионално пенсионно осигуряване, които в съответствие с член 31 от Директива (ЕС) 2016/2341 възлагат на външни доставчици на услуги значителна част от основната си дейност, например управление на активи, актюерски изчисления, счетоводство и управление на данни.

(22) Националните прагове и таксономии за докладване на инцидентите с ИКТ варират значително. Макар чрез съответната работа на Агенцията на Европейския съюз за киберсигурност (ENISA), създадена с Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета, ([11]) и на групата за сътрудничество съгласно Директива (ЕС) 2022/2555 да е възможно да бъдат постигнати допирни точки, по отношение на останалите финансови субекти все още има или могат да възникнат различни подходи към определянето на праговете и използването на таксономиите. В резултат на тези различия са налице множество изисквания, които финансовите субекти трябва да спазват, особено когато извършват дейност в няколко държави членки или са част от финансова група. Освен това такива различия имат потенциал да възпрепятстват създаването на допълнителни единни или централизирани механизми на Съюза, които да ускоряват процеса на докладване и да подпомагат бързия и безпрепятствен обмен на информация между компетентните органи, което е от решаващо значение за противодействие на риска в областта на ИКТ в случай на мащабни атаки с потенциално системни последствия.

(23) За да се намалят административната тежест и евентуалното дублиране на задължения за докладване за някои финансови субекти, изискването за докладване на инциденти съгласно Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета ([12]) следва да престане да се прилага по отношение на доставчиците на платежни услуги, които попадат в обхвата на настоящия регламент. Следователно кредитните институции, институциите за електронни пари, платежните институции и доставчиците на услуги по предоставяне на информация за сметка, посочени в член 33, параграф 1 от посочената директива, следва от датата на прилагане на настоящия регламент да докладват съгласно настоящия регламент всички оперативни или свързани със сигурността инциденти, свързани с плащания, които досега са били докладвани съгласно посочената директива, независимо дали тези инциденти са свързани с ИКТ.

(24) С цел да се осигури възможност на компетентните органи да упражняват надзорни функции, придобивайки пълна представа за естеството, честотата, значимостта и въздействието на инцидентите с ИКТ, както и за да се подобри обменът на информация между съответните публични органи, включително правоприлагащите органи и органите за преструктуриране, в настоящия регламент следва да се предвиди стриктен режим за докладване на инциденти с ИКТ, така че чрез съответните изисквания да се запълнят празнотите, които понастоящем съществуват в законодателството в областта на финансовите услуги, и да се премахнат съществуващите припокривания и дублирания, за да се намалят разходите. От първостепенно значение е да се хармонизира режимът за докладване на инциденти с ИКТ, като се въведат изисквания всички финансови субекти да докладват на компетентните си органи чрез единна рационализирана рамка, както е посочено в настоящия регламент. Освен това на ЕНО следва да бъде предоставено правомощието да доуточняват съответните елементи на рамката за докладване на инциденти с ИКТ, напр. таксономия, времеви рамки, набори от данни, образци и приложими прагове. За да се осигури пълно съответствие с Директива (ЕС) 2022/2555, на финансовите субекти следва да бъде разрешено на доброволна основа да уведомяват съответния компетентен орган за значителни киберзаплахи, когато считат, че киберзаплахата засяга финансовата система, ползвателите на услуги или клиентите.

(25) В някои финансови подсектори бяха разработени изисквания за тестване на оперативната устойчивост на цифровите технологии, установяващи рамки, които невинаги са напълно съгласувани. Това води до потенциално дублиране на разходите за трансграничните финансови субекти и усложнява взаимното признаване на резултатите от тестването на оперативната устойчивост на цифровите технологии, което от своя страна може да предизвика фрагментиране на вътрешния пазар.

([11]) 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).

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

(26) Наред с това, когато не се изисква тестване на ИКТ, уязвимите места остават неразкрити и водят до излагане на финансовия субект на риск в областта на ИКТ, като в крайна сметка създават по-висок риск за стабилността и интегритета на финансовия сектор. Без намеса от страна на Съюза тестването на оперативната устойчивост на цифровите технологии ще продължи да бъде непоследователно и без установена система за взаимно признаване на тестовите резултати за ИКТ в отделните юрисдикции. Освен това, предвид слабата вероятност другите финансови подсектори да възприемат схеми за тестване в значим мащаб, те биха пропуснали потенциалните ползи на една рамка за тестване, що се отнася до разкриването на уязвимите места и рисковете, свързани с ИКТ, и на тестването на капацитета за защита и за непрекъснатост на дейността, което допринася за повишаване на доверието на потребителите, доставчиците и търговските партньори. С цел да се отстранят тези припокривания, различия и празноти, е необходимо да се установят правила за координиран режим на тестване, с което ще се улесни взаимното признаване на обстойните тестове, провеждани от финансовите субекти, отговарящи на критериите, определени в настоящия регламент.

(27) Фактът, че финансовите субекти са зависими от използването на услуги в областта на ИКТ, се дължи отчасти на необходимостта да се адаптират към нововъзникващата конкурентна цифрова глобална икономика, да повишат ефикасността на дейността си и да удовлетворят потребителското търсене. В последните години естеството и обхватът на тази зависимост се променят непрекъснато, което доведе до намаляване на разходите за финансово посредничество, позволи разширяването и разрастването на финансовите дейности и същевременно предложи богат инструментариум, основан на ИКТ, за управление на сложните вътрешни процеси.

(28) За широкото използване на услугите в областта на ИКТ свидетелстват сложните договорни споразумения, в чиито рамки финансовите субекти често срещат затруднения при договарянето на условия, които са съобразени с пруденциалните стандарти или други регулаторни изисквания, приложими към тях, или при ефективното упражняване на специфични права, например права за достъп или одит, дори когато последните са заложени в договорните им споразумения. Освен това, много от тези договорни споразумения не предвиждат достатъчно гаранции, които да позволят цялостното наблюдение на процесите на възлагане на дейности на подизпълнители, което лишава финансовите субекти от способността да оценяват свързаните рискове. В допълнение, поради факта, че третите страни доставчици на услуги в областта на ИКТ често предоставят стандартизирани услуги на различни видове клиенти, подобни договорни споразумения не винаги обслужват адекватно индивидуалните или специфичните нужди на участниците от финансовия сектор.

(29) Въпреки че правото на Съюза в областта на финансовите услуги съдържа някои общи правила относно възлагането на дейности на външни изпълнители, упражняването на наблюдение върху договорното измерение не е напълно установено в правото на Съюза. Поради липсата на ясни и специално пригодени стандарти на Съюза, които да се прилагат за договорните споразумения, сключени с трети страни доставчици на услуги в областта на ИКТ, не се предприемат изчерпателни мерки за отстраняване на външния източник на риск в областта на ИКТ. Поради това е необходимо да се определят някои основни принципи, които да ръководят финансовите субекти при управлението на риска в областта на ИКТ, пораждан от трети страни, като тези принципи са особено важни, когато финансовите субекти прибягват до трети страни доставчици на услуги в областта на ИКТ, за да поддържат изпълняваните от тях критични или важни функции. Тези принципи следва да бъдат придружени от набор от основни договорни права във връзка с някои елементи при изпълнението и прекратяването на договорните споразумения, за да се осигурят определени минимални гаранции с цел укрепване на способността на финансовите субекти ефективно да следят всеки риск в областта на ИКТ, който възниква на равнището на трети страни доставчици на услуги. Тези принципи допълват секторното право, приложимо към възлагането на дейности на външни изпълнители.

(30) Понастоящем се наблюдава известна липса на хомогенност и сближаване по отношение на наблюдението на риска в областта на ИКТ, пораждан от трети страни, и на зависимостта от трети страни доставчици на услуги в областта на ИКТ. Въпреки усилията за регламентиране на възлагането на дейности на външни изпълнители, например Насоките на ЕБО за възлагане на дейности на външни изпълнители от 2019 г. и Насоките на ЕОЦКП относно възлагането на дейности на доставчици на компютърни услуги „в облак“ от 2021 г., по-широкият въпрос за противодействие на системния риск, който може да възникне от експозицията на финансовия сектор към ограничен брой трети страни критични доставчици на услуги в областта на ИКТ не е застъпен в достатъчна степен в законодателството на Съюза. Липсата на правила на равнището на Съюза се утежнява от липсата на национални правила относно правомощията и инструментите, които да позволят на органите за финансов надзор да разберат добре зависимостите от трети страни доставчици на услуги в областта на ИКТ и адекватно да следят рисковете, произтичащи от концентрацията на зависимости от трети страни доставчици на услуги в областта на ИКТ.

(31) Предвид потенциалния системен риск, породен от разрастващата се практика на възлагане на дейности на външни изпълнители и от концентрацията на трети страни доставчици на услуги в областта на ИКТ, и в контекста на недостатъчните национални механизми, които да предоставят на органите за финансов надзор адекватни инструменти за количествено и качествено определяне и противодействие на последиците от риска в областта на ИКТ, възникващ при трети страни критични доставчици на услуги в областта на ИКТ, е необходимо да бъде създадена подходяща надзорна рамка, която да позволява непрекъснато наблюдение на дейностите на третите страни доставчици на услуги в областта на ИКТ, които са критични доставчици на услуги в областта на ИКТ за финансовите субекти, като същевременно се гарантира опазването на поверителността и сигурността на потребителите, които не са финансови субекти. Въпреки че вътрешногруповото предоставяне на услуги в областта на ИКТ поражда специфични рискове и ползи, то не следва автоматично да се счита за по-малко рисково от предоставянето на услуги в областта на ИКТ от доставчици извън финансова група и поради това следва да се подчинява на същата регулаторна рамка. Когато обаче услугите в областта на ИКТ се предоставят от доставчици, които принадлежат към същата финансова група, финансовите субекти може да имат по-високо ниво на контрол върху вътрешногруповите доставчици, което следва да се взема предвид при цялостната оценка на риска.

(32) Тъй като рисковете в областта на ИКТ стават все по-сложни и комплексни, добрите мерки за откриване и предотвратяване на риска в областта на ИКТ зависят до голяма степен от редовния обмен между финансовите субекти на разузнавателни сведения за заплахите и уязвимите места. Обменът на информация допринася за създаване на повишена осведоменост относно киберзаплахите. От своя страна, това увеличава капацитета на финансовите субекти да предотвратяват превръщането на киберзаплахите в реални инциденти с ИКТ и позволява на финансовите субекти по-ефективно да ограничават въздействието на инцидентите с ИКТ и да се възстановяват по-бързо. При липсата на насоки на равнището на Съюза няколко фактора, изглежда, възпрепятстват обмена на разузнавателни сведения, по-специално несигурността по отношение на съвместимостта на този обмен със защитата на данните, антитръстовите норми и правилата за отговорността.

(33) Наред с това съмненията относно 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. Следователно обхватът и качеството на обмена на информация понастоящем остават ограничени и фрагментарни — като полезен обмен се осъществява предимно на местно равнище (чрез национални инициативи) и без съобразени с потребностите на интегрираната финансова система съгласувани споразумения за обмен на информация на равнището на Съюза. Следователно е важно тези канали за комуникация да бъдат укрепени.

(34) Финансовите субекти следва да бъдат насърчавани да обменят помежду си информация и разузнавателни сведения за киберзаплахи и да използват колективно индивидуалните си знания и практически опит на стратегическо, тактическо и оперативно ниво, за да повишат капацитета си за адекватно оценяване, наблюдение, защита и реакция срещу киберзаплахи, посредством участие в споразумения за обмен на информация. Следователно е необходимо да се създадат условия за възникване на равнището на Съюза на механизми за договаряне на доброволен обмен на информация, който, провеждан в защитена среда, ще помага на общността на финансовия сектор да предотвратява и колективно да реагира на киберзаплахи чрез бързо ограничаване на разпространението на риска в областта на ИКТ и възпрепятстване на потенциалното разпространение на проблемите по финансовите канали. Тези механизми следва да спазват приложимите правни норми на Съюза в областта на конкуренцията, посочени в Съобщението на Комисията от 14 януари 2011 г., озаглавено „Насоки относно приложимостта на член 101 от Договора за функционирането на Европейския съюз по отношение на споразуменията за хоризонтално сътрудничество“, както и правилата на Съюза за защита на данните, по-специално Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([13]). Те следва да функционират въз основа на използването на едно или повече от правните основания, предвидени в член 6 от посочения регламент, например в контекста на обработване на лични данни, което е необходимо за целите на легитимните интереси на администратора или на трета страна съгласно член 6, параграф 1, буква е) от посочения регламент, както и в контекста на обработване на лични данни, необходимо за спазването на правно задължение, което се прилага спрямо администратора, или необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора, съгласно посоченото съответно в член 6, параграф 1, букви в) и д) от същия регламент.

([13]) 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) С цел да се поддържа високо равнище на оперативна устойчивост на цифровите технологии за целия финансов сектор и същевременно да не се изостава от технологичното развитие, настоящият регламент следва да се отнася за риска, произтичащ от всички видове услуги в областта на ИКТ. За тази цел определението за услуги в областта на ИКТ в контекста на настоящия регламент следва да се разбира в широк смисъл, като включващо цифровите услуги и услугите за данни, предоставяни чрез системите на ИКТ на един или повече вътрешни или външни ползватели на текуща основа. Това определение следва например да включва т. нар. услуги OTT (over the top), които попадат в категорията на електронните съобщителни услуги. Определението следва да изключва само ограничената категория традиционни аналогови телефонни услуги, които се квалифицират като услуги на обществена комутируема аналогова телефонна мрежа (PSTN), наземни телефонни услуги, услуги на аналогова телефонна мрежа (POTS) или стационарни телефонни услуги.

(36) Независимо от предвидения широк обхват на настоящия регламент, при прилагането на правилата относно оперативната устойчивост на цифровите технологии следва да се имат предвид значителните разлики между финансовите субекти по отношение на техния размер и цялостен рисков профил. Като общ принцип, при разпределянето на ресурси и оперативен капацитет за прилагане на рамката за управление на риска в областта на ИКТ финансовите субекти следва да постигнат нужния баланс между потребностите си, свързани с ИКТ, и своя размер и цялостен рисков профил, естеството, мащаба и сложността на предлаганите от тях услуги и извършваните дейности и операции, а компетентните органи следва да продължат да оценяват и преразглеждат подхода към такова разпределяне.

(37) Доставчиците на услуги по предоставяне на информация за сметка, посочени в член 33, параграф 1 от Директива (ЕС) 2015/2366, са изрично включени в обхвата на настоящия регламент предвид специфичния характер на техните дейности и произтичащите от тях рискове. Освен това институциите за електронни пари и платежните институции, освободени съгласно член 9, параграф 1 от Директива 2009/110/ЕО на Европейския парламент и на Съвета ([14]) и член 32, параграф 1 от Директива (ЕС) 2015/2366, са включени в обхвата на настоящия регламент, дори да не са получили лиценз в съответствие с Директива 2009/110/ЕО за издаване на електронни пари или ако не са получили лиценз в съответствие с Директива (ЕС) 2015/2366 за предоставяне и извършване на платежни услуги. Пощенските джиро институции, посочени в член 2, параграф 5, точка 3 от Директива 2013/36/ЕС на Европейския парламент и на Съвета ([15]) обаче, са изключени от обхвата на настоящия регламент. Компетентен орган за платежните институции, освободени съгласно Директива (ЕС) 2015/2366, институциите за електронни пари, освободени съгласно Директива 2009/110/ЕО, и доставчиците на услуги по предоставяне на информация за сметка, посочени в член 33, параграф 1 от Директива (ЕС) 2015/2366, следва да бъде компетентният орган, определен в съответствие с член 22 от Директива (ЕС) 2015/2366.

(38) По-големите финансови субекти потенциално разполагат с повече ресурси и могат бързо да мобилизират средства за създаването на управленски структури и въвеждането на различни корпоративни стратегии, поради което създаване на по-сложни управленски механизми следва да се изисква само от финансовите субекти, които не са микропредприятия по смисъла на настоящия регламент. Такива субекти могат по-лесно да въведат специални управленски функции за надзор на споразуменията с третите страни доставчици на услуги в областта на ИКТ или за управление на кризи, да организират своето управление на риска в областта на ИКТ според модела на трите защитни слоя или да установят вътрешна система за управление и контрол на риска и да подлагат на вътрешен одит рамката си за управление на риска в областта на ИКТ.

(39) Някои финансови субекти се ползват от освобождаване или за тях се прилага много по-облекчена регулаторна рамка съгласно приложимото специфично секторно законодателство на Съюза. Тези финансови субекти включват лица, управляващи алтернативни инвестиционни фондове, посочени в член 3, параграф 2 от Директива 2011/61/ЕС на Европейския парламент и на Съвета ([16]), застрахователни и презастрахователни предприятия, посочени в член 4 от Директива 2009/138/ЕО на Европейския парламент и на Съвета ([17]), и институции за професионално пенсионно осигуряване, които управляват пенсионни схеми, включващи общо по-малко от 15 членове. С оглед на тези

([14]) 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).

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

([16]) Директива 2011/61/ЕС на Европейския парламент и на Съвета от 8 юни 2011 г. относно лицата, управляващи алтернативни инвестиционни фондове, и за изменение на директиви 2003/41/ЕО и 2009/65/ЕО и на регламенти (ЕО) № 1060/2009 и (ЕС) № 1095/2010 (ОВ L 174, 1.7.2011 г., стр. 1).

([17]) Директива 2009/138/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 г. относно започването и упражняването на застрахователна и презастрахователна дейност (Платежоспособност II) (ОВ L 335, 17.12.2009 г., стр. 1).

освобождавания включването на такива финансови субекти в обхвата на настоящия регламент няма да бъде пропорционално. Освен това настоящият регламент отчита специфичните особености на пазарната структура на застрахователното посредничество, в резултат на което застрахователните посредници, презастрахователните посредници и посредниците, предлагащи застрахователни продукти като допълнителна дейност, квалифицирани като микропредприятия, или като малки или средни предприятия, не следва да бъдат подчинени на настоящия регламент.

(40) Тъй като субектите, посочени в член 2, параграф 5, точки 4—23 от Директива 2013/36/ЕС, са изключени от обхвата на посочената директива, държавите членки следва да могат да решат да освободят от прилагането на настоящия регламент такива субекти, установени на тяхна територия.

(41) Аналогично, за да се съгласува настоящият регламент с обхвата на Директива 2014/65/ЕС на Европейския парламент и на Съвета ([18]), е целесъобразно от обхвата на настоящия регламент да се изключат също физическите и юридическите лица, посочени в членове 2 и 3 от посочената директива, на които е разрешено да предоставят инвестиционни услуги без да е необходимо да получат лиценз съгласно Директива 2014/65/ЕС. Въпреки това, съгласно член 2 от Директива 2014/65/ЕС от нейния обхват са изключени и субекти, които се квалифицират като финансови субекти за целите на настоящия регламент, например централни депозитари на ценни книжа, предприятия за колективно инвестиране или застрахователни и презастрахователни предприятия. Изключването от обхвата на настоящия регламент на лицата и субектите, посочени в членове 2 и 3 от посочената директива, не следва да обхваща тези централни депозитари на ценни книжа, предприятия за колективно инвестиране или застрахователни и презастрахователни предприятия.

(42) Съгласно специфичното секторно законодателство на Съюза за някои финансови субекти се прилагат по-облекчени изисквания или освобождавания по причини, свързани с техния размер или предоставяните от тях услуги. Тази категория финансови субекти включва малки и невзаимосвързани инвестиционни посредници, малки институции за професионално пенсионно осигуряване, които могат да бъдат изключени от съответната държава членка от обхвата на Директива (ЕС) 2016/2341 при условията, предвидени в член 5 от същата директива, и които управляват пенсионни схеми, включващи общо по-малко от сто членове, както и институции, освободени съгласно Директива 2013/36/ЕС. Поради това, в съответствие с принципа на пропорционалност и за да се съхрани духът на специфичното секторно законодателство на Съюза, е целесъобразно също за тези финансови субекти да се прилага опростена рамка за управление на риска в областта на ИКТ съгласно настоящия регламент. Пропорционалният характер на рамката за управление на риска в областта на ИКТ, която обхваща тези финансови субекти, не следва да се нарушава от регулаторните технически стандарти, които трябва да бъдат разработени от ЕНО. Освен това, в съответствие с принципа на пропорционалност, е целесъобразно за платежните институции, посочени в член 32, параграф 1 от Директива (ЕС) 2015/2366, и за институциите за електронни пари, посочени в член 9 от Директива 2009/110/ЕО, които са освободени в съответствие с националното право, което транспонира тези правни актове на Съюза, да се прилага опростена рамка за управление на риска в областта на ИКТ съгласно настоящия регламент, докато платежните институции и институциите за електронни пари, които не са освободени съгласно съответното национално право, което транспонира секторното законодателство на Съюза, следва да спазват общата рамка, установена с настоящия регламент.

(43) Аналогично, от финансовите субекти, които се квалифицират като микропредприятия или за които се прилага опростената рамка за управление на риска в областта на ИКТ съгласно настоящия регламент, не следва да се изисква да определят функция за наблюдение на споразуменията им за използване на услуги в областта на ИКТ, сключени с трети страни доставчици на услуги в областта на ИКТ, нито да определят член на висшето ръководство, който да отговаря за упражняването на надзор върху свързаното с тези доставчици излагане на риск и съответната документация, нито да възлагат отговорността за управление и надзор на риска в областта на ИКТ на контролна функция и да гарантират подходящо равнище на независимост на тази контролна функция, за да се избегнат конфликти на интереси, нито да документират и преразглеждат поне веднъж годишно рамката за управление на риска в областта на ИКТ, нито да подлагат на периодичен вътрешен одит рамката за управление на риска в областта на ИКТ, нито да извършват обстойни оценки след съществени промени в инфраструктурата и процесите на своите мрежови и информационни системи, нито редовно да анализират риска при традиционните системи на ИКТ, нито да подлагат изпълнението на плановете за реакция и възстановяване на ИКТ на независими вътрешни одитни прегледи, нито да разполагат с функция за управление на кризи, да включат в тестването на непрекъснатостта на дейността и на плановете за реакция и възстановяване сценарии за преминаване от първичната инфраструктура на ИКТ към възпроизвеждащите я системи, нито да представят на компетентните органи, при поискване от тяхна страна,

([18]) Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС (ОВ L 173, 12.6.2014 г., стр. 349).

прогноза на съвкупните годишни разходи и загуби в резултат на съществени инциденти с ИКТ, нито да поддържат допълнителен капацитет в областта на ИКТ, нито да уведомяват националните компетентни органи за въведените промени в резултат на преглед на възникнали инциденти с ИКТ, нито постоянно да следят съответното технологично развитие, да създадат всеобхватна програма за тестване на оперативната устойчивост на цифровите технологии като неразделна част от рамката за управление на риска в областта на ИКТ, предвидена в настоящия регламент, или да приемат и подлагат на редовен преглед стратегия за риска в областта на ИКТ, пораждан от трета страна. Наред с това, от микропредприятията следва да се изисква само да оценяват необходимостта от поддържане на посочения допълнителен капацитет в областта на ИКТ въз основа на рисковия им профил. Микропредприятията следва да се ползват от по-гъвкав режим по отношение на програмите за тестване на оперативната устойчивост на цифровите технологии. Когато обмислят вида и честотата на тестванията, които трябва да бъдат осъществени, те следва да постигнат точен баланс между целта за поддържане на висока оперативна устойчивост на цифровите технологии, наличните ресурси и общия им рисков профил. Микропредприятията и финансовите субекти, които се подчиняват на опростената рамка за управление на риска в областта на ИКТ съгласно настоящия регламент, следва да бъдат освободени от изискването да извършват обстойно тестване на инструментите, системите и процесите на ИКТ чрез тестване за проникване (TLPT), тъй като само финансовите субекти, отговарящи на критериите, определени в настоящия регламент, следва да бъдат задължавани да извършват такова тестване. Предвид ограничените им възможности микропредприятията следва да могат да се договарят с третата страна доставчик на услуги в областта на ИКТ, че правата на достъп, проверка и одит на финансовия субект се делегират на независима трета страна, която се определя от третата страна доставчик на услуги в областта на ИКТ, при условие че финансовият субект може да поиска във всеки един момент от съответната независима трета страна цялата относима информация и гаранции относно резултатите от дейността на третата страна доставчик на услуги в областта на ИКТ.

(44) Предвид факта, че само финансовите субекти, определени за целите на обстойното тестване на устойчивостта на цифровите технологии, следва да подлежат на изискването за провеждане на тестване за проникване, административните процеси и финансовите разходи, свързани с провеждането на такива тестове, следва да се поемат от малък процент финансови субекти.

(45) С цел да се осигури пълно съответствие и обща съгласуваност на бизнес стратегиите на финансовите субекти, от една страна, и управлението на риска в областта на ИКТ, от друга, от ръководните органи на финансовите субекти следва да се изисква да играят водеща и активна роля в насочването и адаптирането на рамката за управление на риска в областта на ИКТ и на цялостната стратегия за оперативна устойчивост на цифровите технологии. Подходът, който трябва да бъде възприет от ръководните органи, следва да бъде съсредоточен не само върху средствата за осигуряване на устойчивост на системите на ИКТ, но следва да обхваща също 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 спазване на строга киберхигиена на всички равнища. Крайната отговорност на ръководния орган при управлението на риска в областта на ИКТ на финансовия субект следва да бъде основополагащ принцип на този цялостен подход и да се проявява по-нататък в непрекъсната ангажираност на ръководния орган с контрол върху наблюдението на управлението на риска в областта на ИКТ.

(46) Нещо повече, принципът на крайната и пълна отговорност на ръководния орган за управлението на риска в областта на ИКТ на финансовия субект е обвързан с необходимостта от осигуряване на определени инвестиции, свързани с ИКТ, и общ бюджет на финансовия субект, които да му позволят да постигне високо равнище на оперативна устойчивост на цифровите технологии.

(47) С настоящия регламент, в който са почерпени идеи от съответните международни, национални и секторни най-добри практики, насоки, препоръки и подходи за управление на киберриска, се насърчава набор от принципи, които улесняват цялостното структуриране на управлението на риска в областта на ИКТ. Следователно, стига основният капацитет, въведен от финансовите субекти, да обхваща различните функции в управлението на риска в областта на ИКТ (установяване, защита и предотвратяване, откриване, реакция и възстановяване, обучение и задълбочаване на познанията, и комуникиране), предвидени в настоящия регламент, финансовите субекти следва да имат свободата да използват модели за управление на риска в областта на ИКТ, които са различно структурирани или категоризирани.

(48) За да не се изостава от динамиката в развитието на киберзаплахите, финансовите субекти следва да поддържат актуални системи на ИКТ, които са надеждни и са способни не само да гарантират необходимото за предоставяните от тях услуги обработване на данни, но и да осигурят достатъчно техническа устойчивост, която да им позволи адекватно да удовлетворяват допълнителните нужди от обработка при неблагоприятни пазарни условия или други проблематични ситуации.

(49) Необходими са ефикасни планове за непрекъснатост на дейността и за възстановяване, които да позволяват на финансовите субекти да намират точни и бързи решения на инцидентите с ИКТ, и в частност на кибератаките, като ограничават щетите и дават приоритет на възобновяването на дейностите и мерките за възстановяване на информацията в съответствие с политиката им за съхраняване на резервни копия на данните. Това възобновяване на дейността обаче не следва по никакъв начин да застрашава интегритета и сигурността на мрежовите и информационните системи, нито наличността, автентичността, целостта или поверителността на данните.

(50) Независимо че настоящият регламент позволява на финансовите субекти да определят гъвкаво целите си за продължителността на възстановяване на информацията и за точката на възстановяване, което им дава възможност да установяват подобни цели, като се съобразяват изцяло с естеството и критичността на съответните функции, както и с евентуалните специфични потребности, свързани с дейността, той следва все пак да изисква от тях при определянето на тези цели да извършват оценка на потенциалното общо въздействие върху пазарната ефективност.

(51) Разпространителите на кибератаки обикновено преследват финансови печалби директно при източника, като по този начин излагат финансовите субекти на значителни последици. С цел да не се допусне загуба на интегритета на системите на ИКТ или на достъпа до тях и съответно да се избегнат нарушения на сигурността на данните и увреждане на физическата инфраструктура на ИКТ, докладването на съществени инциденти с ИКТ от финансовите субекти следва да бъде значително подобрено и рационализирано. Докладването на инциденти с ИКТ следва да се хармонизира посредством въвеждането на изискване към всички финансови субекти за пряко докладване пред съответните национални компетентни органи. Когато финансов субект подлежи на надзор от повече от един национален компетентен орган, държавите членки следва да определят един-единствен компетентен орган като адресат на такова докладване. Кредитните институции, класифицирани като значими в съответствие с член 6, параграф 4 от Регламент (ЕС) № 1024/2013 на Съвета ([19]), следва да представят такива доклади на националните компетентни органи, които впоследствие следва да ги предават на Европейската централна банка (ЕЦБ).

(52) Прякото докладване следва да позволи на органите за финансов надзор да получават незабавен достъп до информация за съществени инциденти с ИКТ. Органите за финансов надзор следва, от своя страна, да предават информация за съществени инциденти с ИКТ на публичните нефинансови органи (например компетентните органи и единните звена за контакт съгласно Директива (ЕС) 2022/2555, националните органи за защита на данните, а също и на правоприлагащите органи, когато става въпрос за съществени инциденти с ИКТ с престъпен характер), за да се повиши осведомеността на тези органи за такива инциденти, а в случая с ЕРИКС — да се улесни своевременното оказване на помощ на финансовите субекти, когато е целесъобразно. Освен това, държавите членки следва да могат да определят, че самите финансови субекти следва да предоставят такава информация на публичните органи извън сферата на финансовите услуги. Тези информационни потоци следва да позволят на финансовите субекти бързо да се възползват от всяка относима техническа информация, съвети относно корективните мерки и последващи действия от страна на посочените органи. Информацията за съществени инциденти с ИКТ следва да бъде предавана по веригата: органите за финансов надзор следва да предоставят цялата необходима обратна информация или насоки на финансовия субект, а ЕНО следва да споделят анонимизирани данни за киберзаплахите и уязвимите места, свързани с даден инцидент, с цел да се спомогне за по-широко колективно противодействие.

(53) Въпреки че от всички финансови субекти следва да се изисква да докладват за инциденти, не се очаква това изискване да ги засегне всички по един и същи начин. Всъщност съответните прагове на същественост и сроковете за докладване следва да бъдат надлежно адаптирани в контекста на делегирани актове, основани на регулаторните технически стандарти, които ще бъдат разработени от ЕНО, с цел да се обхванат само съществените инциденти с ИКТ. Освен това при определянето на сроковете за задълженията за докладване следва да се вземат предвид специфичните особености на финансовите субекти.

(54) Настоящият регламент следва да изисква от кредитните институции, платежните институции, доставчиците на услуги по предоставяне на информация за сметка и институциите за електронни пари да докладват за всички операционни или свързани със сигурността инциденти, свързани с плащания — докладвани досега съгласно Директива (ЕС) 2015/2366 — независимо от естеството на инцидента с ИКТ.

([19]) 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).

(55) ЕНО следва да бъдат натоварени със задачата да оценяват осъществимостта и условията за евентуално централизиране на докладите за инциденти с ИКТ на равнището на Съюза. Подобно централизиране може да се изразява във въвеждането на единен портал на ЕС за докладване на съществени инциденти с ИКТ, който или пряко да получава съответните доклади и автоматично да уведомява националните компетентни органи, или само да централизира съответните доклади, препращани от националните компетентни органи, изпълнявайки по този начин координационни функции. ЕНО следва да бъдат натоварени със задачата да изготвят, като се консултират с ЕЦБ и ENISA, съвместен доклад за осъществимостта на създаването на единен портал на ЕС.

(56) С цел да се постигне високо равнище на оперативна устойчивост на цифровите технологии и в съответствие както с приложимите международни стандарти (напр. изложените от Г-7 базови елементи на тестването за проникване), така и с прилаганите в Съюза рамки, напр. TIBER-EU, финансовите субекти следва редовно да тестват доколко ефективно системите им на ИКТ и персоналът им с отговорности в областта на ИКТ са способни да предотвратяват, откриват и реагират на инциденти в областта на ИКТ и да възстановяват информацията, както и да установяват и премахват потенциалните уязвими места на ИКТ. За да се отразят съществуващите различия между отделните финансови подсектори и в рамките на един и същ подсектор по отношение на нивото на подготвеност на финансовите субекти в областта на киберсигурността, тестването следва да обхваща широк набор от инструменти и действия, вариращи от оценяването на базовите изисквания (напр. оценки и сканиране на уязвимите места, анализ на приложенията с отворен код, оценки на сигурността на мрежата, анализ на пропуските, преглед на физическата сигурност, анкети и софтуерни продукти за сканиране, преглед на първичния код, когато такъв е осъществим, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането или тестване по цялата верига) до по-обстойно тестване посредством тестване за проникване. Такова обстойно тестване следва да се изисква само от финансови субекти, които са достатъчно развити от гледна точка на ИКТ, за да могат да го извършват адекватно. Поради това тестването на оперативната устойчивост на цифровите технологии, изисквано съгласно настоящия регламент, следва да бъде по-обстойно при финансовите субекти, отговарящи на критериите, определени в настоящия регламент (напр. големи, системни кредитни институции, които са развити от гледна точка на ИКТ, фондови борси, централни депозитари на ценни книжа и централни контрагенти), отколкото при другите финансови субекти. Същевременно тестването на оперативната устойчивост на цифровите технологии посредством тестване за проникване следва да бъде по-приложимо за финансови субекти, които осъществяват дейност в подсектори за основни финансови услуги и имат системна роля (напр. плащания, банково дело, клиринг и сетълмент), и по-малко приложимо за други подсектори (напр. управители на активи и агенции за кредитен рейтинг).

(57) Финансовите субекти с трансгранична дейност, които упражняват свободата си на установяване или на предоставяне на услуги в Съюза, следва да спазват единен набор от изисквания за обстойно тестване (т.е. тестването за проникване) в своята държава членка по произход, които следва да обхващат и инфраструктурите на ИКТ във всички юрисдикции в Съюза, където трансграничната финансова група извършва дейност, което ще позволи на такива трансгранични финансови групи да правят разходи за тестване на ИКТ само в една юрисдикция.

(58) С цел да се използва експертният опит, който вече е придобит от някои компетентни органи, по-специално по отношение на прилагането на рамката TIBER-EU, настоящият регламент следва да позволява на държавите членки да определят един публичен орган на национално равнище, който да отговаря за финансовия сектор по всички въпроси, свързани с тестването за проникване, или следва да позволява на компетентните органи да делегират, при липса на определен такъв орган, изпълнението на задачи, свързани с тестване за проникване, на друг национален финансов компетентен орган.

(59) Тъй като настоящият регламент не изисква от финансовите субекти да обхванат всички критични или важни функции в едно-единствено тестване за проникване, финансовите субекти следва да разполагат със свободата сами да определят кои и колко на брой критични или важни функции следва да бъдат включени в обхвата на такова тестване.

(60) Съвкупното тестване по смисъла на настоящия регламент — с участието на няколко финансови субекта в тестването за проникване и за което трета страна доставчик на услуги в областта на ИКТ може пряко да сключва договорни споразумения с външни лица, провеждащи тестове — следва да бъде разрешено само когато има разумни основания да се очаква, че качеството или сигурността на услугите, предоставяни от третата страна доставчик на услуги в областта на ИКТ на клиенти, които попадат извън обхвата на настоящия регламент, или поверителността на данните, свързани с такива услуги ще бъдат засегнати неблагоприятно. По отношение на съвкупното тестване следва също така да бъдат предвидени предпазни мерки (указания от един определен финансов субект, калибриране на броя на участващите финансови субекти), за да се гарантира, че участващите финансови субекти, които отговарят на целите на тестването за проникване съгласно настоящия регламент, се подлагат на строго тестване.

(61) За да се използват наличните на корпоративно равнище вътрешни ресурси, настоящият регламент следва да позволи използването на вътрешни лица, провеждащи тестове, за целите на извършването на тестване за проникване, при условие че е налице одобрение от страна на лицето, осъществяващо надзор, няма конфликт на интереси и се прилага периодично редуване при използването на вътрешни и външни лица, провеждащи тестове (на всеки три теста), като същевременно се изисква доставчикът на разузнавателните сведения за заплахи в тестването за проникване винаги да бъде външно лице за финансовия субект. Отговорността за провеждането на тестването за проникване следва да остане изцяло на финансовия субект. Удостоверенията, предоставяни от органите, следва да бъдат единствено за целите на взаимното признаване и не следва да изключват евентуални последващи действия, необходими за справяне с риска в областта на ИКТ, на който е изложен финансовият субект, нито следва да се разглеждат като надзорно одобрение на капацитета на финансовия субект за управление и намаляване на риска в областта на ИКТ.

(62) За да се гарантира надеждното наблюдение на риска в областта на ИКТ, пораждан от трета страна, във финансовия сектор, е необходимо да се установи набор от принципни правила, които да ориентират финансовите субекти при наблюдението на риска, възникващ в контекста на възлагането на функции на трети страни доставчици на услуги в областта на ИКТ, по-специално при услуги в областта на ИКТ, които поддържат критични или важни функции, и в по-общ план в контекста на всяка зависимост от трети страни доставчици на услуги в областта на ИКТ.

(63) За да се преодолее комплексният проблем, произтичащ от различните източници на риск в областта на ИКТ, като същевременно се вземат предвид множеството и разнообразието от доставчици на технологични решения, които позволяват безпроблемното предоставяне на финансови услуги, настоящият регламент следва да обхваща широк кръг от трети страни доставчици на услуги в областта на ИКТ, включително доставчици на компютърни услуги „в облак“, софтуер, услуги за анализ на данни и доставчици на услуги на център за данни. Аналогично, тъй като финансовите субекти следва ефективно и съгласувано да идентифицират и управляват всички видове риск, включително в контекста на услуги в областта на ИКТ, възлагани в рамките на финансова група, следва да се поясни, че предприятията, които са част от финансова група и предоставят услуги в областта на ИКТ предимно на своето предприятие майка или на дъщерни предприятия или клонове на своето предприятие майка, както и финансовите субекти, предоставящи услуги в областта на ИКТ на други финансови субекти, следва също да се считат за трети страни доставчици на услуги в областта на ИКТ съгласно настоящия регламент. На последно място, с оглед на нарастващата зависимост на пазара на платежни услуги от сложни технически решения и в контекста на нововъзникващите видове платежни услуги и решения, свързани с плащанията, участниците в екосистемата на платежните услуги, извършващи дейности по обработка на плащания или управляващи платежни инфраструктури, също следва да се считат за трети страни доставчици на услуги в областта на ИКТ съгласно настоящия регламент, с изключение на централните банки, когато управляват платежни системи или системи за сетълмент на ценни книжа, както и на публичните органи, когато предоставят услуги, свързани с ИКТ, в контекста на изпълнението на държавни функции.

(64) Финансовите субекти следва във всеки един момент да останат изцяло отговорни за спазването на задълженията си по настоящия регламент. Финансовите субекти следва да прилагат пропорционален подход към наблюдението на рисковете, възникващи на нивото на третите страни доставчици на услуги в областта на ИКТ, като надлежно отчитат естеството, степента, комплексния характер и значимостта на зависимостта си в областта на ИКТ, критичността или важността на възложените с договорни споразумения услуги, процеси или функции, и в крайна сметка въз основа на обстойно проучване на възможното потенциално въздействие върху непрекъснатостта и качеството на финансовите услуги на равнище отделен субект или на равнище група, както е целесъобразно.

(65) Осъществяването на такова наблюдение следва да се придържа към стратегически подход към риска в областта на ИКТ, пораждан от трети страни, който да бъде формализиран чрез приемането от ръководния орган на финансовия субект на специфична стратегия за риска в областта на ИКТ, пораждан от трети страни, основаваща се на непрекъснат анализ на всяка зависимост от трети страни доставчици на услуги в областта на ИКТ. За да се повиши осведомеността на надзорните органи относно зависимостта от трети страни доставчици на услуги в областта на ИКТ и с цел да се подпомогне допълнително работата в контекста на създадената с настоящия регламент надзорна рамка, от всички финансови субекти следва да се изисква да поддържат регистър с информация за всички договорни споразумения за използване на услуги в областта на ИКТ, предоставяни от трети страни доставчици на услуги в областта на ИКТ. Органите за финансов надзор следва да могат да изискват пълния регистър или да изискват отделни раздели от него и пози начин да получават съществена информация за придобиване на по-широко разбиране за зависимостите на финансовите субекти в областта на ИКТ.

(66) Формалното сключване на договорни споразумения следва да се крепи и да се предшества от предварителен обстоен анализ, по-специално с акцент върху елементи като критичността или важността на услугите, които ще се поддържат с предвидения договор за ИКТ, необходимите надзорни одобрения или други условия, възможния риск от концентрация, както и прилагането на надлежна проверка в процеса на подбор и оценка на третите страни доставчици на услуги в областта на ИКТ и оценка на потенциалните конфликти на интереси. За договорните споразумения, които засягат критични или важни функции, финансовите субекти следва да отчитат използването на най-актуалните и най-високите стандарти за сигурност на информацията от страна на третите страни доставчици на услуги в областта на ИКТ. Прекратяването на договорните споразумения може да бъде в резултат поне на поредица от обстоятелства, разкриващи недостатъци на ниво трета страна доставчик на услуги в областта на ИКТ,

по-специално съществени нарушения на закона или договорни условия, обстоятелства, разкриващи потенциална промяна в изпълнението на функциите, предвидени в договорните споразумения, доказателства за слабости в цялостното управление на риска в областта на ИКТ на третата страна доставчик на услуги в областта на ИКТ или обстоятелства, сочещи невъзможност на съответния компетентен орган да упражнява ефективен надзор върху финансовия субект.

(67) С цел да се противодейства на системния ефект на риска от концентрация, свързан с трети страни доставчици на услуги в областта на ИКТ, настоящият регламент насърчава балансирано решение посредством възприемането на гъвкав и поетапен подход към този риск от концентрация, тъй като налагането на всякакви строги тавани или стриктни ограничения може да възпрепятства осъществяването на дейността и да ограничи свободата на договаряне. Финансовите субекти следва да извършват задълбочена оценка на планираните от тях договорни споразумения, за да определят вероятността от възникване на такъв риск, включително чрез задълбочен анализ на споразуменията за подизпълнение, особено когато са сключени с трети страни доставчици на услуги в областта на ИКТ, установени в трета държава. На този етап и с оглед на постигането на равновесие между абсолютната необходимост да се запази свободата на договаряне и тази да се гарантира финансова стабилност, определянето на правила за строги тавани и ограничения на експозициите към доставчици трети страна на услуги в областта на ИКТ не се смята за уместно. В контекста на надзорната рамка водещ надзорник, определен съгласно настоящия регламент, следва, по отношение на трети страни критични доставчици на услуги в областта на ИКТ, с голямо внимание да се стреми да придобие пълна представа за мащаба на взаимозависимостите, да установи конкретните случаи, при които е възможно високата концентрация на трети страни критични доставчици на услуги в областта на ИКТ в Съюза да окаже натиск върху стабилността и интегритета на финансовата система на Съюза, и при установяването на такъв специфичен риск да води диалог със съответната трета страна критичен доставчик на услуги в областта на ИКТ.

(68) С цел да се оценява и да се следи редовно способността на трета страна доставчик на услуги в областта на ИКТ да предоставя по сигурен начин услуги на финансов субект без неблагоприятни последици за оперативната устойчивост на цифровите технологии при финансовия субект, някои основни елементи на договорите с трети страни доставчици на услуги в областта на ИКТ следва да бъдат хармонизирани. Подобна хармонизация следва да обхваща минимални елементи, които са от решаващо значение за осигуряването на цялостно наблюдение от страна на финансовия субект на рисковете, които могат да възникнат от трета страна доставчик на услуги в областта на ИКТ, от гледна точка на необходимостта финансовият субект да гарантира устойчивостта на използваните от него цифрови технологии поради сериозната си зависимост от стабилността, функционалността, наличността и сигурността на получаваните услуги в областта на ИКТ.

(69) При предоговарянето на договорни споразумения с цел привеждане в съответствие с изискванията на настоящия регламент финансовите субекти и третите страни доставчици на услуги в областта на ИКТ следва да гарантират, че в тях са включени основните договорни разпоредби, както е предвидено в настоящия регламент.

(70) Освен това определението за „критична или важна функция“, предвидено в настоящия регламент, обхваща „критичните функции“ съгласно определението в член 2, параграф 1, точка 35 от Директива 2014/59/ЕС на Европейския парламент и на Съвета ([20]). Съответно функциите, считани за критични съгласно Директива 2014/59/ЕС, се включват в определението за критични функции по смисъла на настоящия регламент.

(71) Независимо от критичността или важността на функцията, която се поддържа от услугите в областта на ИКТ, договорните споразумения следва по-специално да предвиждат спецификация на подробните описания на функциите и услугите, на местата, където се предоставят такива функции и където трябва да се обработват данните, както и указание за описание на нивото на обслужване. Други особено важни елементи за осигуряването на възможност на финансовия субект да осъществява наблюдение на риска в областта на ИКТ, пораждан от трети страни, са: договорни разпоредби за начина, по който третата страна доставчик на услуги в областта на ИКТ трябва да гарантира достъпността, наличността, цялостността, сигурността и защитата на личните данни; разпоредби, предвиждащи необходимите гаранции, които позволяват достъп, възстановяване на информацията и връщане на данните при несъстоятелност, преструктуриране или прекратяване на дейността на трета страна доставчик на услуги в областта на ИКТ, както и разпоредби, които изискват от третата страна доставчик на услуги в областта на ИКТ да окаже помощ при инциденти с ИКТ, свързани с предоставяните услуги, без допълнителни разходи или на предварително

([20]) Директива 2014/59/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. за създаване на рамка за възстановяване и преструктуриране на кредитни институции и инвестиционни посредници и за изменение на Директива 82/891/ЕИО на Съвета и директиви 2001/24/ЕО, 2002/47/ЕО, 2004/25/ЕО, 2005/56/ЕО, 2007/36/ЕО, 2011/35/ЕС, 2012/30/ЕС и 2013/36/ЕС и на регламенти (ЕС) № 1093/2010 и (ЕС) № 648/2012 на Европейския парламент и на Съвета (ОВ L 173, 12.6.2014 г., стр. 190).

определена цена; разпоредби относно задължението на третата страна доставчик на услуги в областта на ИКТ да оказва пълно съдействие на компетентните органи и органите за преструктуриране на финансовия субект; и разпоредби относно правото на прекратяване на договорните споразумения и свързаните с тях минимални срокове за даване на предизвестие — в съответствие с очакванията на компетентните органи и органите за преструктуриране.

(72) В допълнение на такива договорни разпоредби и с цел да се позволи на финансовите субекти да контролират изцяло всички събития, пораждани от трети страни, които могат да накърнят сигурността на техните системи на ИКТ, договорите за предоставяне на услуги в областта на ИКТ, подпомагащи критични или важни функции, следва също така да съдържат следното: обстойно описание на нивото на обслужване с точни количествени и качествени цели за ефективност, за да може, ако договореното ниво на обслужване стане незадоволително, да бъдат предприети възможно най-бързо подходящите корективни мерки; съответните срокове и задължения за докладване, с които е обвързана третата страна доставчик на услуги в областта на ИКТ в случай на събития, които потенциално могат съществено да засегнат способността ѝ ефективно да предоставя съответните услуги в областта на ИКТ; изискване към третата страна доставчик на услуги в областта на ИКТ да прилага и тества планове за действие при извънредни ситуации и да разполага с мерки, инструменти и политики за сигурност на ИКТ, които дават възможност за сигурно предоставяне на услуги, както и да участва и пълноценно да сътрудничи при тестването за проникване, извършвано от финансовия субект.

(73) Договорите за предоставяне на услуги в областта на ИКТ, подпомагащи критични или важни функции следва да съдържат и разпоредби, даващи възможност да се упражнят правата на достъп, проверка и одит от страна на финансовия субект или от определена трета страна, както и правото на копиране, като инструменти от решаващо значение за текущото наблюдение от страна на финансовите субекти на ефективността на този доставчик, заедно с пълното сътрудничество на доставчика на услуги по време на проверките. Компетентният орган на финансовия субект би следвало също да има правото на проверка и одит на третата страна доставчик на услуги в областта на ИКТ, при съответното уведомяване на този доставчик и защита на поверителната информация.

(74) В такива договорни споразумения следва да бъдат предвидени и специални изходни стратегии, за да могат да бъдат определени по-конкретно задължителни преходни периоди, по време на които третите страни доставчици на услуги в областта на ИКТ следва да продължат да предоставят съответните услуги, така че да се ограничи рискът от смущения за финансовия субект, или реално да му се позволи да започне да използва услугите на други такива доставчици, или, като алтернативен вариант, да премине към собствени разработени решения — в зависимост от степента на сложност на предоставяната услуга в областта на ИКТ. Освен това финансовите субекти, попадащи в обхвата на Директива 2014/59/ЕС, следва да гарантират, че съответните договори за услуги в областта на ИКТ са надеждни и напълно изпълними в случай на преструктуриране на тези финансови субекти. Следователно в съответствие с очакванията на органите за преструктуриране тези финансови субекти следва да гарантират, че съответните договори за услуги в областта на ИКТ са устойчиви в случай на преструктуриране. Докато продължават да изпълняват задълженията си за плащане, тези финансови субекти следва да гарантират, наред с други изисквания, че съответните договори за услуги в областта на ИКТ съдържат клаузи, с които не се допуска прекратяване, спиране и модифициране въз основа на реорганизация или преструктуриране.

(75) Освен това доброволното използване на стандартните договорни клаузи, разработени от публични органи или институции на Съюза, по-специално използването на договорни клаузи, разработени от Комисията за компютърните услуги „в облак“, може допълнително да успокои финансовите субекти и третите страни доставчици на услуги в областта на ИКТ, тъй като ще се повиши правната сигурност относно използването във финансовия сектор на компютърни услуги „в облак“ при пълно съобразяване с изискванията и очакванията, предвидени в законодателството на Съюза за финансовите услуги. Разработването на стандартни договорни клаузи 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, които да могат да бъдат използвани от финансовите субекти за възлагане на компютърни услуги „в облак“ на външни доставчици, и почива на работата на заинтересованите страни от редица сектори в областта на тези услуги, която Комисията подпомогна, като улесни участието на финансовия сектор.

(76) С цел да се насърчи сближаването на надзорните подходи за справяне с пораждания от трети страни риск в областта на ИКТ във финансовия сектор и да се повиши ефикасността на тези подходи, както и да се засили оперативната устойчивост на цифровите технологии при финансовите субекти, които за предоставянето на услуги в областта на ИКТ, подпомагащи предоставянето на финансови услуги, разчитат на трети страни критични доставчици на услуги в областта на ИКТ, и оттам — да се допринесе за съхраняването на стабилността на финансовата система на Съюза и за целостта на вътрешния пазар на финансови услуги, за третите страни критични доставчици на услуги в областта на ИКТ следва да се прилага надзорна рамка на равнището на Съюза. Въпреки че създаването на надзорната рамка е оправдано от добавената стойност от предприемането на действия на равнището на Съюза и поради присъщата роля

и особености на използването на услуги в областта на ИКТ при предоставянето на финансови услуги, следва същевременно да се припомни, че това решение изглежда подходящо само в контекста на настоящия регламент, който урежда конкретно оперативната устойчивост на цифровите технологии във финансовия сектор. Тази надзорна рамка обаче не следва да се разглежда като нов модел за надзор от страна на Съюза в областта на финансовите услуги и дейности.

(77) Надзорната рамка следва да се прилага само за трети страни критични доставчици на услуги в областта на ИКТ. Поради това следва да има механизъм за определянето им, така че да се вземат под внимание измерението и естеството на зависимостта на финансовия сектор от тях. Този механизъм следва да включва набор от количествени и качествени критерии, които ще поставят определящите критичния характер параметри като основа за включване в надзорната рамка. За да се гарантира точността на тази оценка и независимо от корпоративната структура на третата страна доставчик на услуги в областта на ИКТ, в случай на трета страна доставчик на услуги в областта на ИКТ, която е част от по-голяма група, тези критерии следва да отчитат цялата структура на групата на третата страна доставчик на услуги в областта на ИКТ. От друга страна третите страни критични доставчици на услуги в областта на ИКТ, които не са автоматично определени в резултат на прилагането на горепосочените критерии, следва да могат да се включат към надзорната рамка на доброволен принцип, като съответно от нея бъдат изключени трети страни доставчици на услуги в областта на ИКТ, които вече са обект на надзорните механизми, подпомагащи изпълнението на задачите на Европейската система на централните банки, посочени в член 127, параграф 2 от ДФЕС.

(78) По подобен начин финансовите субекти, които предоставят услуги в областта на ИКТ на други финансови субекти, макар и да принадлежат към категорията трети страни доставчици на услуги в областта на ИКТ съгласно настоящия регламент, също следва да бъдат изключени от надзорната рамка, тъй като вече са обект на надзорните механизми, установени в съответното законодателство на Съюза за финансовите услуги. Когато е приложимо, в контекста на надзорните си дейности компетентните органи следва да вземат предвид риска за финансовите субекти, свързан с ИКТ, произтичащ от финансови субекти, които предоставят услуги в областта на ИКТ. По същия начин, поради съществуващите механизми за наблюдение на риска на равнище група, третите страни доставчици на услуги в областта на ИКТ, които предоставят услуги предимно на субектите от собствената си група, също следва да бъдат изключени от надзорната рамка. Третите страни доставчици на услуги в областта на ИКТ, които предоставят услуги в областта на ИКТ само в една държава членка на финансови субекти, извършващи дейност само в тази държава членка, също следва да бъдат изключени от механизма за определяне поради ограничената си дейност и липсата на трансгранично въздействие.

(79) Цифровият преход при финансовите услуги доведе до безпрецедентно равнище на използване и осланяне на услугите в областта на ИКТ. Тъй като стана немислимо предоставянето на финансови услуги без използването на компютърни услуги „в облак“, софтуерни решения и услуги, свързани с данни, финансовата екосистема на Съюза стана неразривно свързана и зависима от определени услуги в областта на ИКТ, предоставяни от доставчици на услуги в областта на ИКТ. Някои от тези доставчици — новатори в разработването и прилагането на технологии, основани на ИКТ — играят съществена роля в предоставянето на финансови услуги или са станали неразривна част от веригата за създаване на стойност в областта на финансовите услуги. По този начин те се превърнаха в елементи от критично значение за стабилността и целостта на финансовата система на Съюза. Това широко разпространено осланяне на услуги, предоставяни от трети страни критични доставчици на услуги в областта на ИКТ, съчетано с взаимозависимостта на информационните системи на различните пазарни участници, създава пряк и потенциално сериозен риск за системата на финансови услуги в Съюза и за непрекъснатостта на предоставянето на финансови услуги, ако трети страни критични доставчици на услуги в областта на ИКТ бъдат засегнати от оперативни смущения или съществени киберинциденти. Киберинцидентите имат отличителната способност да се мултиплицират и разпространяват в цялата финансова система значително по-бързо, отколкото други видове рискове, наблюдавани във финансовия сектор, и могат да се разпростират сред секторите и отвъд географските граници. Те имат потенциала да прераснат в системна криза, при която доверието във финансовата система би било подкопано поради смущения във функциите, подпомагащи реалната икономика, или поради значителни финансови загуби, като достигнат до равнище, което финансовата система не е в състояние да понесе или което изисква прилагането на сериозни мерки за поемане на сътресения. За да се предотврати реализирането на такива сценарии, като по този начин се застраши финансовата стабилност и цялост на Съюза, от съществено значение е да се осигури сближаване на надзорните практики, свързани с пораждания от трети страни риск в областта на ИКТ в областта на финансите, по-специално чрез нови правила, позволяващи надзор от страна на Съюза върху третите страни критични доставчици на услуги в областта на ИКТ.

(80) Надзорната рамка до голяма степен зависи от степента на сътрудничество между водещия надзорник и третата страна критичен доставчик на услуги в областта на ИКТ, която предоставя на финансовите субекти услуги, засягащи предоставянето на финансови услуги. Успешният надзор се основава, наред с другото, на способността на водещия надзорник ефективно да провежда мисии за наблюдение и проверки, за да оценява правилата, механизмите за контрол и процесите, използвани от третите страни критични доставчици на услуги в областта на ИКТ, както и да оценява потенциалното кумулативно въздействие на техните дейности върху финансовата стабилност и целостта на финансовата система. В същото време е от решаващо значение третите страни критични доставчици на услуги в областта на ИКТ да следват препоръките на водещия надзорник и да преодоляват установените от него проблеми. Тъй като липсата на сътрудничество от трета страна критичен доставчик на услуги в областта на ИКТ, която предоставя услуги, засягащи предоставянето на финансови услуги — като например отказ да даде достъп до своите помещения или да предостави информация — в крайна сметка би лишил водещия надзорник от основните му инструменти за оценка на риска в областта на ИКТ, пораждан от трети страни, и би могъл да окаже неблагоприятно въздействие върху финансовата стабилност и целостта на финансовата система, е необходимо да се предвиди също така подходящ режим на санкции.

(81) В този контекст необходимостта водещият надзорник да налага наказателни плащания, за да принуди критичните доставчици трета страна на услуги в областта на ИКТ да спазват предвидените в настоящия регламент задължения за прозрачност и достъп, не следва да бъде застрашена от трудности, породени от принудителното изпълнение на тези наказателни плащания по отношение на установени в трети държави трети страни критични доставчици на услуги в областта на ИКТ. С цел да се осигури изпълнимостта на тези санкции и да се даде възможност за бързо въвеждане на процедури, с които да се гарантира правото на защита на третите страни критични доставчици на услуги в областта на ИКТ в контекста на механизма за определяне и на издаването на препоръки, от тези трети страни критични доставчици на услуги в областта на ИКТ, които предоставят на финансовите субекти услуги, засягащи предоставянето на финансови услуги, следва да се изисква да поддържат адекватно търговско присъствие в Съюза. Поради естеството на надзора и липсата на сравними договорености в други юрисдикции не съществуват подходящи алтернативни механизми за постигането на тази цел чрез ефективно сътрудничество с финансовите надзорни органи в трети държави във връзка с наблюдението на въздействието на операционните рискове при цифровите технологии, пораждани от системните трети страни доставчици на услуги в областта на ИКТ, определени като установени в трети държави трети страни критични доставчици на услуги в областта на ИКТ. Поради това, за да продължи да предоставя услуги в областта на ИКТ на финансови субекти в Съюза, установена в трета държава трета страна доставчик на услуги в областта на ИКТ, която в съответствие с настоящия регламент е определена като критичен доставчик, в срок от 12 месеца след определянето му като такъв следва да предприеме всички необходими мерки, за да гарантира учредяването си в Съюза, посредством създаването на дъщерно дружество, както е определено в достиженията на правото на Съюза, а именно в Директива 2013/34/ЕС на Европейския парламент и на Съвета ([21]).

(82) Изискването за създаване на дъщерно дружество в Съюза не следва да възпрепятства третата страна критичен доставчик на услуги в областта на ИКТ да предоставя услуги в областта на ИКТ и свързаната с тях техническа поддръжка от съоръжения и инфраструктура, разположени извън Съюза. Настоящият регламент не налага задължение за локализиране на данните, тъй като не изисква съхраняването или обработването на данни да се извършва в Съюза.

(83) Третите страни критични доставчици на услуги в областта на ИКТ следва да могат да предоставят услуги в областта на ИКТ от всяко място по света, не непременно или не само от помещения, намиращи се в Съюза. Надзорните дейности следва да се извършват първо в помещенията, разположени в Съюза, и чрез взаимодействие със субекти, намиращи се в Съюза, включително дъщерните дружества, създадени от третите страни критични доставчици на услуги в областта на ИКТ съгласно настоящия регламент. Такива действия в рамките на Съюза обаче може да се окажат недостатъчни, за да може водещият надзорник да изпълнява пълноценно и ефективно задълженията си съгласно настоящия регламент. Ето защо водещият надзорник следва също така да може да упражнява съответните си надзорни правомощия в трети държави. Упражняването на тези правомощия в трети държави следва да позволява на водещия надзорник да проверява съоръженията, от които услугите в областта на ИКТ или услугите за техническа поддръжка действително се предоставят или управляват от третата страна критичен доставчик на услуги в областта на ИКТ, и следва да предоставя на водещия надзорник цялостно и оперативно разбиране за управлението на риска в областта на ИКТ от третата страна критичен доставчик на услуги в областта на ИКТ. Възможността водещият надзорник, в качеството си на агенция на Съюза, да упражнява правомощия извън територията на Съюза следва да бъде надлежно уредена от съответните условия, по-специално съгласието на съответната трета страна критичен доставчик на услуги в областта на ИКТ. По подобен начин съответните органи на третата държава следва да бъдат информирани за дейностите на водещия надзорник на тяхната територия и да не са възразили срещу изпълнението им. За да се гарантира обаче ефикасност на прилагането и без да се засягат съответните области на компетентност на институциите на Съюза и на

([21]) Директива 2013/34/ЕС на Европейския парламент и на Съвета от 26 юни 2013 г. относно годишните финансови отчети, консолидираните финансови отчети и свързаните доклади на някои видове предприятия и за изменение на Директива 2006/43/ЕО на Европейския парламент и на Съвета и за отмяна на директиви 78/660/ЕИО и 83/349/ЕИО на Съвета (ОВ L 182, 29.6.2013 г., стр. 19).

държавите членки, тези правомощия трябва също така да бъдат изцяло заложени в сключени споразумения за административно сътрудничество със съответните органи на съответната трета държава. Поради това настоящият регламент следва да позволи на ЕНО да сключват споразумения за административно сътрудничество със съответните органи на трети държави, които по друг начин не следва да създават правни задължения по отношение на Съюза и неговите държави членки.

(84) С цел да се улесни комуникацията с водещия надзорник и да се осигури подходящо представителство, третите страни критични доставчици на услуги в областта на ИКТ, които са част от група, следва да определят едно юридическо лице за свое координационно звено.

(85) Надзорната рамка не следва да засяга компетентността на държавите членки да провеждат собствени надзорни мисии или мисии за наблюдение на третите страни доставчици на услуги в областта на ИКТ, които не са определени като критични съгласно настоящия регламент, но които биха могли да се смятат за важни в национален аспект.

(86) За да се използва многопластовата 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 в областта на ИКТ. Той следва да бъде подкрепен от нов подкомитет (Надзорният форум), който да извършва подготвителната работа както за целите на решенията, касаещи отделни трети страни критични доставчици на услуги в областта на ИКТ, така и за издаването на препоръките, отправяни към всички такива доставчици, по-специално във връзка със сравнителния анализ на програмите за надзор на третите страни критични доставчици на услуги в областта на ИКТ и с определянето на най-добрите практики с оглед на рисковете от концентрация на такива доставчици.

(87) С цел да се гарантира, че третите страни критични доставчици на услуги в областта на ИКТ са обект на подходящ и ефективен надзор на равнището на Съюза, в настоящия регламент се предвижда, че всеки от трите ЕНО може да бъде определен за водещ надзорник. Индивидуалното разпределяне на всяка трета страна критичен доставчик на услуги в областта на ИКТ към един от трите ЕНО следва да бъде резултат от оценка на това дали финансовите субекти, извършващи дейност във финансовите сектори, за които отговаря съответният ЕНО, са преобладаващи. Този подход следва да доведе до балансирано разпределение на задачите и отговорностите между трите ЕНО в контекста на упражняването на надзорните функции и следва да доведе до използване по най-добрия начин на човешките ресурси и техническия експертен опит, налични във всеки от трите ЕНО.

(88) На водещите надзорници следва да бъдат предоставени необходимите правомощия за провеждане на разследвания, извършване на проверки на място и от разстояние в помещенията и местата на третите страни критични доставчици на услуги в областта на ИКТ и получаване на пълна и актуална информация. Тези правомощия следва да позволят на водещия надзорник да има реална представа за вида, мащаба и въздействието на риска в областта на ИКТ, пораждан от трети страни, за финансовите субекти и в общ план — за финансовата система на Съюза. Възлагането на ЕНО на водещата роля по надзор е предпоставка за разбирането и анализирането на системното измерение на риска в областта на ИКТ във финансовия сектор. Въздействието на третите страни критични доставчици на услуги в областта на ИКТ върху финансовия сектор в Съюза и потенциалните проблеми, породени от риска от концентрация на такива доставчици, налагат общ подход на равнището на Съюза. Едновременното извършване на множество одити и правата за достъп, упражнявани поотделно от множество компетентни органи, работещи малко или повече изолирано един от друг, възпрепятстват органите за финансов надзор да извършат обстойното и цялостно проучване в Съюза на риска в областта на ИКТ, пораждан от трети страни, а и същевременно създават дублирания, тежест и сложност за третите страни критични доставчици на услуги в областта на ИКТ, ако бъдат обект на многобройни искания за наблюдение и проверки.

(89) Поради това, че определянето им като критични, им оказва значително въздействие, настоящият регламент следва да гарантира, че правата на третите страни критични доставчици на услуги в областта на ИКТ се спазват през целия период на изпълнение на надзорната рамка. Преди да бъдат определени като критични, такива доставчици следва например да имат правото да представят на водещия надзорник мотивирано становище, съдържащо всяка информация от значение за целите на оценката, свързана с тяхното определяне. Тъй като на водещия надзорник следва да бъде предоставено правомощието да отправя препоръки относно рисковете в областта на ИКТ и подходящите защитни средства, включително правомощието да се противопоставя на определени договорни споразумения, което като краен резултат влияе върху стабилността на финансовия субект или на финансовата система, на третите страни критични доставчици на услуги в областта на ИКТ следва също така да бъде дадена възможност, преди финализирането на тези препоръки, да предоставят обяснения относно очакваното въздействие на предвидените в препоръките решения върху клиентите, които са субекти извън обхвата на настоящия регламент, и да

формулират решения за намаляване на рисковете. Третите страни критични доставчици на услуги в областта на ИКТ, които не са съгласни с препоръките, следва да представят аргументирано обяснение за намерението си да не одобрят препоръката. Когато такова аргументирано обяснение не е представено или се смята за недостатъчно, водещият надзорник следва да публикува известие, в което се описва накратко въпросът за неспазването.

(90) Компетентните органи следва надлежно да включват задачата за проверка на спазването по същество на препоръките, издадени от водещия надзорник, сред своите функции във връзка с пруденциалния надзор върху финансовите субекти. Компетентните органи следва да могат да изискват от финансовите субекти да предприемат допълнителни мерки за справяне с рисковете, установени в препоръките на водещия надзорник, и следва своевременно да изпращат уведомления за това. Когато водещият надзорник отправя препоръки към третите страни критични доставчици на услуги в областта на ИКТ, подлежащи на надзор съгласно Директива (ЕС) 2022/2555, компетентните органи следва да могат доброволно, и преди да приемат допълнителни мерки, да се консултират с компетентните органи съгласно посочената директива, за да се насърчи координиран подход по отношение на въпросните трети страни критични доставчици на услуги в областта на ИКТ.

(91) Упражняването на надзор следва да се ръководи от три оперативни принципа, които имат за цел да гарантират: а) тясна координация на ЕНО в ролята им на водещ надзорник чрез съвместна мрежа за надзор (СМН), б) съгласуваност с рамката, установена с Директива (ЕС) 2022/2555 (чрез доброволни консултации с органите съгласно посочената директива, за да се избегне дублирането на мерки, насочени към третите страни критични доставчици на услуги в областта на ИКТ), и в) полагане на грижа за свеждане до минимум на потенциалния риск от смущения в услугите, предоставяни от третите страни критични доставчици на услуги в областта на ИКТ на клиенти, които са субекти извън обхвата на настоящия регламент.

(92) Надзорната рамка не следва да заменя, нито по някакъв начин или за някакви части да премахва изискването за управление от самите финансови субекти на рисковете, породени от използването на трети страни доставчици на услуги в областта на ИКТ, включително задължението за поддържане на текущо наблюдение на сключените договорни споразумения с трети страни критични доставчици на услуги в областта на ИКТ. По подобен начин надзорната рамка не следва да засяга пълната отговорност, която финансовите субекти носят за спазването на всички правни задължения, предвидени в настоящия регламент и в съответното законодателство за финансовите услуги.

(93) С цел да се избегнат дублиранията и припокриванията компетентните органи следва да не предприемат индивидуални мерки за наблюдаване на риска при третите страни критични доставчици на услуги в областта на ИКТ и в това отношение следва да разчитат на съответната оценка на водещия надзорник. Всички мерки следва при всички случаи да бъдат предварително съгласувани и одобрени от водещия надзорник в контекста на изпълнението на задачите от надзорната рамка.

(94) С цел да се насърчи сближаването в международен план на най-добрите практики, които да се използват при прегледа и наблюдението на начина, по който третите страни доставчици 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 на трети държави.

(95) С цел да се използват специфичните компетенции, техническите умения и опит на персонала със специализация в областта на операционния риск и риска в областта на ИКТ, натрупани в рамките на компетентните органи, трите ЕНО и, на доброволен принцип, компетентните по силата на Директива (ЕС) 2022/2555 органи водещият надзорник следва да използва националния надзорен капацитет и знания и да създаде специални анализаторски екипи за всяко трета страна критичен доставчик на услуги в областта на ИКТ, като приобщи екипи от различни области за подпомагане на подготовката и изпълнението на надзорните дейности, включително общи разследвания и проверки на третите страни критични доставчици на услуги в областта на ИКТ, както и всички необходими последващи действия.

(96) Разходите, произтичащи от надзорните задачи, ще бъдат изцяло финансирани от таксите, събирани от третите страни критични доставчици на услуги в областта на ИКТ, но преди надзорната рамка да започне да се прилага, ЕНО вероятно ще имат разходи за въвеждането на специални системи на ИКТ в подкрепа на предстоящия надзор, тъй като тези системи ще трябва да бъдат разработени и внедрени преди това. Поради това настоящият регламент предвижда хибриден модел на финансиране, при който надзорната рамка като такава ще се финансира изцяло от такси, а разработването на системите на ИКТ на ЕНО ще се финансира от вноските на Съюза и на националните компетентни органи.

(97) Компетентните органи следва да разполагат с всички необходими правомощия за надзор, разследване и санкциониране с оглед на надлежното изпълнение на задълженията си съгласно настоящия регламент. По принцип те следва да публикуват уведомления за административните санкции, които налагат. Финансовите субекти и третите страни доставчици на услуги в областта на ИКТ могат да бъдат установени в различни държави членки и да подлежат на надзор от различни компетентни органи, поради което прилагането на настоящия регламент следва да бъде улеснено, от една страна, чрез тясно сътрудничество между съответните компетентни органи, включително с ЕЦБ по отношение на възложените ѝ специфични задачи от Регламент (ЕС) № 1024/2013 на Съвета, и, от друга страна, чрез консултации с ЕНО посредством взаимен обмен на сведения и взаимопомощ при съответните надзорни действия.

(98) С цел да се извърши допълнително количествено и качествено уточняване на критериите за определяне на третите страни доставчици на услуги в областта на ИКТ като критични и да се хармонизират таксите за упражняването на надзор, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 от ДФЕС, за допълване на настоящия регламент, като бъдат доуточнени: системното въздействие, което отказ на системите или оперативна неизправност при трета страна доставчик на услуги в областта на ИКТ може да има върху финансовите субекти, на които тя предоставя услуги в областта на ИКТ; броят на глобалните системно значими институции (Г-СЗИ) или другите системно значими институции (Д-СЗИ), които се осланят на въпросната трета страна доставчик на услуги в областта на ИКТ; броят на третите страни доставчици на услуги в областта на ИКТ, които осъществяват дейност на даден пазар; разходите за прехвърляне на данните и работното натоварване, свързано с ИКТ към други трети страни доставчици на услуги в областта на ИКТ; както и размерът на таксите за упражняване на надзор и начинът на плащането им. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище, и тези консултации да бъдат проведени в съответствие с принципите, заложени в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество ([22]). По-специално, с цел осигуряване на равно участие при подготовката на делегираните актове, Европейският парламент и Съветът следва да получават всички документи едновременно с експертите от държавите членки, като техните експерти следва да получават систематично достъп до заседанията на експертните групи на Комисията, занимаващи се с подготовката на делегираните актове.

(99) Регулаторните технически 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 в областта на ИКТ, докладването за съществен инцидент с ИКТ, тестването, свързано с такъв инцидент, както и във връзка с базовите изисквания за надеждно наблюдаване на риска в областта на ИКТ, пораждан от трети страни. Комисията и ЕНО следва да съобразят прилагането на тези стандарти и изисквания с размера и цялостния рисков профил на финансовите субекти и с естеството, мащаба и сложността на техните услуги, дейности и операции. На Комисията следва да бъде предоставено правомощието да приема тези регулаторни технически стандарти чрез делегирани актове съгласно член 290 от ДФЕС и в съответствие с членове 10—14 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

(100) С цел да се улесни сравнимостта на докладването за съществени инциденти с ИКТ и съществени операционни или свързани със сигурността инциденти, свързани с плащания, както и да се осигури прозрачност на договорните споразумения за услуги в областта на ИКТ, предоставяни от трета страна доставчик на такива услуги, на ЕНО следва да бъде възложено да разработят проекти на технически стандарти за изпълнение, с които да се установят стандартизирани образци, формуляри и процедури, които финансовите субекти да използват за докладване за съществени инциденти с ИКТ и съществени операционни или свързани със сигурността инциденти, свързани с плащания, както и стандартизирани образци за информационния регистър. При разработването на тези стандарти ЕНО следва да вземат предвид размера и цялостния рисков профил на финансовите субекти и естеството, мащаба и сложността на техните услуги, дейности и операции. На Комисията следва да бъде предоставено правомощието да приема тези технически стандарти за изпълнение чрез актове за изпълнение съгласно член 291 от ДФЕС и в съответствие с член 15 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

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

(101) Тъй като допълнителните изисквания вече са определени в делегираните актове и актовете за изпълнение въз основа на техническите регулаторни стандарти и техническите стандарти за изпълнение, предвидени в регламенти (ЕО) № 1060/2009 ([23]), (ЕС) № 648/2012 ([24]), (ЕС) № 600/2014 ([25]) и (ЕС) № 909/2014 ([26]) на Европейския парламент и на Съвета, на ЕНО е целесъобразно да се възложи, индивидуално или съвместно в рамките на 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 в областта на ИКТ.

(102) С настоящия регламент и с Директива (ЕС) 2022/2556 на Европейския парламент и на Съвета ([27]) се консолидират разпоредбите относно управлението на риска в областта на ИКТ в множество регламенти и директиви от достиженията на правото на Съюза в областта на финансовите услуги, включително регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и Регламент (ЕС) 2016/1011 ([28]) на Европейския парламент и на Съвета, поради което с цел осигуряване на пълна съгласуваност посочените регламенти следва да бъдат изменени, за да се поясни, че приложимите разпоредби относно риска в областта на ИКТ се съдържат в настоящия регламент.

(103) Поради това обхватът на съответните членове, свързани с операционния риск, въз основа на които правомощията, предвидени в регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011, обусловиха приемането на делегирани актове и актове за изпълнение, следва да бъде стеснен с оглед на включването в настоящия регламент на всички разпоредби, обхващащи аспектите на оперативната устойчивост на цифровите технологии, които понастоящем са част от посочените регламенти.

(104) Потенциалният системен киберриск, свързан с използването на инфраструктури на ИКТ, които позволяват функционирането на платежните системи и предоставянето на дейности по обработване на плащания, следва да бъде надлежно разгледан на равнището на Съюза чрез хармонизирани правила за устойчивост на цифровите технологии. За тази цел Комисията следва бързо да оцени необходимостта от преразглеждане на обхвата на настоящия регламент, като същевременно приведе този преглед в съответствие с резултатите от цялостния преглед, предвиден съгласно Директива (ЕС) 2015/2366. Многобройните широкомащабни атаки през последното десетилетие показват как платежните системи са изложени на риск от киберзаплахи. Поради това, че се намират в центъра на веригата от платежни услуги и имат силни взаимовръзки с финансовата система като цяло, платежните системи и дейностите по обработка на плащания придобиха критично значение за функционирането на финансовите пазари в Съюза. Кибератаките срещу такива системи могат да причинят сериозни оперативни смущения в дейността с пряко отражение върху ключови икономически функции, като например улесняване на плащанията, и непреки последици за свързаните икономически процеси. До въвеждането на равнището на Съюза на хармонизиран режим и надзор на операторите на платежни системи и обработващите субекти, при прилагането на правила за операторите на платежни системи и обработващите субекти, които подлежат на надзор в собствената им юрисдикция, държавите членки могат, с оглед на прилагането на сходни пазарни практики, да черпят вдъхновение от изискванията за оперативна устойчивост на цифровите технологии, определени в настоящия регламент.

([23]) Регламент (ЕО) № 1060/2009 на Европейския парламент и на Съвета от 16 септември 2009 г. относно агенциите за кредитен рейтинг (ОВ L 302, 17.11.2009 г., стр. 1).

([24]) Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ L 201, 27.7.2012 г., стр. 1).

([25]) Регламент (ЕС) № 600/2014 на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 173, 12.6.2014 г., стр. 84).

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

([27]) Директива (ЕС) 2022/2556 на Европейския парламент и на Съвета от 14 декември 2022 г. за изменение на директиви 2009/65/ЕО, 2009/138/ЕО, 2011/61/ЕС, 2013/36/ЕС, 2014/59/ЕС, 2014/65/ЕС, (ЕС) 2015/2366 и (ЕС) 2016/2341 по отношение на оперативната устойчивост на цифровите технологии във финансовия сектор (вж. страница 153 от настоящия брой на Официален вестник).

([28]) 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).

(105) Доколкото целта на настоящия регламент — постигане на значителна оперативна устойчивост на цифровите технологии при поднадзорните финансови субекти — не може да бъде постигната в достатъчна степен от държавите членки, тъй като налага да се хармонизират множество разнородни правила в правото на Съюза и в националното право, 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.

(106) В съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([29]) беше проведена консултация с Европейския надзорен орган по защита на данните, който прие становище на 10 май 2021 г. ([30]),

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

Общи разпоредби

Член 1

Предмет

1. За да се постигне високо общо равнище на оперативна устойчивост на цифровите технологии, с настоящия регламент се установяват единни изисквания за сигурността на мрежовите и информационните системи, които поддържат работните процеси на финансовите субекти, както следва:

а) изисквания към финансовите субекти във връзка с:

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

   ii) докладването пред компетентните органи за съществени инциденти с ИКТ и уведомяването им на доброволни начала за значителни киберзаплахи;

   iii) докладването пред компетентните органи за съществени операционни или свързани със сигурността инциденти, свързани с плащания, от страна на финансовите субекти, посочени в член 2, параграф 1, букви а)—г);

   iv) тестването на оперативната устойчивост на цифровите технологии;

   v) обмена на информация и разузнавателни сведения за киберзаплахите и уязвимите места;

   vi) мерките за стабилното управление на риска в областта на ИКТ, пораждан от трети страни;

б) изисквания във връзка с договорните споразумения, сключвани между третите страни доставчици на услуги в областта на ИКТ и финансовите субекти;

в) правила за създаването и изпълнението на надзорната рамка за третите страни критични доставчици на услуги в областта на ИКТ при предоставянето на услуги на финансовите субекти;

г) правила 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 съществени или важни субекти съгласно националните разпоредби, с които се транспонира член 3 от Директива (ЕС) 2022/2555, настоящият регламент се смята, за целите на член 4 от посочената директива, за специфичен за сектора правен акт на Съюза.

3. Настоящият регламент не засяга отговорността на държавите членки по отношение на основните държавни функции, свързани с обществената сигурност, отбраната и националната сигурност в съответствие с правото на Съюза.

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

([30]) ОВ C 229, 15.6.2021 г., стр. 16.

Член 2

Обхват

1. Без да се засягат параграфи 3 и 4, настоящият регламент се прилага за следните субекти:

а) кредитни институции;

б) платежни институции, включително платежни институции, освободени съгласно Директива (ЕС) 2015/2366;

в) доставчици на услуги по предоставяне на информация за сметка;

г) институции за електронни пари, включително институции за електронни пари, освободени съгласно Директива 2009/110/ЕО;

д) инвестиционни посредници;

е) доставчици на услуги за криптоактиви, лицензирани съгласно Регламента на Европейския парламент и на Съвета относно пазарите на криптоактиви и за изменение на регламенти (ЕС) № 1093/2010 и (ЕС) № 1095/2010 и на директиви 2013/36/ЕС и (ЕС) 2019/1937 (наричан по-нататък „Регламентът относно пазарите на криптоактиви“), и емитенти на токени, обезпечени с активи;

ж) централни депозитари на ценни книжа;

з) централни контрагенти;

и) места на търговия;

й) регистри на трансакции;

к) лица, управляващи алтернативни инвестиционни фондове;

л) управляващи дружества;

м) доставчици на услуги за докладване на данни;

н) застрахователни и презастрахователни предприятия;

о) застрахователни посредници, презастрахователни посредници и посредници, предлагащи застрахователни продукти като допълнителна дейност;

п) институции за професионално пенсионно осигуряване;

р) агенции за кредитен рейтинг;

с) администратори на критични бенчмаркове;

т) доставчици на услуги за колективно финансиране;

у) регистри на секюритизации;

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

2. За целите на настоящия регламент субектите, посочени в параграф 1, букви а) — у) се наричат общо „финансови субекти“.

3. Настоящият регламент не се прилага за:

а) лицата, управляващи алтернативни инвестиционни фондове, посочени в член 3, параграф 2 от Директива 2011/61/ЕС;

б) застрахователните и презастрахователните предприятия, посочени в член 4 от Директива 2009/138/ЕО;

в) институциите за професионално пенсионно осигуряване, които управляват пенсионни схеми, в които участват общо не повече от 15 членове;

г) физическите или юридическите лица, освободени съгласно членове 2 и 3 от Директива 2014/65/ЕС;

д) застрахователните посредници, презастрахователните посредници и посредниците, предлагащи застрахователни продукти като допълнителна дейност, които са микро-, малки или средни предприятия;

е) пощенските джиро институции, посочени в член 2, параграф 5, точка 3 от Директива 2013/36/ЕС.

4. Държавите членки могат да изключат от обхвата на настоящия регламент субектите, посочени в член 2, параграф 5, точки 4—23 от Директива 2013/36/ЕС, които се намират на тяхна територия. Когато държава членка се възползва от тази възможност, тя информира Комисията за това, както и за всякакви последващи промени във връзка с това. Комисията прави тази информация обществено достояние на своя уебсайт или чрез други лесно достъпни средства.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „оперативна устойчивост на цифровите технологии“ означава способността на финансов субект да изгражда, осигурява и преглежда своята оперативна цялост и надеждност, като осигурява пряко или непряко — чрез ползване на услуги, предоставяни от трети страни доставчици на услуги в областта на ИКТ, пълния набор от свързан с ИКТ капацитет, необходим за сигурността на използваните от него мрежови и информационни системи, и който поддържа непрекъснатото предоставяне на финансови услуги и тяхното качество, включително при смущения;

2) „мрежова и информационна система“ означава мрежова и информационна система съгласно определението в член 6, точка 1 от Директива (ЕС) 2022/2555;

3) „наследена система на ИКТ“ означава система на ИКТ, която е достигнала края на жизнения си цикъл, която не е подходяща за модернизиране или поправка поради технологични или търговски причини или вече не се поддържа от своя доставчик или от трета страна доставчик на услуги в областта на ИКТ, но която все още се използва и поддържа функциите на финансовия субект;

4) „сигурност на мрежовите и информационните системи“ означава сигурност на мрежовите и информационните системи съгласно определението в член 6, точка 2 от Директива (ЕС) 2022/2555;

5) „риск в областта на ИКТ“ означава всяко установимо при обичайни условия обстоятелство във връзка с използването на мрежови и информационни системи, което, ако се реализира, може да застраши сигурността на мрежовите и информационните системи, на зависим от технологиите инструмент или процес, на операциите или процесите, или на предоставянето на услуги, като предизвика неблагоприятни последици в цифровата или физическата среда;

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

7) „актив на ИКТ“ означава софтуерен или хардуерен актив в мрежовите и информационните системи, използвани от финансовия субект;

8) „инцидент с ИКТ“ означава единично събитие или поредица от свързани събития, които не са планирани от финансовия субект, застрашават сигурността на мрежовите и информационните системи и имат неблагоприятно въздействие върху наличността, автентичността, цялостността или поверителността на данните, или върху предоставяните от финансовия субект услуги;

9) „операционен или свързан със сигурността инцидент, свързан с плащания“ означава единично събитие или поредица от свързани събития, които не са планирани от финансовите субекти, посочени в член 2, параграф 1, букви а)—г), независимо дали са свързани с ИКТ или не, и имат неблагоприятно въздействие върху наличността, автентичността, цялостността или поверителността на свързаните с плащания данни, или върху свързаните с плащания услуги, предоставяни от финансовия субект;

10) „съществен инцидент с ИКТ“ означава инцидент с ИКТ, който има силно неблагоприятно въздействие върху мрежовите и информационните системи, поддържащи критични или важни функции на финансовия субект;

11) „съществен операционен или свързан със сигурността инцидент, свързан с плащания“ означава операционен или свързан със сигурността инцидент, свързан с плащания, който има силно неблагоприятно въздействие върху предоставяните услуги, свързани с плащания;

12) „киберзаплаха“ означава киберзаплаха съгласно определението в член 2, точка 8 от Регламент (ЕС) 2019/881;

13) „значителна киберзаплаха“ означава киберзаплаха, чиито технически характеристики показват, че би могла да доведе до съществен инцидент с ИКТ или до съществен операционен или свързан със сигурността инцидент, свързан с плащания;

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

15) „разузнавателни сведения за заплахи“ означава информация, която е обобщена, обработена, анализирана, разтълкувана или обогатена, за да се осигури необходимият контекст с оглед на вземането на решения и за да се създадат условия за адекватно и достатъчно разбиране с оглед ограничаването на последствията от инцидент с ИКТ или от киберзаплаха, включително техническите белези на дадена кибератака, отговорните за нея лица и техният начин на действие и мотивация;

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

17) „тестване за проникване (TLPT)“ означава симулиране на тактиката, техниките и процедурите на реални източници на заплаха, за които се счита, че представляват истинска киберзаплаха; тази симулация представлява контролиран, специално разработен и опиращ се на разузнавателни сведения (червен екип) тест на критичните оперативни производствени системи на финансовия субект;

18) „риск в областта на ИКТ, пораждан от трета страна“ означава риск в областта на ИКТ, който може да възникне за финансов субект във връзка с използваните от него услуги в областта на ИКТ, предоставяни от трета страна доставчик на такива услуги или от нейни поддоставчици, включително чрез споразумения за възлагане на дейности на външни изпълнители;

19) „трета страна доставчик на услуги в областта на ИКТ“ означава предприятие, което предоставя услуги в областта на ИКТ;

20) „вътрешногрупов доставчик на услуги в областта на ИКТ“ означава предприятие, което е част от финансова група и предоставя предимно услуги в областта на ИКТ на финансови субекти от същата група или на финансови субекти, които са част от една и съща институционална защитна схема, включително на техните предприятия майки, дъщерни предприятия, клонове или други субекти, намиращи се в обща собственост или под общ контрол;

21) „услуги в областта на ИКТ“ означава цифрови услуги и услуги за данни, предоставяни непрекъснато чрез системите на ИКТ на един или повече вътрешни или външни ползватели, включително хардуер като услуга и хардуерни услуги, което включва техническа поддръжка чрез актуализации на софтуер или фърмуер от доставчика на хардуер и изключва традиционните аналогови телефонни услуги;

22) „критична или важна функция“ означава функция, чието смущение би намалило съществено финансовите резултати на даден финансов субект, или стабилността или непрекъснатостта на неговите услуги и дейности, или функция, чието прекъсване, неизправност или срив би намалило съществено възможността на даден финансов субект да продължи да изпълнява условията и задълженията, свързани с неговия лиценз или останалите си задължения съгласно приложимото право в областта на финансовите услуги;

23) „трета страна критичен доставчик на услуги в областта на ИКТ“ означава трета страна, която е доставчик на услуги в областта на ИКТ, определен като имащ критично значение в съответствие с член 31;

24) „трета страна доставчик на услуги в областта на ИКТ, установен в трета държава“ означава трета страна доставчик на услуги в областта на ИКТ, който е установено в трета държава юридическо лице, което е сключило договорно споразумение с финансов субект за предоставяне на услуги в областта на ИКТ;

25) „дъщерно предприятие“ означава дъщерно предприятие по смисъла на член 2, точка 10 и член 22 от Директива 2013/34/ЕС;

26) „група“ означава група съгласно определението в член 2, точка 11 от Директива 2013/34/ЕС;

27) „предприятие майка“ означава предприятие майка по смисъла на член 2, точка 9 и член 22 от Директива 2013/34/ЕС;

28) „поддоставчик на ИКТ, установен в трета държава“ означава поддоставчик на ИКТ, който е установено в трета държава юридическо лице, което е сключило договорно споразумение с трета страна доставчик на услуги в областта на ИКТ или с трета страна доставчик на услуги в областта на ИКТ, установен в трета държава;

29) „риск от концентрация при ИКТ“ означава експозиция към дадена трета страна критичен доставчик на услуги в областта на ИКТ или към множество свързани такива доставчици, която поражда известна степен на зависимост от такива доставчици, така че ако съответният доставчик не бъде достъпен, престане да предоставя услугите си или понесе друг вид неизправност, това потенциално може да застраши способността на финансовия субект да изпълнява критични или важни функции или да му причини други видове неблагоприятни последици, включително големи загуби**,** или да застраши финансовата стабилност на Съюза като цяло;

30) „ръководен орган“ означава ръководен орган съгласно определението в 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 на Европейския парламент и на Съвета ([31]), член 2, параграф 1, точка 45 от Регламент (ЕС) № 909/2014, член 3, параграф 1, точка 20 от Регламент (ЕС) 2016/1011 и относимата разпоредба от Регламента относно пазарите на криптоактиви, или еквивалентните лица, които действително управляват субекта или изпълняват ключови функции в съответствие с приложимото право на Съюза или национално право;

31) „кредитна институция“ означава кредитна институция съгласно определението в член 4, параграф 1, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета ([32]);

32) „институция, освободена съгласно Директива 2013/36/ЕС“ означава субект, посочен в член 2, параграф 5, точки 4—23 от Директива 2013/36/ЕС;

33) „инвестиционен посредник“ означава инвестиционен посредник съгласно определението в член 4, параграф 1, точка 1 от Директива 2014/65/ЕС;

34) „малък и невзаимосвързан инвестиционен посредник“ означава инвестиционен посредник, който отговаря на условията по член 12, параграф 1 от Регламент (ЕС) 2019/2033 на Европейския парламент и на Съвета ([33]);

35) „платежна институция“ означава платежна институция съгласно определението в член 4, точка 4 от Директива (ЕС) 2015/2366;

36) „платежна институция, освободена съгласно Директива (ЕС) 2015/2366“ означава платежна институция, освободена съгласно член 32, параграф 1 от Директива (ЕС) 2015/2366;

37) „доставчик на услуги по предоставяне на информация за сметка“ означава доставчик на услуги по предоставяне на информация за сметка, както е посочено в член 33, параграф 1 от Директива (ЕС) 2015/2366;

38) „институция за електронни пари“ означава институция за електронни пари съгласно определението в член 2, точка 1 от Директива 2009/110/ЕО на Европейския парламент и на Съвета;

39) „институция за електронни пари, освободена съгласно Директива 2009/110/ЕО“ означава институция за електронни пари, ползваща се от освобождаване, както е посочено в член 9, параграф 1 от Директива 2009/110/ЕО;

40) „централен контрагент“ означава централен контрагент съгласно определението в член 2, точка 1 от Регламент (ЕС) № 648/2012;

41) „регистър на трансакции“ означава регистър на трансакции съгласно определението в член 2, точка 2 от Регламент (ЕС) № 648/2012;

42) „централен депозитар на ценни книжа“ означава централен депозитар на ценни книжа съгласно определението в член 2, параграф 1, точка 1 от Регламент (ЕС) № 909/2014;

43) „място на търговия“ означава място на търговия съгласно определението в член 4, параграф 1, точка 24 от Директива 2014/65/ЕС;

44) „лице, управляващо алтернативни инвестиционни фондове“ означава лице, управляващо алтернативни инвестиционни фондове съгласно определението в член 4, параграф 1, буква б) от Директива 2011/61/ЕС;

45) „управляващо дружество“ означава управляващо дружество съгласно определението в член 2, параграф 1, буква б) от Директива 2009/65/ЕО;

46) „доставчик на услуги за докладване на данни“ означава доставчик на услуги за докладване на данни по смисъла на Регламент (ЕС) № 600/2014, както е посочен в член 2, параграф 1, точки 34—36;

47) „застрахователно предприятие“ означава застрахователно предприятие съгласно определението в член 13, точка 1 от Директива 2009/138/ЕО;

48) „презастрахователно предприятие“ означава презастрахователно предприятие съгласно определението в член 13, точка 4 от Директива 2009/138/ЕО;

([31]) Директива 2009/65/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно координирането на законовите, подзаконовите и административните разпоредби относно предприятията за колективно инвестиране в прехвърлими ценни книжа (ПКИПЦК) (ОВ L 302, 17.11.2009 г., стр. 32).

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

([33]) Регламент (ЕС) 2019/2033 на Европейския парламент и на Съвета от 27 ноември 2019 г. относно пруденциалните изисквания за инвестиционните посредници и за изменение на регламенти (ЕС) № 1093/2010, (ЕС) № 575/2013, (ЕС) № 600/2014 и (ЕС) № 806/2014 (ОВ L 314, 5.12.2019 г., стр. 1).

49) „застрахователен посредник“ означава застрахователен посредник съгласно определението в член 2, параграф 1, точка 3 от Директива (ЕС) 2016/97 на Европейския парламент и на Съвета ([34]);

50) „посредник, предлагащ застрахователни продукти като допълнителна дейност“ означава посредник, предлагащ застрахователни продукти като допълнителна дейност съгласно определението в член 2, параграф 1, точка 4 от Директива (ЕС) 2016/97;

51) „презастрахователен посредник“ означава презастрахователен посредник съгласно определението в член 2, параграф 1, точка 5 от Директива (ЕС) 2016/97;

52) „институция за професионално пенсионно осигуряване“ означава институция за професионално пенсионно осигуряване съгласно определението в член 6, точка 1 от Директива (ЕС) 2016/2341;

53) „малка институция за професионално пенсионно осигуряване“ означава институция за професионално пенсионно осигуряване, която управлява пенсионни схеми, в които участват общо по-малко от 100 членове;

54) „агенция за кредитен рейтинг“ означава агенция за кредитен рейтинг съгласно определението в член 3, параграф 1, буква б) от Регламент (ЕО) № 1060/2009;

55) „доставчик на услуги за криптоактиви“ означава доставчик на услуги за криптоактиви съгласно определението в относимата разпоредба от Регламента относно пазарите на криптоактиви;

56) „емитент на токени, обезпечени с активи“ означава емитент на токени, обезпечени с активи съгласно определението в относимата разпоредба от Регламента относно пазарите на криптоактиви;

57) „администратор на критични бенчмаркове“ означава администратор на критични бенчмаркове съгласно определението в член 3, параграф 1, точка 25 от Регламент (ЕС) 2016/1011;

58) „доставчик на услуги за колективно финансиране“ означава доставчик на услуги за колективно финансиране съгласно определението в член 2, параграф 1, буква д) от Регламент (ЕС) 2020/1503 на Европейския парламент и на Съвета ([35]);

59) „регистър на секюритизации“ означава регистър на секюритизации съгласно определението в член 2, точка 23 от Регламент (ЕС) 2017/2402 на Европейския парламент и на Съвета ([36]);

60) „микропредприятие“ означава финансов субект, различен от място на търговия, централен контрагент, регистър на трансакции или централен депозитар на ценни книжа, който има под 10 служители и чийто годишен оборот и/или общо салдо по годишния счетоводен баланс не надхвърля 2 милиона евро;

61) „водещ надзорник“ означава Европейският надзорен орган, назначен в съответствие с член 31, параграф 1, буква б) от настоящия регламент;

62) „Съвместен комитет“ означава комитетът, посочен в член 54 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010;

63) „малко предприятие“ означава финансов субект, който има 10 или повече служители, но по-малко от 50 служители и чийто годишен оборот и/или общо салдо по годишния счетоводен баланс надхвърля 2 милиона евро, но не надхвърля 10 милиона евро;

64) „средно предприятие“ означава финансов субект, който не е малко предприятие и има под 250 служители и чийто годишен оборот не надхвърля 50 милиона евро и/или чието общо салдо по годишния счетоводен баланс не надхвърля 43 милиона евро;

65) „публичен орган“ означава всеки държавен орган или друг орган на публичната администрация, включително националните централни банки.

([34]) Директива (ЕС) 2016/97 на Европейския парламент и на Съвета от 20 януари 2016 г. относно разпространението на застрахователни продукти (ОВ L 26, 2.2.2016 г., стр. 19).

([35]) Регламент (ЕС) 2020/1503 на Европейския парламент и на Съвета от 7 октомври 2020 г. относно европейските доставчици на услуги за колективно финансиране на предприятията и за изменение на Регламент (ЕС) 2017/1129 и на Директива (ЕС) 2019/1937 (ОВ L 347, 20.10.2020 г., стр. 1).

([36]) Регламент (ЕС) 2017/2402 на Европейския парламент и на Съвета от 12 декември 2017 г. за определяне на обща рамка за секюритизациите и за създаване на специфична рамка за опростени, прозрачни и стандартизирани секюритизации, и за изменение на директиви 2009/65/ЕО, 2009/138/ЕО и 2011/61/ЕС, и регламенти (ЕО) № 1060/2009 и (ЕС) № 648/2012 (ОВ L 347, 28.12.2017 г., стр. 35).

Член 4

Принцип на пропорционалност

1. Финансовите субекти прилагат правилата, определени в глава II, в съответствие с принципа на пропорционалност, като вземат предвид своя размер и цялостен рисков профил, както и естеството, мащаба и сложността на своите услуги, дейности и операции.

2. Освен това прилагането от финансовите субекти на глави III и IV и на глава V, раздел I е пропорционално на техния размер и цялостен рисков профил, както и на естеството, мащаба и сложността на техните услуги, дейности и операции, както е изрично предвидено в съответните правила в тези глави.

3. Компетентните органи разглеждат прилагането на принципа на пропорционалност от финансовите субекти при прегледа на съгласуваността на рамката за управление на риска в областта на ИКТ въз основа на докладите, представени по искане на компетентните органи съгласно член 6, параграф 5 и член 16, параграф 2.

ГЛАВА II

Управление на риска в областта на ИКТ

Раздел I

Член 5

Управление и организация

1. Финансовите субекти разполагат с вътрешна рамка за управление и контрол, която гарантира ефективно и разумно управление на риска в областта на ИКТ, в съответствие с член 6, параграф 4, с оглед постигането на високо равнище на оперативна устойчивост на цифровите технологии.

2. Ръководният орган на финансовия субект определя, одобрява, упражнява надзор върху и носи отговорност за изпълнението на всички действия във връзка с посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ.

За целите на първа алинея ръководният орган:

а) носи крайната отговорност за управлението на риска в областта на ИКТ за финансовия субект;

б) въвежда политики, които имат за цел да осигурят поддържането на високи стандарти за наличността, автентичността, цялостността и поверителността на данните;

в) определя ясни роли и отговорности за всички свързани с ИКТ длъжности и установява подходящи правила за управление, за да се гарантират ефективна и навременна комуникация, сътрудничество и координация между тези длъжности;

г) носи цялостната отговорност за изготвянето и одобряването на стратегията за оперативна устойчивост на цифровите технологии, посочена в член 6, параграф 8, включително за определянето на подходящото ниво на толерантност към риска в областта на ИКТ за финансовия субект, както е посочено в член 6, параграф 8, буква б);

д) одобрява, упражнява надзор и периодично прави преглед на изпълнението на политиката на финансовия субект за непрекъснатост на дейността на ИКТ и на плановете му за реакция и възстановяване на ИКТ, посочени в член 11, съответно параграфи 1 и 3, които може да се приемат като целенасочена специфична политика, представляваща неразделна част от цялостната политика на финансовия субект за непрекъснатост на дейността и от плана за реакция и възстановяване;

е) одобрява и периодично прави преглед на плановете на финансовия субект за вътрешен одит на ИКТ, на одитите на ИКТ и на съществените промени в тях;

ж) разпределя и периодично прави преглед на подходящия бюджет за покриване на потребностите на финансовия субект във връзка с оперативната устойчивост на цифровите технологии по отношение на всички видове ресурси, включително съответните програми за повишаване на осведомеността за сигурността на ИКТ и обучението за оперативната устойчивост на цифровите технологии, посочени в член 13, параграф 6, както и уменията в областта на ИКТ на целия персонал;

з) одобрява и периодично прави преглед на политиката на финансовия субект относно споразуменията за използването на услуги в областта на ИКТ, предоставяни от трети страни доставчици на такива услуги;

и) въвежда канали за докладване на корпоративно равнище, които му позволяват да бъде надлежно информиран за:

i) споразуменията, сключени с трети страни доставчици на услуги в областта на ИКТ относно използването на такива услуги,

ii) всякакви относими планирани съществени промени по отношение на третите страни доставчици на услуги в областта на ИКТ,

iii) потенциалното отражение на такива промени върху критичните или важните функции, предмет на тези споразумения, включително обобщен анализ на риска, за да се оцени въздействието на тези промени, и поне съществените инциденти с ИКТ и тяхното въздействие, както и мерките за реакция и възстановяване и корективните мерки.

3. Финансовите субекти, без микропредприятията, определят функция, която да осъществява наблюдение върху сключените с третите страни доставчици на услуги в областта на ИКТ договорни споразумения за използване на услуги в областта на ИКТ или възлагат на член на висшето ръководство да упражнява надзор върху свързания с тези доставчици риск и съответната документация.

4. Членовете на ръководния орган на финансовия субект активно поддържат достатъчно актуални знания и умения, за да разбират и оценяват рисковете в областта на ИКТ и тяхното въздействие върху дейността на финансовия субект, включително като редовно преминават специално обучение, съизмеримо с управлявания риск в областта на ИКТ.

Раздел II

Член 6

Рамка за управление на риска в областта на ИКТ

1. Финансовите субекти разполагат с надеждна, широкообхватна и добре документирана рамка за управление на риска в областта на ИКТ като част от цялостната им система за управление на риска, която им позволява да се справят бързо, ефикасно и широкообхватно с риска в областта на ИКТ и да поддържат високо равнище на оперативна устойчивост на цифровите технологии.

2. Рамката за управление на риска в областта на ИКТ включва най-малко стратегии, политики, процедури, протоколи за ИКТ и инструменти, основани на ИКТ, които са необходими за надлежната и подходяща защита на всички информационни активи и активи на ИКТ, включително компютърен софтуер, хардуер, сървъри, както и за защитата на всички относими физически компоненти и инфраструктури, като например помещения, центрове за данни и зони, определени като чувствителни, така че да се гарантира, че всички информационни активи и активи на ИКТ са подходящо защитени от рискове, включително от увреждане и непозволен достъп или използване.

3. В съответствие със своята рамка за управление на риска в областта на ИКТ финансовите субекти свеждат до минимум въздействието на риска в областта на ИКТ чрез прилагане на подходящи стратегии, политики, процедури, протоколи за ИКТ и инструменти. При поискване те предоставят на компетентните органи пълна и актуална информация за риска в областта на ИКТ и за своята рамка за управление на риска в областта на ИКТ.

4. Финансовите субекти, без микропредприятията, възлагат на дадена контролна функция отговорността за управление и надзор на риска в областта на ИКТ и осигуряват подходящо ниво на независимост на тази контролна функция, за да се избегнат конфликти на интереси. Финансовите субекти гарантират подходящо разделяне и независимост на функциите за управление на риска в областта на ИКТ, контролните функции и функциите за вътрешен одит, според модела на трите защитни слоя или свой модел за управление и контрол на риска.

5. Рамката за управление на риска в областта на ИКТ се документира и се преразглежда поне веднъж годишно — или периодично за микропредприятията — както и при съществени инциденти с ИКТ, като това се прави съобразно инструкциите на надзорните органи или заключенията, направени в резултат от съответните тестове на оперативната устойчивост на цифровите технологии или от одитните процеси. Рамката се усъвършенства непрекъснато въз основа на натрупания при нейното прилагане и наблюдаване опит. На компетентния орган се представя доклад за прегледа на рамката за управление на риска в областта на ИКТ при поискване от негова страна.

6. Рамката за управление на риска в областта на ИКТ на финансовите субекти, без микропредприятията, подлежи на редовен вътрешен одит от одитори в съответствие с плана за одит на финансовия субект. Тези одитори притежават достатъчно знания, умения и експертен опит във връзка с риска в областта на ИКТ, както и подходящо ниво на независимост. Честотата и насочеността на одитите на ИКТ са съобразени с риска в областта на ИКТ на финансовия субект.

7. Въз основа на заключенията от вътрешния одитен преглед финансовите субекти въвеждат официален процес на последващи действия, включително правила за своевременна проверка и отстраняване на критично важните проблеми, посочени в заключенията от одита на ИКТ.

8. Рамката за управление на риска в областта на ИКТ включва стратегия за оперативна устойчивост на цифровите технологии, в която се описва нейното прилагане. За тази цел в стратегията за оперативна устойчивост на цифровите технологии се посочват методите за противодействие на риска в областта на ИКТ и за постигането на конкретни цели в областта на ИКТ, както следва:

а) обяснява се как рамката за управление на риска в областта на ИКТ подпомага стратегията и целите, които финансовият субект си е поставил за своята стопанска дейност;

б) определя се нивото на толерантност към риска в областта на ИКТ според склонността на финансовия субект за поемане на риск и се проучва допустимата степен на въздействие при смущения на ИКТ;

в) залагат се ясни цели за сигурност на информацията, включително ключови показатели за ефективност и ключови рискови показатели;

г) обяснява се референтната архитектура на ИКТ и всички промени, необходими за постигането на конкретни цели за дейността;

д) очертават се различните въведени механизми за откриване на инциденти с ИКТ, за предотвратяване на тяхното въздействие и за осигуряване на защита срещу него;

е) демонстрира се текущото състояние на оперативната устойчивост на цифровите технологии въз основа на броя на съществените инциденти с ИКТ, за които е било съобщено, и ефективността на превантивните мерки;

ж) извършва се тестване на оперативната устойчивост на цифровите технологии в съответствие с глава IV от настоящия регламент;

з) очертава се комуникационната стратегия при настъпване на инциденти с ИКТ, чието оповестяване се изисква в съответствие с член 14.

9. Финансовите субекти могат, в контекста на стратегията за оперативна устойчивост на цифровите технологии, посочена в параграф 8, да определят цялостна стратегия за прибягване до множество доставчици на ИКТ, на равнище група или субект, в която се посочват ключовите зависимости от третите страни доставчици на услуги в областта на ИКТ и се обяснява логиката зад избора на съответните трети страни доставчици на услуги в областта на ИКТ.

10. Финансовите субекти могат, в съответствие с правото на Съюза и националното секторно право, да възлагат задачите по проверка на спазването на изискванията за управление на риска в областта на ИКТ на вътрешногрупови или външни предприятия. В случай на такова възлагане на външен изпълнител финансовият субект продължава да носи цялата отговорност за проверката на спазването на изискванията за управление на риска в областта на ИКТ.

Член 7

Системи и протоколи на ИКТ и основани на ИКТ инструменти

С цел да се справят с риска в областта на ИКТ и да го управляват, финансовите субекти използват и поддържат в актуален вид системи и протоколи на ИКТ и основани на ИКТ инструменти, които са:

а) съобразени с мащаба на операциите, посредством които те провеждат дейността си, в съответствие с принципа на пропорционалност, посочен в член 4;

б) надеждни;

в) с достатъчен капацитет 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, включително при въвеждането на нови технологии;

г) технологично устойчиви, така че да могат адекватно да удовлетворяват необходимостта от допълнително обработване на информация, изисквано при неблагоприятни пазарни условия или други проблематични ситуации.

Член 8

Идентифициране

1. Като част от посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ финансовите субекти идентифицират, класифицират и документират по подходящ начин всички поддържани от ИКТ работни функции, роли и отговорности, информационните активи и активите на ИКТ, поддържащи тези функции, както и техните роли и зависимости във връзка с рисковете в областта на ИКТ. Когато е необходимо — но поне веднъж годишно — финансовите субекти правят преглед на адекватността на тази класификация и на съответната документация.

2. Финансовите субекти непрекъснато идентифицират всички източници на риск в областта на ИКТ, по-специално доколко са изложени на риск от или свързан със други финансови субекти, и оценяват киберзаплахите и уязвимите места на ИКТ, които имат отношение към техните поддържани от ИКТ работни функции, информационни активи и активи на ИКТ. Финансовите субекти редовно — и поне веднъж годишно — 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 поддържани от ИКТ работни функции, информационни активи или активи на ИКТ.

4. Финансовите субекти идентифицират всички информационни активи и активи на ИКТ, включително в отдалечените обекти, мрежови ресурси и хардуер, и правят опис на онези от тях, за които считат, че са от критично значение. Те описват конфигурацията на информационните активи и активите на ИКТ, както и връзките и взаимозависимостта между различните информационни активи и активи на ИКТ.

5. Финансовите субекти идентифицират и документират всички процеси, които зависят от трети страни доставчици на услуги в областта на ИКТ, и идентифицират взаимовръзките с онези трети страни доставчици на услуги в областта на ИКТ, които предоставят услуги, поддържащи критични или важни функции.

6. За целите на параграфи 1, 4 и 5 финансовите субекти поддържат съответните списъци и ги актуализират периодично и всеки път, когато настъпи съществена промяна по параграф 3.

7. Финансовите субекти, без микропредприятията, редовно — но поне веднъж годишно — правят специална оценка на риска в областта на ИКТ за всички наследените системи на ИКТ, и винаги преди и след свързването на технологии, приложения или системи.

Член 9

Защита и предотвратяване

1. С цел адекватна защита на системите на ИКТ и с оглед на организирането на мерките за реакция финансовите субекти неотклонно наблюдават и контролират сигурността и функционирането на системите на ИКТ и основаните на ИКТ инструменти, и свеждат до минимум въздействието на риска в областта на ИКТ чрез въвеждането на подходящи инструменти, политики и процедури за сигурност на ИКТ.

2. Финансовите субекти проектират, възлагат и прилагат политики, процедури, протоколи и инструменти за сигурност на ИКТ, които имат за цел да осигурят устойчивостта, непрекъснатостта и наличността на системите на ИКТ, и по-специално онези, които поддържат критични или важни функции, и да поддържат високи стандарти за наличността, автентичността, цялостността и поверителността на данните при тяхното съхранение, използване или предаване.

3. За постигане на целите, посочени в параграф 2, финансовите субекти използват ИКТ решения и процеси, които са подходящи в съответствие с член 4. Тези ИКТ решения и процеси:

а) гарантират сигурността на средствата за предаване на данни;

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

в) предотвратяват липсата на наличност, нарушаването на автентичността, цялостността и поверителността и загубата на данни;

г) гарантират, че данните са защитени от рискове, произтичащи от управлението на данните, включително лошо администриране, рискове, свързани с обработването им, и човешка грешка.

(4) Като част от посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ финансовите субекти:

а) разработват и документират политика за сигурност на информацията, в която определят правила за защита на наличността, автентичността, цялостността и поверителността на данните, информационните активи и активите на ИКТ, включително тези на техните клиенти, когато е приложимо;

б) създават, следвайки подход, при който се отчита рискът, стабилна структура за управление на мрежите и инфраструктурата с помощта на подходящи техники, методи и протоколи, което може да включва използването на автоматизирани механизми за обособяване на засегнатите при кибератаки информационни активи;

в) прилагат политики, които ограничават физическия или логическия достъп до информационните активи и активите на ИКТ единствено 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, и гарантират разумното им управление;

г) прилагат политики и протоколи за стабилни механизми за удостоверяване на автентичността, като използват съответните стандарти и специални системи за проверки и предпазни мерки за криптографските ключове, с които данните са криптирани след одобрено тяхно класифициране и извършена оценка на риска в областта на ИКТ;

д) прилагат документирани политики, процедури и контролни механизми за управление на промените в ИКТ — включително на промените в софтуера, хардуера, компонентите на фърмуера, параметрите на системите или сигурността — които почиват на подход с оценка на риска и са неразделна част от цялостния процес на управление на промените от страна на финансовия субект с цел да се гарантира контролираното записване, тестване, оценяване, одобряване, прилагане и проверяване на всички промени в системите на ИКТ;

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

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

За целите на първа алинея, буква д) процесът на управление на промените в ИКТ се одобрява от подходяща йерархична стълбица и за него се въвеждат специални протоколи.

Член 10

Откриване

1. Както е посочено в член 17, финансовите субекти разполагат с механизми за бързо откриване на необичайните дейности — включително проблеми с функционирането на мрежата на ИКТ и инциденти с ИКТ, както и за идентифицирането на потенциалните точки, чиято повреда може да доведе до общ отказ на системите.

Механизмите по първа алинея се тестват редовно, както е посочено в член 25.

2. Механизмите за откриване по параграф 1 позволяват множество нива на контрол, определят прагове за отправяне на предупреждение и критерии за задействане и иницииране на процеси за реакция при инциденти с ИКТ, включително автоматични механизми за предупреждаване на съответните служители, отговорни за реагирането при инциденти с ИКТ.

3. Финансовите субекти отделят достатъчно ресурси и оперативен капацитет за наблюдение на активността на ползвателите, възникналите аномалии при ИКТ и инцидентите с ИКТ, особено кибератаките.

4. Доставчиците на услуги за докладване на данни разполагат наред с това и със системи, които могат да извършват надеждна проверка за пълнота на отчетите на сделките, да откриват пропуски и явни грешки и да изискват повторното предоставяне на посочените отчети.

Член 11

Реакция и възстановяване

1. Като част от посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ и въз основа на посочените в член 8 изисквания за идентифициране, финансовите субекти въвеждат широкообхватна политика за непрекъснатост на дейността на ИКТ, която може да бъде приета като специална отделна политика, явяваща се неразделна част от цялостната политика на финансовия субект за непрекъснатост на дейността.

2. Финансовите субекти прилагат политиката за непрекъснатост на дейността на ИКТ чрез специални, подходящи и документирани правила, планове, процедури и механизми, които имат за цел:

а) да се осигури непрекъснатостта на критичните или важните функции на финансовия субект;

б) да се предприемат бързи, подходящи и ефективни ответни действия и разрешаване на всички инциденти с ИКТ, така че да се ограничават щетите и да се отдава приоритет на възобновяването на функционирането и на възстановяването на информацията;

в) след всеки вид инцидент с ИКТ да се задействат без забавяне специални планове за прилагане на мерки, процеси и технологии за овладяването му и за предотвратяването на допълнителни щети, както и специални процедури за реакция и възстановяване, установени в член 12;

г) да се прави оценка на предварителните последици, щети и загуби;

д) да се определят действията за комуникация и за управление на кризи с цел актуализираната информация да се предаде на всички имащи отношение вътрешни служители и външни заинтересовани страни — както е посочено в член 14, и да се докладва на компетентните органи — както е посочено в член 19.

3. Като част от посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ финансовите субекти прилагат свързани с нея планове за реакция и възстановяване на ИКТ, които при всички финансови субекти освен микропредприятията подлежат на независими вътрешни одитни прегледи.

4. Финансовите субекти въвеждат, поддържат и периодично тестват подходящи планове за непрекъснатост на дейността на ИКТ, по-специално по отношение на критичните или важните функции, възложени с договори на трети страни доставчици на услуги в областта на ИКТ.

5. Като част от цялостната политика за непрекъснатост на дейността финансовите субекти извършват анализ на въздействието върху дейността (АВД) на експозициите си към сериозни смущения в дейността. В рамките на АВД финансовите субекти оценяват потенциалното въздействие на сериозните смущения в дейността въз основа на количествени и качествени критерии, като използват вътрешни и външни данни и анализ на сценарии, ако е целесъобразно. АВД разглежда доколко са критични идентифицираните и описани работни функции, поддържащи процеси, зависимости от трета страна и информационните активи, както и тяхната взаимозависимост. Финансовите субекти гарантират, че активите на ИКТ и услугите в областта на ИКТ се проектират и използват в пълно съответствие с АВД, по-специално с цел да се осигури адекватно възпроизвеждане на всички критични компоненти.

6. Като част от широкообхватното си управление на риска в областта на ИКТ финансовите субекти:

а) тестват плановете за непрекъснатост на дейността на ИКТ и плановете за реакция и възстановяване на ИКТ във връзка със системите на ИКТ, поддържащи всички функции, най-малко веднъж годишно, както и при съществени промени в системите на ИКТ, които поддържат критични или важни функции;

б) тестват изготвените в съответствие с член 14 планове за комуникация при криза.

За целите на първа алинея, буква а) финансовите субекти, без микропредприятията, предвиждат в тестовите си планове сценарии за кибератаки и преминаване от първичната инфраструктура на ИКТ към възпроизвеждащия я капацитет, резервни копия и възпроизвеждащи системи, необходими за изпълнение на задълженията по член 12.

Финансовите субекти извършват редовен преглед на своята политика за непрекъснатост на дейността на ИКТ и на плановете си за реакция и възстановяване на ИКТ, като вземат предвид резултатите тестовете, от проведени съгласно първа алинея, и препоръките от одитните проверки или надзорните прегледи.

7. Финансовите субекти, без микропредприятията, разполагат с функция за управление на кризи, която, при задействане на техните планове за непрекъснатост на дейността на ИКТ или на плановете им за реакция и възстановяване на ИКТ, наред с другото определя ясни процедури за управление на вътрешната и външната комуникация при кризи в съответствие с член 14.

8. При задействане на плановете им за непрекъснатост на дейността на ИКТ и на плановете им за реакция и възстановяване на ИКТ, финансовите субекти пазят леснодостъпни записи на действията преди и по време на събитията, нарушили обичайното функциониране.

9. Централните депозитари на ценни книжа предоставят на компетентните органи копия от резултатите от тестовете за непрекъснатост на дейността на ИКТ или от подобни упражнения.

10. Финансовите субекти, без микропредприятията, докладват на компетентните органи по тяхно искане предварителна оценка на агрегираните годишни разходи и загуби, причинени от съществени инциденти с ИКТ.

11. В съответствие с член 16 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010 ЕНО, чрез Съвместния комитет, разработват до 17 юли 2024 г. общи насоки за предварителната оценка на агрегираните годишни разходи и загуби, посочени в параграф 10.

Член 12

Политики и процедури за съхраняване на резервни копия, процедури и методи за възстановяване на информацията

1. С цел да се осигури максимално бързо възстановяване на системите на ИКТ и на данните, с ограничени смущения и загуби, финансовите субекти разработват и документират като част от рамката си за управление на риска в областта на ИКТ:

а) политики и процедури за съхраняване на резервни копия на данните, в които се определя обхватът на данните, за които се съхраняват резервни копия, както и минималната честота на това копиране, въз основа на това доколко е критично значението на данните и какво е нивото им на поверителност;

б) процедури и методи за възстановяване на информацията.

2. Финансовите субекти създават резервни системи, които могат да бъдат задействани в съответствие с политиките и процедурите за съхраняване на резервни копия, както и процедури и методи за възстановяване. Активирането на резервните системи не застрашава сигурността на мрежовите и информационните системи, нито наличността, автентичността, цялостността или поверителността на данните. Процедурите за съхраняване на резервни копия и процедурите и методите за възстановяване на информацията се тестват периодично.

3. Когато финансовите субекти използват собствени системи за възстановяване на резервните копия на данните, те използват системи на ИКТ, които са отделени физически и логически от основната им система на ИКТ. Системите на ИКТ са защитени по сигурен начин от непозволен достъп или неизправност на ИКТ и дават възможност за своевременно възстановяване на услугите, които използват данни и резервни копия на системите, когато е необходимо.

При централните контрагенти плановете за възстановяване осигуряват възможност за възстановяването на всички трансакции към момента на смущението, така че централният контрагент да може да продължи да функционира по надежден начин и да приключи сетълмента на определената дата.

Доставчиците на услуги за докладване на данни освен това поддържат достатъчно ресурси и разполагат с резервни механизми и механизми за възстановяване, за да предлагат и поддържат услугите си по всяко време.

4. Финансовите субекти, без микропредприятията, поддържат възпроизвеждащи ИКТ системи, чиито ресурси, капацитет и функции са достатъчни за задоволяване на потребностите на дейността. Микропредприятията оценяват необходимостта от поддържане на такива възпроизвеждащи ИКТ системи въз основа на рисковия си профил.

5. Централните депозитари на ценни книжа поддържат поне един допълнителен обект за обработка, разполагащ с достатъчно ресурси, капацитет, функции и правила относно персонала за задоволяване на потребностите на дейността.

Допълнителният обект за обработка:

а) се намира на физическо разстояние от основния обект за обработка, така че да има различен 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 критичните или важните функции или за предоставяне на такова ниво на обслужване, което позволява на финансовия субект да извършва операциите от критично значение в рамките на заложените цели за възстановяване на информацията;

в) е непосредствено достъпен за персонала на финансовия субект, в случай че основният обект за обработка е станал недостъпен, така че да се осигури непрекъснатостта на критичните или важните функции.

6. Когато определят целите си за продължителността на възстановяване на информацията и за точката на възстановяване за всяка функция, финансовите субекти взимат предвид дали функцията е критична или важна и 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 необходимите проверки, включително множествени проверки и сравнение на възстановените с оригиналните данни, за да се гарантира поддържането на най-високо ниво на пълнота на данните. Тези проверки се извършват и когато се възстановяват данни от външни заинтересовани страни, така че да се осигури съгласуваност на всички данни между отделните системи.

Член 13

Обучение и развитие

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

2. Финансовите субекти извършват прегледи на възникналите инциденти с ИКТ, след като съществен инцидент с ИКТ прекъсне основната им дейност, за да проучат причините за смущението и да установят какво е необходимо да се подобри в основаните на ИКТ операции или в посочената в член 11 политика за непрекъснатост на дейността на ИКТ.

При поискване финансовите субекти, без микропредприятията, съобщават на компетентните органи промените, които са били въведени след посочените в първа алинея прегледи на възникналите инциденти с ИКТ.

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, включително по отношение на следното:

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

б) качеството и бързината на техническата експертиза, когато извършването на такава е счетено за целесъобразно;

в) ефективността на процедурата на финансовия субект за пренасочване на управлението на инцидентите;

г) ефективността на вътрешната и външната комуникация.

3. В процеса на оценка на риска в областта на ИКТ надлежно и непрекъснато се добавя натрупаният опит от проведените в съответствие с членове 26 и 27 тестове на оперативната устойчивост на цифровите технологии, от реалните инциденти с ИКТ — особено кибератаките, както и от срещнатите предизвикателства при задействането на плановете за непрекъснатост на дейността на ИКТ и плановете за реакция и възстановяване на ИКТ, а така също и съответната информация, обменяна с контрагентите и оценявана при надзорните прегледи. Тези констатации съставляват основата на подходящи преразглеждания на съответните компоненти на посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ.

4. Финансовите субекти наблюдават доколко ефективно се провежда стратегията им за оперативна устойчивост на цифровите технологии, посочена в член 6, параграф 8. С цел да определят степента, в която техните ИКТ са изложени на риск, особено във връзка с критични или важни функции, да задълбочат познанията си за киберсигурността и да усъвършенстват готовността си в тази област, финансовите субекти картографират тенденцията при рисковете в областта на 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 субекти 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 и обучения се прилагат за всички служители и за висшето ръководство и имат ниво на сложност, съобразено с обхвата на техните функции. Когато е целесъобразно, финансовите субекти включват и третите страни доставчици на услуги в областта на ИКТ в съответните си схеми за обучение в съответствие с член 30, параграф 2, буква и).

7. Финансовите субекти, без микропредприятията, 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 се запознават с най-новите процеси за управление на риска в областта на ИКТ, за да могат ефективно да противодействат на настоящите или новите форми на кибератаки.

Член 14

Комуникация

1. Като част от посочената в член 6, параграф 1 рамка за управление на риска в областта на ИКТ финансовите субекти разполагат с планове за комуникация при криза, които предвиждат отговорно уведомяване на клиентите и контрагентите, а по необходимост — и на обществеността, поне за съществените инциденти с ИКТ или уязвими места.

2. Като част от рамката за управление на риска в областта на ИКТ финансовите субекти прилагат комуникационни политики за собствения си персонал и за външните заинтересовани страни. В комуникационната политика за персонала се взема под внимание необходимостта да се прави разлика между персонала, зает с управлението на риска в областта на ИКТ, и по-специално персонала, отговарящ за реакцията и възстановяването, и персонала, който трябва да бъде уведомяван.

3. За изпълнението на комуникационната стратегия при инциденти в областта на ИКТ отговаря поне един служител на финансовия субект, като за тази цел изпълнява и функцията връзки с обществеността и медиите.

Член 15

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

В рамките на съвместния комитет и в консултации с Агенцията на Европейския съюз за киберсигурност (ENISA) ЕНО разработват общи проекти на регулаторни технически стандарти с оглед на следното:

а) определяне на допълнителните елементи, които да бъдат включени в посочените в член 9, параграф 2 стратегии, 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 запазят, включително чрез криптиране, наличността, автентичността, цялостността и поверителността на данните, както и да се осигури точното и бързо предаване на данните, без съществени смущения и неоправдано забавяне;

б) разработване на допълнителни компоненти на посочените в член 9, параграф 4, буква в) механизми за контрол на правата на управление на достъпа 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 риска в областта на ИКТ чрез подходящи показатели за моделите на използване на мрежата, за часовите пояси, за дейността, свързана с информационните технологии, и за неизвестните устройства;

в) доразработване на посочените в член 10, параграф 1 механизми за бързо откриване на необичайните дейности, както и на посочените в член 10, параграф 2 критерии за задействане на процесите за откриване на инциденти при ИКТ и за реакция;

г) доуточняване на компонентите на посочената в член 11, параграф 1 политика за непрекъснатост на дейността на ИКТ;

д) доуточняване на изискванията за тестване на посочените в член 11, параграф 6 планове за непрекъснатост на дейността на ИКТ с цел тестването надлежно да обхваща всички сценарии, при които критична 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 трети страни доставчици на услуги в областта на ИКТ, а когато е приложимо — и политическия риск в юрисдикциите на съответните доставчици;

е) доуточняване на компонентите на посочените в член 11, параграф 3 планове за реакция и възстановяване на ИКТ;

ж) доуточняване на съдържанието и формата на посочения в член 6, параграф 5 доклад за прегледа на рамката за управление на риска в областта на ИКТ;

Когато разработват тези проекти на регулаторни технически стандарти, ЕНО вземат предвид размера и цялостния рисков профил на финансовия субект и естеството, мащаба и сложността на неговите услуги, дейности и операции, като същевременно надлежно отчитат всяка специфична характеристика, произтичаща от различното естество на дейностите в различните сектори на финансовите услуги.

ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до 17 януари 2024 г.

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

Член 16

Опростена рамка за управление на риска в областта на ИКТ

1. Членове 5—15 от настоящия регламент не се прилагат за малки и невзаимосвързани инвестиционни посредници, платежни институции, освободени съгласно Директива (ЕС) 2015/2366; институции, освободени съгласно Директива 2013/36/ЕС, по отношение на които държавите членки са решили да не прилагат възможността, посочена в член 2, параграф 4 от настоящия регламент; институции за електронни пари, освободени съгласно Директива 2009/110/ЕО; и малки институции за професионално пенсионно осигуряване.

Без да се засяга първа алинея посочените в нея субекти:

а) въвеждат и поддържат стабилна и документирана рамка за управление на риска в областта на ИКТ, в която се описват подробно механизмите и мерките, насочени към бързо, ефикасно и многоаспектно управление на риска в областта на ИКТ, включително за защита на съответните физически компоненти и инфраструктури;

б) непрекъснато наблюдават сигурността и функционирането на всички системи на ИКТ;

в) свеждат до минимум въздействието на риска в областта на ИКТ чрез използване на стабилни, устойчиви и поддържани в актуален вид системи и протоколи на ИКТ и основани на ИКТ инструменти, които са подходящи да подпомагат изпълнението на техните дейности и предоставянето на услуги, и защитават адекватно наличността, автентичността, цялостността и поверителността на данните в мрежовите и информационните системи;

г) осигуряват възможност за бързо установяване и откриване на източниците на риск в областта на ИКТ и аномалии в мрежовите и информационните системи и за бързо справяне с инциденти с ИКТ;

д) определят ключовите зависимости от третите страни доставчици на услуги в областта на ИКТ;

е) осигуряват непрекъснатостта на критичните и важните функции чрез планове за непрекъснатост на дейността и мерки за реакция и възстановяване, които включват най-малко мерки за съхраняване на резервни копия и възстановяване;

ж) редовно тестват плановете и мерките, посочени в буква е), както и ефективността на мерките за контрол, предприети в съответствие с букви а) и в);

з) прилагат, по целесъобразност, съответните оперативни заключения, произтичащи от тестовете, посочени в буква ж), и от анализа след инциденти в процеса на оценка на риска в областта на ИКТ, и разработват, в съответствие с нуждите и профила на риска в областта на ИКТ, програми за повишаване на осведомеността за сигурността на ИКТ и обучения по оперативна устойчивост на цифровите технологии за персонала и ръководството.

2. Рамката за управление на риска в областта на ИКТ, посочена в параграф 1, втора алинея, буква а), се документира и преразглежда периодично и при възникване на съществени инциденти с ИКТ в съответствие с надзорните инструкции. Рамката се усъвършенства непрекъснато въз основа на натрупания при нейното прилагане и наблюдаване опит. На компетентния орган се представя доклад за прегледа на рамката за управление на риска в областта на ИКТ при поискване от негова страна.

3. В рамите на съвместния комитет и в консултации с ENISA ЕНО разработват общи проекти на регулаторни технически стандарти с оглед на следното:

а) доуточняване на елементите, които да бъдат включени в рамката за управление на риска в областта на ИКТ, посочена в параграф 1, втора алинея, буква а);

б) доуточняване на елементите във връзка със системите, протоколите и инструментите за свеждане до минимум на въздействието на риска в областта на ИКТ, посочено в параграф 1, втора алинея, буква в), така че да се гарантира сигурността на мрежите, да се създадат подходящи защитни механизми срещу проникване и срещу злоупотреба с данните, да се запазят наличността, автентичността, цялостността и поверителността на данните;

в) доуточняване на компонентите на плановете за непрекъснатост на дейността на ИКТ, посочени в параграф 1, втора алинея, буква е);

г) доуточняване на правилата за тестване на плановете за непрекъснатост на дейността и гарантиране на ефективността на мерките за контрол, посочени в параграф 1, втора алинея, буква ж), и гарантиране това тестване надлежно да обхваща всички сценарии, при които критична или важна функция се предоставя с неприемливо ниско качество или не се предоставя изобщо;

д) доуточняване на съдържанието и формата на доклада за прегледа на рамката за управление на риска в областта на ИКТ, посочен в параграф 2.

Когато разработват тези проекти на регулаторни технически стандарти, ЕНО вземат предвид размера и цялостния рисков профил на финансовите субекти и естеството, мащаба и сложността на техните услуги, дейности и операции.

ЕНО предават на Комисията тези проекти на регулаторни технически стандарти до 17 януари 2024 г.

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

ГЛАВА III

Инциденти с ИКТ — управление, класифициране и докладване

Член 17

Процес за управление на инцидентите с ИКТ

1. Финансовите субекти определят, въвеждат и прилагат процес за управление на инцидентите с ИКТ, чрез който да се откриват, управляват и докладват инцидентите с ИКТ.

2. Финансовите субекти документират всички инциденти с ИКТ и значителни киберзаплахи. Финансовите субекти въвеждат подходящи процедури и процеси за последователно и интегрирано наблюдаване, справяне и проследяване на инцидентите с ИКТ, така че да се установят, документират и преодолеят основните причини за тях, за да се предотврати появата им.

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

а) определят се показатели за ранно предупреждение;

б) въвеждат се процедури за установяване, проследяване, регистриране, категоризиране и класифициране на инцидентите с ИКТ според техния приоритет и тежест и според критичността на засегнатите услуги — в съответствия с критериите по член 18, параграф 1;

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

г) изготвят се планове за комуникация с персонала, външните заинтересовани страни и медиите в съответствие с член 14, както и планове за уведомяване на клиентите, за процедури за вътрешно пренасочване на управлението на инцидентите, включително на оплакванията на клиентите във връзка с ИКТ, както и планове за предоставяне на информация на контрагентите — финансови субекти, ако това е необходимо;

д) гарантира се, че поне съществените инциденти с ИКТ се докладват на съответното висше ръководство и че ръководният орган се уведомява поне за съществените инциденти с ИКТ, като се обяснява оказаното въздействие и реакцията и се посочва какви допълнителни контролни мерки трябва да се въведат в резултат на такива инциденти с ИКТ;

е) въвеждат се процедури за реакция при инцидент с ИКТ, за да се ограничат последиците и своевременно да се възобнови обичайното и сигурно функциониране на услугите.

Член 18

Класифициране на инцидентите с ИКТ и киберзаплахите

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

а) броя и/или значимостта на клиентите или финансовите контрагенти, засегнати от инцидента с ИКТ, и, когато е приложимо, размера или броя на трансакциите, засегнати от инцидента с ИКТ, както и евентуално въздействие на инцидента с ИКТ върху репутацията;

б) продължителността на инцидента с ИКТ, включително периода на прекъсване на услугата;

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

г) загубата на данни в резултат на инцидента с ИКТ, във връзка с наличността, автентичността, цялостността или поверителността на данните;

д) критичната значимост на засегнатите услуги, включително на сделките и операциите на финансовия субект;

е) икономическите последици, по-специално преките и непреките разходи и загуби, от инцидента с ИКТ в абсолютно и в относително изражение.

2. Финансовите субекти класифицират киберзаплахите като значими въз основа на критичността на изложените на риск услуги, включително трансакциите и операциите на финансовия субект, броя и/или значимостта на клиентите или финансовите контрагенти, към които е насочена киберзаплахата, и географския обхват на изложените на риск райони.

3. В рамките на съвместния комитет и в консултации с ЕЦБ и ENISA ЕНО разработват общи проекти на регулаторни технически стандарти за доуточняване на:

а) критериите по параграф 1, включително праговете на същественост за определяне на съществените инциденти с ИКТ или, ако е приложимо, съществените операционни или свързани със сигурността инциденти, свързани с плащания, които трябва да бъдат докладвани по силата на член 19, параграф 1;

б) критериите, които компетентните органи трябва да прилагат, когато оценяват значението на съществени инциденти с ИКТ или, ако е приложимо, съществени операционни или свързани със сигурността инциденти, свързани с плащания, за съответните компетентни органи в други държави членки, и информацията в докладите за съществени инциденти с ИКТ или, ако е приложимо, съществени операционни или свързани със сигурността инциденти, свързани с плащания, която трябва да бъде споделяна с други компетентни органи по силата на член 19, параграфи 6 и 7;

в) критериите по параграф 2 от настоящия член, включително високите прагове на същественост за определяне на значителните киберзаплахи.

4. При разработването на посочените в параграф 3 от настоящия член общи проекти на регулаторни технически стандарти ЕНО се съобразяват с критериите по член 4, параграф 2, както и с международните стандарти, насоки и спецификации, разработени и публикувани от ENISA, включително и за други икономически сектори, когато е целесъобразно. За целите на прилагането на критериите по член 4, параграф 2 ЕНО надлежно отчитат необходимостта микропредприятията и малките и средните предприятия да мобилизират достатъчно ресурси и капацитет, за да се гарантира бързото управление на инцидентите с ИКТ.

ЕНО предават на Комисията тези общи проекти на регулаторни технически стандарти до 17 януари 2024 г.

На Комисията се делегират правомощия да допълни настоящия регламент, като приеме посочените в параграф 3 регулаторни технически стандарти в съответствие с членове 10—14 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

Член 19

Докладване за съществените инциденти с ИКТ и уведомяване на доброволен принцип за значителни киберзаплахи

1. Финансовите субекти докладват на съответния компетентен орган по член 46 за съществените инциденти с ИКТ в съответствие с параграф 4 от настоящия член.

Когато финансов субект подлежи на надзор от повече от един национален компетентен орган, посочен в член 46, държавите членки определят един-единствен орган за компетентен орган, който отговаря за изпълнението на функциите и задълженията, предвидени в настоящия член.

Кредитните институции, класифицирани като значими в съответствие с член 6, параграф 4 от Регламент (ЕС) № 1024/2013, докладват за съществените инциденти с ИКТ на съответния национален компетентен орган, определен в съответствие с член 4 от Директива 2013/36/ЕС, който незабавно предава този доклад на ЕЦБ.

За целите на първа алинея финансовите субекти събират и проучват цялата съответна информация, след което по образеца, посочен в член 20, изготвят първоначалното уведомление и докладите по параграф 4 от настоящия член, които предават на компетентния орган. В случай че техническа невъзможност възпрепятства подаването на първоначалното уведомление по образеца, финансовите субекти уведомяват компетентния орган за това чрез алтернативни средства.

Първоначалното уведомление и докладите по параграф 4 съдържат 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.

Без да се засяга докладването по първа алинея от финансовия субект на съответния компетентен орган, държавите членки могат допълнително да определят, че някои или всички финансови субекти предоставят също първоначалното уведомление и всички доклади по параграф 4 от настоящия член по образците, посочени в член 20, на компетентните органи или на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), определени или установени в съответствие с Директива (ЕС) 2022/2555.

2. Финансовите субекти могат на доброволен принцип да уведомяват съответния компетентен орган за значителни киберзаплахи, когато преценят, че заплахата е от значение за финансовата система, ползвателите на услугите или клиентите. Съответният компетентен орган може да предостави такава информация на други имащи отношение органи по параграф 6.

Кредитните институции, класифицирани като значими в съответствие с член 6, параграф 4 от Регламент (ЕС) № 1024/2013, могат на доброволен принцип да уведомяват за значителни киберзаплахи съответния национален компетентен орган, определен в съответствие с член 4 от Директива 2013/36/ЕС, който незабавно предава това уведомление на ЕЦБ.

Държавите членки могат да определят, че финансовите субекти, които уведомяват на доброволен принцип в съответствие с първа алинея, могат също така да предават това уведомление на ЕРИКС, определени или установени в съответствие с Директива (ЕС) 2022/2555.

3. Когато възникне съществен инцидент с ИКТ и той има последици за финансовите интереси на клиентите, финансовите субекти възможно най-бързо след като узнаят за него уведомяват клиентите си за съществения инцидент с ИКТ и за предприетите мерки за ограничаване на неблагоприятните последици.

В случай на значителна киберзаплаха финансовите субекти информират, когато е приложимо, клиентите си, които са потенциално засегнати, за всички подходящи мерки за защита, които клиентите биха могли да предприемат.

4. В сроковете, които се определят в съответствие с член 20, първа алинея, буква а), точка ii), финансовите субекти предоставят на съответния компетентен орган следното:

а) първоначално уведомление;

б) неокончателен доклад след първоначалното уведомление по буква а), веднага след като статусът на първоначалния инцидент се промени значително или справянето със съществения инцидент с ИКТ се промени въз основа на нова налична информация, 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, и когато са налице действителните стойности на въздействието, с които могат да се заместят прогнозните.

5. Финансовите субекти могат, в съответствие с правото на Съюза и националното секторно право, да възлагат на трета страна доставчик на услуги посочените в настоящия член задължения за докладване. В случаите на такова възлагане на задължения финансовият субект остава изцяло отговорен за изпълнението на изискванията за докладване на инциденти.

6. При получаване на първоначалното уведомление и на всеки доклад по параграф 4 компетентният орган своевременно предоставя подробна информация за съществения инцидент с ИКТ на следните получатели, според случая, въз основа на съответните им компетенции:

а) ЕБО, ЕОЦКП или ЕОЗППО;

б) ЕЦБ, когато става въпрос за финансовите субекти по член 2, параграф 1, букви а), б) и г);

в) компетентните органи, единните звена за контакт или ЕРИКС, определени или установени в съответствие с Директива (ЕС) 2022/2555;

г) органите за преструктуриране, посочени в член 3 от Директива 2014/59/ЕС, и Единния съвет за преструктуриране (ЕСП) по отношение на субектите, посочени в член 7, параграф 2 от Регламент (ЕС) № 806/2014 на Европейския парламент и на Съвета ([37]), и по отношение на субектите и групите, посочени в член 7, параграф 4, буква б) и параграф 5 от Регламент (ЕС) № 806/2014, ако тази подробна информация се отнася до инциденти, които представляват риск за осигуряването на критични функции по смисъла на член 2, параграф 1, точка 35 от Директива 2014/59/ЕС; и

д) други имащи отношение публични органи съгласно националното право.

7. След получаване на информацията в съответствие с параграф 6 ЕБО, ЕОЦКП или ЕОЗППО, както и ЕЦБ, в консултации с ENISA и в сътрудничество със съответния компетентен орган, оценяват доколко съществениият инцидент с ИКТ е от значение за компетентните органи в други държави членки. След тази оценка ЕБО, ЕОЦКП или ЕОЗППО уведомяват възможно най-бързо съответните компетентни органи в други държави членки за това. 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.

([37]) Регламент (ЕС) № 806/2014 на Европейския парламент и на Съвета от 15 юли 2014 г. за установяването на еднообразни правила и еднообразна процедура за преструктурирането на кредитни институции и някои инвестиционни посредници в рамките на Единния механизъм за преструктуриране и Единния фонд за преструктуриране и за изменение на Регламент (ЕС) № 1093/2010 (ОВ L 225, 30.7.2014 г., стр. 1).

8. Уведомяването, което ЕОЦКП трябва да извърши съгласно параграф 7 от настоящия член, не засяга отговорността на компетентния орган спешно да предаде на съответния орган в приемащата държава членка подробна информация за сериозния инцидент с ИКТ, когато централен депозитар на ценни книжа извършва значителна трансгранична дейност в приемащата държава членка, сериозният инцидент с ИКТ има вероятност да окаже сериозни последици за финансовите пазари на приемащата държава членка и когато между компетентните органи има договорености за сътрудничество във връзка с надзора върху финансовите субекти.

Член 20

Хармонизиране на съдържанието и на образците за докладване

В рамките на съвместния комитет и в консултации с ЕЦБ и ENISA ЕНО разработват:

а) общи проекти на регулаторни технически стандарти:

i) за установяване на съдържанието на докладите за съществени инциденти с ИКТ, за да се отразят критериите по член 18, параграф 1 и да се включат допълнителни елементи, като например подробна информация за установяване на значението на докладването за други държави членки и дали инцидентът представлява или не съществен операционен или свързан със сигурността инцидент, свързан с плащания;

ii) за определяне на сроковете за първоначалното уведомление и за всеки доклад по член 19, параграф 4;

iii) за установяване на съдържанието на уведомлението за значителни киберзаплахи.

При разработването на тези проекти на регулаторни технически стандарти ЕНО вземат предвид размера и цялостния рисков профил на финансовите субекти и естеството, мащаба и сложността на техните услуги, дейности и операции, и по-специално с цел да се гарантира, че за целите на настоящия параграф, буква а), точка ii) различните срокове могат да отразяват, когато е целесъобразно, особеностите на финансовите сектори, без да се засяга поддържането на последователен подход към докладването на инциденти с ИКТ съгласно настоящия регламент и Директива (ЕС) 2022/2555. Ако е приложимо, ЕНО предоставят обосновка, когато се отклоняват от подходите, възприети в контекста на посочената директива;

б) общи проекти на технически стандарти за изпълнение за установяване на стандартните формуляри, образци и процедури, с които финансовите субекти да докладват за съществени инциденти с ИКТ и да уведомяват за значителни киберзаплахи.

ЕНО предават на Комисията общите проекти на регулаторни технически стандарти, посочени в първа алинея, буква а) и общите проекти на технически стандарти за изпълнение по първи параграф, буква б) до 17 юли 2024 г.

На Комисията се делегират правомощия да допълни настоящия регламент, като приеме посочените в първа алинея, буква а) общи регулаторни технически стандарти в съответствие с членове 10—14 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

На Комисията се предоставя правомощието да приеме посочените в първа алинея, буква б) общи технически стандарти за изпълнение в съответствие с член 15 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

Член 21

Централизиране на докладването за съществени инциденти с ИКТ

1. В рамките на съвместния комитет и в консултации с ЕЦБ и ENISA ЕНО изготвят съвместен доклад за оценка на осъществимостта на допълнително централизиране на уведомяването за инциденти чрез създаването на единен портал на ЕС за уведомяване от финансовите субекти за съществените инциденти с ИКТ. В съвместния доклад се проучват начините за улесняване на докладването за инциденти 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. Съвместният доклад по параграф 1 съдържа като минимум следните елементи:

а) предварителните условия за създаването на единен портал на ЕС;

б) ползата, ограниченията и рисковете, включително рисковете, свързани с високата концентрация на чувствителна информация;

в) необходимия капацитет за осигуряване на оперативна съвместимост с други съответни схеми за докладване;

г) елементите на оперативното управление;

д) условията за членство;

е) техническите договорености за достъп на финансовите субекти и националните компетентни органи до единния портал на ЕС;

ж) предварителна оценка на финансовите разходи за създаването на оперативната платформа на единния портал на ЕС, включително за необходимия експертен опит.

3. ЕНО предават на Европейския парламент, Съвета и Комисията доклада по параграф 1 до 17 януари 2025 г.

Член 22

Обратна информация от надзорните органи

1. Независимо от техническите данни, съвети или корективни мерки и последващото проследяване, които могат да бъдат предоставени, когато е приложимо и в съответствие с националното право, от ЕРИКС съгласно Директива (ЕС) 2022/2555, при получаване на първоначалното уведомление и на всеки доклад по член 19, параграф 4 компетентният орган потвърждава получаването и, когато е осъществимо, може своевременно да предостави подходяща и пропорционална обратна информация или указания на високо равнище на финансовия субект, по-специално като предостави всякаква относима анонимизирана информация и разузнавателни сведения за сходни заплахи, и може да обсъди коригиращите мерки, прилагани на равнището на финансовия субект, и начините за свеждане до минимум и за смекчаване на неблагоприятното въздействие в целия финансов сектор. Независимо от предоставената от надзорните органи обратна информация, финансовите субекти остават изцяло отговорни за справянето с инцидентите с ИКТ, докладвани съгласно член 19, параграф 1, и за последиците от тях.

2. ЕНО докладват ежегодно, чрез съвместния комитет, като се опират на анонимизирани и обобщени данни, за съществените инциденти с ИКТ, за които в съответствие с член 19, параграф 6 компетентните органи предоставят подробна информация, като посочват най-малкото броя на съществените инциденти с ИКТ, техния характер, последиците за операциите на финансовите субекти или на клиентите, предприетите коригиращи мерки и направените разходи.

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

Член 23

Операционни или свързани със сигурността инциденти, свързани с плащания, засягащи кредитни институции, платежни институции, доставчици на услуги по предоставяне на информация за сметка и институции за електронни пари

Изискванията, посочени в настоящата глава, се прилагат и по отношение на операционните или свързаните със сигурността инциденти, свързани с плащания, както и по отношение на съществените операционни или свързани със сигурността инциденти, свързани с плащания, когато те засягат кредитни институции, платежни институции, доставчици на услуги по предоставяне на информация за сметка и институции за електронни пари.

ГЛАВА IV

Тестване на оперативната устойчивост на цифровите технологии

Член 24

Общи изисквания за тестването на оперативната устойчивост на цифровите технологии

1. С цел да оценят доколко са подготвени за справяне с инциденти с ИКТ, да установят слабостите, недостатъците и пропуските в оперативната устойчивост на цифровите технологии, както и с оглед на бързото прилагане на корективни мерки, като вземат предвид критериите, посочени в член 4, параграф 2, финансовите субекти, без микропредприятията, въвеждат, поддържат и актуализират стабилна и всеобхватна програма за тестване на оперативната устойчивост на цифровите технологии като неразделна част от рамката за управление на риска в областта на ИКТ, посочена в член 6.

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 членове 25 и 26.

3. Когато изпълняват посочената в параграф 1 от настоящия член програма за тестване на оперативната устойчивост на цифровите технологии, финансовите субекти, без микропредприятията, следват подход, при който се отчита рискът, като вземат предвид определените в член 4, параграф 2 критерии и като надлежно отчитат променливото естество на рисковете в областта на ИКТ, специфичните рискове, на които съответният финансов субект е или би могъл да бъде изложен, критичността на информационните активи и на предоставяните услуги, както и всеки друг фактор, който финансовият субект счете за подходящ.

4. Финансовите субекти, без микропредприятията, гарантират, че тестването се извършва от независими страни — вътрешни или външни. Когато тестовете се извършват от вътрешно лице, провеждащо тестове, финансовите субекти отделят достатъчно ресурси и гарантират, че конфликтите на интереси се избягват по време на етапите на проектиране и изпълнение на теста.

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

6. Финансовите субекти, без микропредприятията, гарантират извършването най-малко веднъж годишно на подходящи тестове за всички системи и приложения на ИКТ, поддържащи критични или важни функции.

Член 25

Тестване на инструментите и системите на ИКТ

1. Посочената в член 24 програма за тестване на оперативната устойчивост на цифровите технологии предвижда, в съответствие с критериите, посочени в член 4, параграф 2, провеждането на подходящи тестове, като например оценки и сканиране на уязвимите места, анализ на приложенията с отворен код, оценки на сигурността на мрежата, анализ на пропуските, преглед на физическата сигурност, анкети и сканиране на програмните продукти, преглед на първичния код, когато такъв е осъществим, тестване на различни сценарии, тестване на съвместимостта, тестване на функционирането, тестване по цялата верига и тестване за проникване.

2. Централните депозитари на ценни книжа и централните контрагенти извършват оценки на уязвимите места преди внедряване или вторично внедряване на нови или съществуващи приложения и инфраструктурни компоненти и на услуги в областта на ИКТ, поддържащи критични или важни функции на финансовия субект.

3. Микропредприятията извършват тестовете, посочени в параграф 1, като съчетават подход, при който се отчита рискът, със стратегическо планиране на тестването на ИКТ, като надлежно отчитат необходимостта от намиране на балансиран подход между мащаба на ресурсите и времето, което трябва да бъде отделено за тестването на ИКТ, предвидено в настоящия член, от една страна, и неотложността, вида на риска, критичността на информационните активи и на предоставяните услуги, както и всеки друг фактор от значение, включително способността на финансовия субект да поема премерени рискове, от друга страна.

Член 26

Обстойно тестване на инструментите, системите и процесите на ИКТ чрез тестване за проникване

1. Финансовите субекти, различни от субектите, посочени в член 16, параграф 1, първа алинея и от микропредприятията, които са идентифицирани в съответствие с параграф 8, трета алинея от настоящия член, провеждат най-малко веднъж на 3 години обстойно тестване посредством тестване за проникване. Въз основа на рисковия профил на финансовия субект и предвид оперативните обстоятелства компетентният орган може, когато е необходимо, да поиска от финансовия субект да намали или увеличи тази честота.

2. Всяко тестване за проникване включва няколко или всички критични или важни функции на финансовия субект, като се тестват оперативните производствени системи, поддържащи тези функции.

Финансовите субекти идентифицират всички относими основни системи, процеси и технологии в областта на ИКТ, които поддържат критични или важни функции, както и услугите в областта на ИКТ, включително такива, поддържащи критични или важни функции, които са възложени на външен изпълнител или с договор на трети страни доставчици на услуги в областта на ИКТ.

Финансовите субекти оценяват кои критични или важни функции е необходимо да бъдат обхванати от тестването за проникване. Точният обхват на тестването за проникване се определя в зависимост от резултата от тази оценка и се валидира от компетентните органи.

3. Когато тестването за проникване обхваща трети страни доставчици на услуги в областта на ИКТ, финансовите субекти предприемат необходимите мерки и въвеждат предпазни механизми, за да гарантират участието в тестването за проникване на тези трети страни доставчици на услуги в областта на ИКТ, като във всеки един момент са изцяло отговорни за осигуряване на спазването на настоящия регламент.

4. Без да се засягат разпоредбите на параграф 2, първа и втора алинея, когато има разумни основания да се очаква, че участието в тестването за проникване на трета страна доставчик на услуги в областта на ИКТ, посочено в параграф 3, ще се отрази неблагоприятно на качеството или сигурността на услугите, предоставяни от третата страна доставчик на услуги в областта на ИКТ на клиенти, които са субекти извън обхвата на настоящия регламент, или на поверителността на данните, свързани с тези услуги, финансовият субект и третата страна доставчик на услуги в областта на ИКТ може да се договорят писмено третата страна доставчик на услуги в областта на ИКТ да сключи директно договорно споразумение с външно лице, провеждащо тестове, за целите на провеждането, под ръководството на определен финансов субект, на съвкупно тестване за проникване, включващо няколко финансови субекта (съвкупно тестване), на които третата страна доставчик на услуги в областта на ИКТ предоставя услуги.

Съвкупното тестване обхваща съответната гама услуги в областта на ИКТ, поддържащи критичните или важните функции, възложени с договор от финансовите субекти на съответната трета страна доставчик на услуги в областта на ИКТ. Съвкупното тестване се счита за тестване за проникване, извършено от финансовите субекти, участващи в съвкупното тестване.

Броят на финансовите субекти, участващи в съвкупното тестване, се планира внимателно предвид сложността и вида на обхванатите услуги.

5. Финансовите субекти, в сътрудничество с третите страни доставчици на услуги в областта на ИКТ и другите участващи страни, включително лицата, провеждащи тестове, но без компетентните органи, упражняват ефективни контролни функции при управлението на риска, за да се смекчи рискът за самите тях, за техните контрагенти или за финансовия сектор от потенциално отражение върху данните, увреждане на активите и смущения във критичните или важните функции, услуги или операции.

6. Когато тестването приключи и бъдат приети докладите и плановете за корективни мерки, финансовият субект и, когато е приложимо, външните лица, провели тестовете, предоставят на определения съгласно параграф 9 или 10 орган обобщение на констатациите, плановете за корективни мерки и документацията, която доказва, че тестването за проникване е било проведено в съответствие с изискванията.

7. Органите издават на финансовите субекти удостоверение, с което потвърждават, че тестването е извършено в съответствие с изискванията, посочени в документацията, за да се даде възможност за взаимно признаване от компетентните органи на резултатите от тестването за проникване. Финансовият субект уведомява съответния компетентен орган за удостоверението, обобщението на съответните констатации и плановете за корективни мерки.

Без да се засяга това удостоверяване, финансовите субекти във всеки един момент са изцяло отговорни за въздействието на тестовете, посочени в параграф 4.

8. Финансовите субекти наемат лица за извършване на тестването за целите на тестването за проникване в съответствие с член 27. Когато финансовите субекти използват вътрешни лица, провеждащи тестовете, за целите на извършването на тестване за проникване, те наемат външни лица, провеждащи тестове, на всеки три теста.

Кредитните институции, класифицирани като значими в съответствие с член 6, параграф 4 от Регламент (ЕС) № 1024/2013, използват само външни лица, провеждащи тестове, в съответствие с член 27, параграф 1, букви а)—д).

Компетентните органи определят финансовите субекти, от които се изисква да извършват тестване за проникване, като вземат предвид критериите, посочени в член 4, параграф 2, въз основа на оценка на следното:

а) фактори за въздействието, по-специално до каква степен предоставяните от финансовия субект услуги и предприеманите от него дейности оказват въздействие върху финансовия сектор;

б) евентуални опасения за финансовата стабилност, включително системния характер на финансовия субект на равнището на Съюза или на национално равнище, доколкото е приложимо;

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

9. Държавите членки може да определят единен публичен орган във финансовия сектор, който да отговаря на национално равнище за свързаните с тестването за проникване въпроси във финансовия сектор, и му възлагат всички правомощия и задачи за тази цел.

10. Ако няма определен орган в съответствие с параграф 9 от настоящия член и без да се засяга правомощието за определяне на финансовите субекти, които са задължени да извършват тестване за проникване, компетентният орган може да делегира изпълнението на някои или на всички задачи, посочени в настоящия член и член 27, на друг национален орган във финансовия сектор.

11. Съгласувано с ЕЦБ ЕНО разработват съвместни проекти за регулаторни технически стандарти съгласно рамката TIBER-EU за доуточняване на:

а) използваните критерии за целите на прилагането на параграф 8, втора алинея;

б) изискванията и стандартите, уреждащи използването на вътрешни лица, провеждащи тестове;

в) изискванията във връзка със:

i) обхвата на тестването за проникване, посочен в параграф 2;

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

iii) резултатите, приключването на процеса и коригиращите мерки;

г) вида на необходимото сътрудничество за надзорни и други цели с оглед на изпълнението на тестването за проникване, както и за улесняване на взаимното признаване на тестването, при финансовите субекти 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.

При разработването на тези проекти на регулаторни технически стандарти ЕНО надлежно отчитат всяка специфична характеристика, произтичаща от различното естество на дейностите в различните сектори на финансовите услуги.

ЕНО представят тези проекти на регулаторни технически стандарти на Комисията до 17 юли 2024 г.

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

Член 27

Изисквания към лицата, провеждащи тестване за проникване

1. За провеждането на тестване за проникване финансовите субекти използват само 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 разузнавателните сведения за заплахи, тестването за проникване и тестването на защитните механизми при симулиране на реални условия (червен екип);

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

г) предоставят независима гаранция или одитен доклад за доброто управление на рисковете, свързани с провеждането на тестване за проникване, включително подходяща защита на поверителната информация на финансовия субект и средства за правна защита във връзка с рисковете за дейността на финансовия субект;

д) разполагат с надлежно и цялостно застрахователно покритие за професионална отговорност, включително срещу риска от неправомерно поведение и небрежност.

2. При използване на вътрешни лица, провеждащи тестове, финансовите субекти гарантират, че наред с изискванията по параграф 1, са изпълнени и следните условия:

а) такова използване е одобрено от съответния компетентен орган или от единния публичен орган, определен в съответствие с член 26, параграфи 9 и 10;

б) съответният компетентен орган се е уверил, че финансовият субект отделя достатъчно ресурси и гарантира, че конфликтите на интереси се избягват по време на етапите на проектиране и изпълнение на теста; и

в) доставчикът на разузнавателни сведения за заплахи е външно лице спрямо финансовия субект.

3. Финансовите субекти гарантират, че в договорите, сключени с външни лица, провеждащи тестове, се изисква добро управление на резултатите от тестването за проникване, и че обработването на данни въз основа на тях, включително всякакво генериране, съхраняване, обобщаване, описване, докладване, съобщаване или унищожаване, не поражда рискове за финансовия субект.

ГЛАВА V

Управление на риска в областта на ИКТ, пораждан от трети страни

Раздел I

Основни принципи за добро управление на риска в областта на ИКТ, пораждан от трети страни

Член 28

Общи принципи

1. Финансовите субекти управляват риска в областта на ИКТ, пораждан от трети страни като неразделна част от компонента „риск в областта на ИКТ“ на своята рамка за управление на риска в областта на ИКТ, както е посочено в член 6, параграф 1 и съобразно следните принципи:

а) финансовите субекти, които с оглед на стопанската си дейност са сключили договорни споразумения 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 право в областта на финансовите услуги, както и за преценката, че тези задължения са изпълнени;

б) финансовите субекти управляват риска в областта на ИКТ, пораждан от трети страни, съобразно принципа на пропорционалност, като вземат предвид:

i) естеството, мащаба, сложността и значението на зависимостите във връзка с ИКТ,

ii) рисковете, свързани с договорните споразумения за услуги в областта на ИКТ, сключени с трети страни доставчици на услуги в областта на ИКТ, като отчитат критичния или важен характер на съответната услуга, процес или функция, както и потенциалното въздействие на тези рискове върху непрекъснатостта и наличността на финансовите услуги и дейности на равнището на отделния субект и на групата.

2. Като част от своята рамка за управление на риска в областта на ИКТ финансовите субекти, различни от субектите, посочени в член 16, параграф 1, първа алинея, и от микропредприятията, приемат и редовно преразглеждат стратегия за риска в областта на ИКТ, пораждан от трети страни, като вземат предвид, когато е приложимо, стратегията за прибягване до множество доставчици, посочена в член 6, параграф 9. Стратегията за риска в областта на ИКТ, пораждан от трети страни включва политика за използването на услуги в областта на ИКТ, поддържащи критичните или важните функции, предоставяни от трети страни доставчици на такива услуги, и се прилага както на индивидуална основа, така и, според случая, на подконсолидирана и консолидирана основа. Въз основа на оценка на цялостния рисков профил на финансовия субект и на мащаба и сложността на бизнес услугите ръководният орган редовно прави преглед на идентифицираните рискове по отношение на договорни споразумения за използване на услуги в областта на ИКТ, поддържащи критични или важни функции.

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

Договорните споразумения по първа алинея се документират по подходящ начин, като тези, които се отнасят до услуги на ИКТ в подкрепа на критични или важни функции, се обособяват от останалите.

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

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 сключат договорно споразумение за услуги в областта на ИКТ, поддържащи критични или важни функции, както и когато дадена функция се е превърнала в критична или важна.

4. Преди да сключат договорно споразумение за услуги в областта на ИКТ финансовите субекти:

а) преценяват дали договорното споразумение се отнася до услуги в областта на ИКТ, поддържащи критична или важна функция;

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

в) идентифицират и оценяват всички съответни рискове, свързани с договорното споразумение, включително вероятността такова договорно споразумение допринесе за засилване на риска от концентрация в областта на ИКТ, както е посочено в член 29;

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

д) идентифицират и оценяват конфликтите на интереси, които договорното споразумение може да породи.

5. Финансовите субекти могат да сключват договорни споразумения само с трети страни доставчици на услуги в областта на ИКТ, които удовлетворяват подходящи стандарти за сигурност на информацията. Когато договорното споразумение се отнася до критични или важни функции, преди сключването му финансовите субекти надлежно отчитат използването от третите страни доставчици на услуги в областта на ИКТ на най-актуалните и висококачествени стандарти за сигурност на информацията.

6. Когато упражняват правата си за достъп, проверка и одит на дадена трета страна доставчик 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 договорните споразумения с третите страни доставчици на услуги в областта на ИКТ, които съдържат технически аспекти със значителна сложност, финансовите субекти се уверяват, че одиторите — независимо дали са вътрешни или външни или са група от одитори, притежават подходящите знания и умения, за да извършат ефективно съответните одити и оценки.

7. Финансовите субекти правят необходимото, за да гарантират, че договорните споразумения за ползването на услуги в областта на ИКТ могат да бъдат прекратени при всяко от следните обстоятелства:

а) при съществено нарушение на приложимите законови или подзаконови актове или на разпоредбите на договора, извършено от третата страна доставчик на услуги в областта на ИКТ;

б) при наличието на обстоятелства, установени при наблюдението на риска в областта на ИКТ, пораждан от трета страна, за които се смята, че могат да променят изпълнението на предоставяните по силата на договорното споразумение функции, включително съществени промени, които засягат договора или положението на третата страна доставчик на услуги в областта на ИКТ;

в) ако са налице свидетелства за слабости в цялостното управление на риска в областта на ИКТ от третата страна доставчик на услуги в областта на ИКТ, и по-специално в начина, по който той осигурява наличността, автентичността, цялостността и поверителността на данните, независимо дали става въпрос за лични данни, други чувствителни данни, или за данни, които не са от личен характер;

г) ако условията на съответното договорно споразумение или свързани с него обстоятелства не позволяват на компетентния орган да продължи да упражнява ефективен надзор върху финансовия субект.

8. За услуги в областта на ИКТ, поддържащи критични или важни функции, финансовите субекти въвеждат изходни стратегии. В изходните стратегии се отчитат рисковете, които могат да възникнат при дадена трета страна доставчик на услуги в областта на ИКТ — прекратяване на дейността, влошаване на качеството на предоставяните услуги в областта на ИКТ, смущения в дейността на финансовия субект поради неподходящо или неуспешно предоставяне на услуги в областта на ИКТ, възникване на съществен риск, свързан с подходящото и непрекъснатото изпълнение на съответната услуга в областта на ИКТ, или прекратяване на договорните споразумения с трети страни доставчици на услуги в областта на ИКТ — при някое от обстоятелствата, изброени в параграф 7.

Финансовите субекти се уверяват, че могат да прекратят всяко договорно споразумение, без това:

а) да прекъсне стопанската им дейност,

б) да ограничи спазването на регулаторните изисквания;

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

Изходните планове са изчерпателни, документирани и, в съответствие с критериите, посочени в член 4, параграф 2, достатъчно се тестват и периодично се подлагат на преглед.

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

Финансовите субекти въвеждат подходящи мерки за действие при извънредни ситуации, за да осигурят непрекъснатост на дейността при възникване на обстоятелствата, посочени в първа алинея.

9. В рамките на съвместния комитет ЕНО разработват проекти на технически стандарти за изпълнение за определяне на стандартните образци за целите на регистъра на информацията по параграф 3, включително на информацията, която е обща за всички договорни споразумения за услуги в областта на ИКТ. ЕНО представят тези проекти на технически стандарти за изпълнение на Комисията до 17 януари 2024 г.

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

10. ЕНО разработват чрез съвместния комитет проекти на регулаторни технически стандарти за доуточняване на подробното съдържание на посочената в параграф 2 политика по отношение на договорните споразумения за услуги в областта на ИКТ, поддържащи критични или важни функции, предоставяни от трети страни доставчици на услуги в областта на ИКТ.

Когато разработват тези проекти на регулаторни технически стандарти, ЕНО вземат предвид размера на финансовите субекти, цялостния им рисков профил, както и естеството, мащаба и сложността на техните услуги, дейности и операции. ЕНО представят тези проекти на регулаторни технически стандарти на Комисията до 17 януари 2024 г.

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

Член 29

Предварителна оценка на риска от концентрация на ИКТ на равнището на субектите

1. При идентифицирането и оценяването на риска от концентрация на ИКТ, посочен в член 28, параграф 4, буква в), финансовите субекти преценяват също дали предвижданото договорно споразумение за услуги в областта на ИКТ, подпомагащи критични или важни функции, би довело при сключването си до някое от следните последствия:

а) договор с трета страна доставчик на услуги в областта на ИКТ, която не може да бъде лесно заменена; или

б) множество договорни споразумения за услуги в областта на ИКТ, подпомагащи критични или важни функции, сключени с една и съща трета страна доставчик на такива услуги или с тясно взаимосвързани трети страни доставчици на такива услуги.

Финансовите субекти проучват разходите и ползите от алтернативни решения — например прибягване до различни трети страни доставчици 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 договорните споразумения за ползване на услуги в областта на ИКТ, поддържащи критични или важни функции, позволяват на третата страна доставчик на такива услуги да възлага на свой ред услуги в областта на ИКТ, поддържащи критични или важни функции, на други подизпълнители, които са трета страна доставчик на услуги в областта на ИКТ, финансовите субекти преценяват потенциалните ползи и рискове от такова възлагане на подизпълнители, особено когато поддоставчикът на ИКТ е установен в трета държава.

Когато договорното споразумение е за услуги в областта на ИКТ, поддържащи критични или важни функции, финансовите субекти надлежно вземат предвид приложимите правни норми при несъстоятелност на третата страна доставчик на услуги в областта на ИКТ, както и евентуалните ограничения, ако спешно им се наложи да получат обратно данните си от въпросния доставчик.

Когато договорното споразумение за услуги в областта на ИКТ, поддържащи критични или важни функции, е сключено с трета страна доставчик на услуги в областта на ИКТ, установена в трета държава, финансовите субекти, в допълнение към съображенията, посочени във втора алинея, вземат предвид също така съблюдаването на правилата на Съюза за защита на личните данни и ефективното прилагане на правото във въпросната трета държава.

Когато в договорното споразумение за услуги в областта на ИКТ, поддържащи критични или важни функции, е предвидено възлагане на дейностите на подизпълнители, 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 това отношение.

Член 30

Основни договорни клаузи

1. Правата и задълженията на финансовия субект и на третата страна доставчик на услуги в областта на ИКТ се определят ясно и се посочват в писмен вид. Пълният текст на договора включва клаузи за нивото на обслужване и се оформя в писмен документ, който е на разположение на страните на хартиен носител, или в документ с друг траен и достъпен формат, който позволява документът да бъде изтеглен.

2. Договорните споразумения за услуги в областта на ИКТ съдържат най-малко следните елементи:

а) ясно и пълно описание на всички функции и услуги в областта на ИКТ, които третата страна доставчик на услуги в областта на ИКТ трябва да предостави, като се посочва дали се позволява възлагане на подизпълнители на услуга в областта на ИКТ, поддържаща критична или важна функция, или на съществени части от нея, както и, ако такава възможност е предвидена, приложимите условия при такова възлагане на подизпълнители;

б) местата, а именно регионите или държавите, където трябва да бъдат предоставяни договорно възложените функции и услуги в областта на ИКТ или тези, възложени на подизпълнители, както и мястото, на което трябва да бъдат обработвани данните, включително мястото им на съхранение, както и изискването към третата страна доставчик на услуги в областта на ИКТ да уведоми предварително финансовия субект, ако възнамерява да промени тези места;

в) разпоредби относно наличността, автентичността, цялостността и поверителността във връзка със защитата на данните, включително личните данни;

г) разпоредби 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 третата страна доставчик на услуги в областта на ИКТ, или в случай на прекратяване на договорното споразумение;

д) описание на нивото на обслужване, включително на актуализиране и преглед на предоставяните услуги;

е) задължението на третата страна доставчик на услуги в областта на ИКТ да предоставя помощ на финансовия субект без допълнителни разходи или на предварително определена цена, когато възникне инцидент с ИКТ, свързан с предоставяната на финансовия субект услуга в областта на ИКТ;

ж) задължението на третата страна доставчик на услуги в областта на ИКТ да оказва пълно съдействие на компетентните органи и на органите за преструктуриране на финансовия субект, включително и на лицата, назначени от тях;

з) правото на прекратяване на договорните споразумения и свързаните с него минимални срокове за предизвестие — съобразно очакванията на компетентните органи и органите за преструктуриране;

и) условията за участие на третите страни доставчици на услуги в областта на ИКТ в програмите на финансовите субекти за повишаване на осведомеността относно сигурността на ИКТ и в обучението по оперативна устойчивост на цифровите технологии в съответствие с член 13, параграф 6.

3. В допълнение към елементите, посочени в параграф 2, договорните споразумения за услуги в областта на ИКТ, поддържащи критични или важни функции, включват най-малко следното:

а) обстойно описание на нивото на обслужване, включително на актуализиране и преглед на предоставяните услуги, с точни количествени и качествени цели за ефективност в рамките на договореното ниво на обслужване, така че финансовият субект да може ефективно да следи риска в областта на ИКТ, пораждан от трети страни и да предприеме възможно най-бързо подходящите корективни мерки, ако договореното ниво на обслужване не се спазва;

б) задълженията на третата страна доставчик на услуги в областта на ИКТ да докладва на финансовия субект, както и съответните срокове за това, включително задължението да го уведомява за всяко обстоятелство, което би могло да засегне съществено способността на третата страна доставчик на услуги в областта на ИКТ да предоставя ефективно услуги в областта на ИКТ или да изпълнява ефективно критични или важни функции в съответствие с договореното ниво на обслужване;

в) изисквания към третата страна доставчик на услуги в областта на ИКТ да прилага и тества планове за действие при извънредни ситуации, както и да разполага с мерки, инструменти и политики за сигурност на ИКТ, които осигуряват подходящо ниво на сигурност за предоставянето на услуги от финансовия субект, както е предвидено в отнасящата се до него нормативна уредба;

г) задължението на третата страна доставчик на услуги в областта на ИКТ да участва и да оказва пълно съдействие при тестването за проникване на финансовия субект, както е посочено в членове 26 и 27;

д) правото на финансовия субект текущо да наблюдава ефективността на третата страна доставчик на услуги в областта на ИКТ, което включва:

i) неограничено право на достъп, проверка и одит от страна на финансовия субект или определена за целта трета страна, както и от страна на компетентния орган, а също и право да бъдат взети копия на съответната документация на място, ако тя е от ключово значение за операциите на третата страна доставчик на услуги в областта на ИКТ, като други договорни споразумения или политики за изпълнение не възпрепятстват, нито ограничават ефективното упражняване на това право;

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

iii) ангажимента от страна на третата страна доставчик на услуги в областта на ИКТ да сътрудничи изцяло при проверките и одитите на място, извършвани от компетентните органи, водещия надзорник, финансовия субект или от определена за целта трета страна; и

iv) задължението да предоставя подробна информация относно обхвата, процедурите, които трябва да бъдат следвани, и честотата на такива проверки и одити;

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

i) по време на който третата страна доставчик на услуги в областта на ИКТ продължава да предоставя съответните функции или услуги в областта на ИКТ с цел да се ограничи рискът за финансовия субект от смущение в дейността или да се гарантира ефективната му реорганизация или преструктуриране;

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

Чрез дерогация от буква д) третата страна доставчик на услуги в областта на ИКТ и финансовият субект, който е микропредприятие, може да се споразумеят, че правата на финансовия субект на достъп, проверка и одит може да бъдат делегирани на независима трета страна, определена от третата страна доставчик на услуги в областта на ИКТ, както и че финансовият субект може да поиска във всеки един момент информация и гаранции относно резултатите от дейността на третата страна доставчик на услуги в областта на ИКТ.

4. Когато се договарят, финансовите субекти и третите страни доставчици на услуги в областта на ИКТ обмислят използването на стандартни договорни клаузи, разработени от публични органи, за конкретни услуги.

5. ЕНО разработват чрез съвместния комитет проекти на регулаторни технически стандарти с цел доуточняване на елементите, посочени в параграф 2, буква а), които финансовият субект трябва да определи и оцени, когато възлага на подизпълнители услуги в областта на ИКТ, поддържащи критични или важни функции.

Когато разработват тези проекти на регулаторни технически стандарти, ЕНО вземат предвид размера на финансовите субекти, цялостния им рисков профил, както и естеството, мащаба и сложността на техните услуги, дейности и операции.

ЕНО представят тези проекти на регулаторни технически стандарти на Комисията до 17 юли 2024 г.

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

Раздел II

Надзорна рамка за трети страни критични доставчици на услуги в областта на ИКТ

Член 31

Определяне на третите страни критични доставчици на услуги в областта на ИКТ

1. В рамките на съвместния си комитет и по препоръка на създадения с член 32, параграф 1 надзорен форум ЕНО:

а) определят след оценка, при която се вземат под внимание посочените в параграф 2 критерии, критичните за финансовите субекти трети страни доставчици на услуги в областта на ИКТ;

б) определят за водещ надзорник на всяка от третите страни критични доставчици на услуги в областта на ИКТ отговорния ЕНО в съответствие с регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 или (ЕС) № 1095/2010 за финансовите субекти, които съвместно притежават най-големия дял от общите активи спрямо стойността на общите активи на всички финансови субекти, използващи услугите на съответната трета страна критичен доставчик на услуги в областта на ИКТ, в съответствие със сбора на отделните счетоводни баланси на тези финансови субекти.

2. Определянето по параграф 1, буква а) се основава на всеки от следните критерии във връзка с услугите в областта на ИКТ, предоставяни от трета страна доставчик на услуги в областта на ИКТ:

а) системното въздействие върху стабилността, непрекъснатостта или качеството на предоставяните финансови услуги, в случай че дадена трета страна доставчик на услуги в областта на ИКТ бъде изправена пред мащабна оперативна неспособност да предоставя услугите си — предвид броя финансови субекти, които се ползват от услугите ѝ, и общата стойност на техните активи;

б) системния характер или значение на финансовите субекти, които обслужва дадената трета страна доставчик 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 съответната трета страна доставчик на услуги в областта на ИКТ;

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

в) степента, в която критичните или важните функции на даден финансов субект зависят от услугите, предоставяни от една и съща трета страна доставчик на услуги в областта на ИКТ, без значение дали тази зависимост е пряка, непряка или възникнала поради възлагане на услугите на подизпълнители услуги;

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

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

ii) трудности по отношение на частичното или пълно прехвърляне на съответните данни и работно натоварване от дадената трета страна доставчик на услуги в областта на ИКТ към друга трета страна 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 риска в областта на ИКТ или на други операционни рискове за финансовия субект.

3. Когато третата страна доставчик на услуги в областта на ИКТ е част от група, посочените в параграф 2 критерии се вземат под внимание по отношение на услугите в областта на ИКТ, предоставяни от групата като цяло.

4. Третите страни критични доставчици на услуги в областта на ИКТ и са част от група, определят едно юридическо лице като координационно звено, което да осигурява подходящо представителство и комуникация с водещия надзорник.

5. Водещият надзорник уведомява третата страна доставчик на услуги в областта на ИКТ за резултатите от оценката за целите на определянето, посочено в параграф 1, буква а). В срок от 6 седмици от датата на уведомлението третата страна доставчик на услуги в областта на ИКТ може да представи на водещия надзорник мотивирано становище с цялата необходима информация за целите на оценката. Водещият надзорник разглежда мотивираното становище и може да поиска да бъде представена допълнителна информация в срок от 30 календарни дни от получаването на такова становище.

След като определят дадена трета страна за критичен доставчик на услуги в областта на ИКТ, ЕНО, чрез съвместния комитет, уведомяват за това съответната трета страна доставчик на услуги в областта на ИКТ, като я информират и за началната дата, от която тя подлежи на надзор. Тази начална дата е не по-късно от един месец след уведомлението. Третата страна доставчик на услуги в областта на ИКТ уведомява финансовите субекти, на които предоставя услуги, че е определена за критичен доставчик.

6. На Комисията се предоставя правомощието да приеме делегиран акт в съответствие с член 57, за да допълни настоящия регламент, като доуточни критериите, посочени в параграф 2 от настоящия член, до 17 юли 2024 г.

7. Към определянето по параграф 1, буква а) се пристъпва само след като Комисията приеме делегиран акт съгласно параграф 6.

8. Определянето, посочено в параграф 1, буква а), не се прилага по отношение на:

i) финансови субекти, предоставящи услуги в областта на ИКТ на други финансови субекти;

ii) третите страни доставчици 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;

iii) вътрешногрупови доставчици на услуги в областта на ИКТ;

iv) трети страни доставчици на услуги в областта на ИКТ, които предоставят услуги в областта на ИКТ само в една държава членка на финансови субекти, които извършват дейност само в тази държава членка.

9. Чрез съвместния си комитет ЕНО съставят, публикуват и годишно актуализират списък на третите страни критични за Съюза доставчици на услуги в областта на ИКТ.

10. За целите на параграф 1, буква а) компетентните органи ежегодно и в обобщен вид предават на създадения с член 32 надзорен форум информацията, посочена в член 28, параграф 3, трета алинея. Въз основа на получената от компетентните органи информация надзорният форум оценява зависимостта на финансовите субекти от трети страни доставчици на услуги в областта на ИКТ.

11. Третите страни доставчици на услуги в областта на ИКТ, които не са включени в посочения в параграф 9 списък, могат да поискат да бъдат определени за критични в съответствие с параграф 1, буква а).

За целите на първа алинея съответната трета страна доставчик на услуги в областта на ИКТ подава до ЕБО, ЕОЦКП или ЕОЗППО обосновано заявление, а посочените органи решават в рамките на съвместния комитет дали да я определят за критичен доставчик в съответствие с параграф 1, буква а).

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

12. Финансовите субекти ползват услугите на трета страна доставчик на услуги в областта на ИКТ, която е определена за критичен доставчик в съответствие с параграф 1, буква а) само ако въпросната трета страна е регистрирала дъщерно предприятие в Съюза в рамките на 12 месеца след определянето.

13. Третата страна критичен доставчик на услуги в областта на ИКТ, посочена в параграф 12, уведомява водещия надзорник за всякакви промени в структурата на управление на дъщерното предприятие, регистрирано в Съюза.

Член 32

Структура на надзорната рамка

1. По силата на член 57, параграф 1 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010 съвместният комитет създава надзорен форум като свой подкомитет, който да подпомага неговата работа и тази на водещия надзорник, посочен в член 31, параграф 1, буква б), по въпросите на риска в областта на ИКТ, пораждан от трета страна за финансовите сектори. Надзорният форум подготвя проектите за съвместни позиции и проектите за общи актове на съвместния комитет в тази сфера.

В надзорния форум редовно се обсъждат съответните обстоятелства във връзка с риска в областта на ИКТ и с уязвимите места на ИКТ, като се насърчава последователен подход за наблюдаване на равнището на Съюза на риска в областта на ИКТ, пораждан от трети страни.

2. Надзорният форум ежегодно прави колективна оценка на резултатите и констатациите от надзорните действия, проведени за всички трети страни критични доставчици на услуги в областта на ИКТ, и насърчава координационни мерки за подобряване на оперативната устойчивост на цифровите технологии при финансовите субекти, за възприемане на най-добрите практики с оглед на риска от концентрация 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 третите страни критични доставчици на услуги в областта на ИКТ, които показатели съвместният комитет да приеме като съвместни позиции на ЕНО съгласно член 56, параграф 1 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

4. В състава на надзорния форум влизат:

а) председателите на ЕНО;

б) по един представител на високо равнище от настоящия персонал на съответния компетентен орган, посочен в член 46, от всяка държава членка;

в) изпълнителните директори на всеки ЕНО, както и по един представител от Комисията, от ЕССР, от ЕЦБ и от ENISA, като наблюдатели.

г) когато е целесъобразно, по един допълнителен представител на компетентен орган, посочен в член 46, от всяка държава членка като наблюдател;

д) ако е приложимо, по един представител на компетентните органи, определени или установени в съответствие с Директива (ЕС) 2022/2555, отговарящи за надзора на съществен или важен субект, попадащ в обхвата на посочената директива, който е определен за трета страна критичен доставчик на услуги в областта на ИКТ, като наблюдател.

Надзорният форум може, когато е целесъобразно, да потърси съвет от независими експерти, назначени в съответствие с параграф 6.

5. Всяка държава членка определя съответния компетентен орган, чийто член на персонала е представителят на високо равнище, посочен в параграф 4, първа алинея, буква б), и информира за това водещия надзорник.

ЕНО публикуват на уебсайта си списъка на представителите на високо равнище от настоящия персонал на съответния компетентен орган, определени от държавите членки.

6. Независимите експерти, посочени в параграф 4, втора алинея, се назначават от надзорния форум от група експерти, избрани след публичен и прозрачен процес на кандидатстване.

Независимите експерти се назначават въз основа на експертния им опит по въпросите на финансовата стабилност, оперативната устойчивост на цифровите технологии и по въпроси, свързани със сигурността на ИКТ. Те действат независимо и обективно единствено в интерес на Съюза като цяло, като нямат право да искат, нито да приемат указания от институциите или органите на Съюза, от правителства на държави членки или от други публични органи или частни организации.

7. В съответствие с член 16 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010, до 17 юли 2024 г. ЕНО издават за целите на настоящия раздел насоки за сътрудничеството между ЕНО и компетентните органи, които обхващат подробните процедури и условия за разпределение и изпълнение на задачите между компетентните органи и ЕНО, както и подробности относно обмена на информация, необходими на компетентните органи, за да се гарантира изпълнението на препоръките по член 35, параграф 1, буква г), отправени към трети страни критични доставчици на услуги в областта на ИКТ.

8. Изискванията в настоящия раздел не засягат прилагането на Директива (ЕС) 2022/2555, нито на другите надзорни норми на Съюза, приложими за доставчиците на компютърни услуги „в облак“.

9. ЕНО, чрез съвместния комитет и въз основа на подготвителната работа, извършена от надзорния форум, ежегодно представят на Европейския парламент, Съвета и Комисията доклад за прилагането на настоящия раздел.

Член 33

Задачи на водещия надзорник

1. Водещият надзорник, определен в съответствие с член 31, параграф 1, буква б), осъществява надзор над определените трети страни критични доставчици на услуги в областта на ИКТ, и за целите на всички въпроси, свързани с надзора, е основното звено за контакт за тези трети страни критични доставчици на услуги в областта на ИКТ.

2. За целите на параграф 1 водещият надзорник оценява дали всяка трета страна критичен доставчик на услуги в областта на ИКТ разполага с подробни, надеждни и ефективни правила, процедури, механизми и договорености за управление на риска в областта на ИКТ, който може да породи за финансовите субекти.

Оценката, посочена в първа алинея, е насочена главно към услугите в областта на ИКТ, предоставяни от третата страна критичен доставчик на услуги в областта на ИКТ, поддържащи критичните или важните функции на финансовите субекти. Когато е необходимо за справяне с всички съответни рискове, тази оценка обхваща и услуги в областта на ИКТ, поддържащи функции, които не са критични или важни.

3. Оценката, посочена в параграф 2, обхваща:

а) изискванията във връзка с ИКТ за гарантиране по-специално на сигурността, наличността, непрекъснатостта, капацитета за увеличаване и качеството на услугите, предоставяни на финансовите субекти от третата страна критичен доставчик на услуги в областта на ИКТ, както и способността неотклонно да се спазват високи стандарти за наличност, автентичност, цялостност или поверителност на данните;

б) физическата сигурност, която допринася за гарантиране на сигурността на ИКТ, включително сигурността на помещенията, оборудването, центровете за данни);

в) процесите по управление на риска, включително политиките за управление на риска в областта на ИКТ, политиката за непрекъснатост на дейността на ИКТ и плановете за реакция и възстановяване на ИКТ;

г) управленските механизми за ефективно управление на риска в областта на ИКТ, включително организационна структура с ясни, прозрачни и последователни области на отговорност и правила за отчетността;

д) идентифицирането, наблюдаването и своевременното уведомяване на финансовите субекти за съществените инциденти с ИКТ, управлението и отстраняването на такива инциденти, в частност — на кибератаките;

е) механизмите за преносимост на данните, за преносимост на приложенията и за оперативна съвместимост, чрез които се осигурява ефективно упражняване от финансовите субекти на правото на прекратяване на деловите взаимоотношения;

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

з) одитите на ИКТ;

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

4. Въз основа на оценката, посочена в параграф 2, и в координация със съвместната мрежа за надзор (СМН), посочена в член 34, параграф 1, водещият надзорник приема ясен, подробен и обоснован индивидуален план за надзор, в който се описват годишните цели на надзора и основните действия по надзора, планирани за всяко трета страна критичен доставчик на услуги в областта на ИКТ. Този план се предава всяка година на третата страна критичен доставчик на услуги в областта на ИКТ.

Преди приемането на плана за надзор водещият надзорник предава проекта на плана за надзор на третата страна критичен доставчик на услуги в областта на ИКТ.

При получаване на проекта на плана за надзор третата страна критичен доставчик на услуги в областта на ИКТ, може в срок от 15 календарни дни да представи мотивирано становище, в което да докаже очакваното въздействие върху клиентите, които са субекти извън обхвата на настоящия регламент, и когато е целесъобразно, да формулира решения за смекчаване на рисковете.

5. След приемането на годишните планове за надзор, посочени параграф 4, и предаването им на третите страни критични доставчици на услуги в областта на ИКТ, компетентните органи могат да приемат мерки спрямо тези критични доставчици само в съгласие с водещия надзорник.

Член 34

Оперативна координация между водещите надзорници

1. За да се осигури последователен подход към надзорните дейности и да се създадат условия за координирани общи стратегии за надзор и съгласувани оперативни подходи и работни методики, трите водещи надзорници, определени в съответствие с член 31, параграф 1, буква б), създават СМН, така че да се координират на подготвителните етапи и да се координират при провеждането на надзорните дейности по отношение на надзираваните от тях трети страни критични доставчици на услуги в областта на ИКТ, както и в хода на всякакви действия, които може да са необходими съгласно член 42.

2. За целите на параграф 1 водещите надзорници изготвят общ протокол за надзор, в който се определят подробните процедури, които трябва да се следват за осъществяване на ежедневната координация и за осигуряване на бърза комуникация и реакции. Протоколът периодично се преразглежда, за да бъдат отразени оперативните нужди, по-специално развитието на практическите договорености за надзор.

3. Водещият надзорник може според случая да се обърне към ЕЦБ и ENISA с искане да предоставят техническо становище, да споделят практически опит или да се присъединят към конкретни координационни срещи на СМН.

Член 35

Правомощия на водещия надзорник

1. За изпълнението на предвидените в настоящия раздел задачи водещият надзорник разполага със следните правомощия по отношение на критичните трети страни доставчици на услуги в областта на ИКТ:

а) да изисква цялата имаща отношение информация и документация съгласно член 37;

б) да провежда общи разследвания и проверки съгласно съответно членове 38 и 39;

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

г) да издава препоръки в областите, посочени в член 33, параграф 3, 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 третите страни критични доставчици 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 отказ на системата, или за да се сведе до минимум възможното системно въздействие върху финансовия сектор на Съюза на материализирал се риск от концентрация на ИКТ;

iii) всяко планирано възлагане на подизпълнители, когато водещият надзорник прецени, че възлагането на подизпълнители, включително споразуменията за възлагане на подизпълнители, които третата страна критичен доставчик на услуги в областта на ИКТ възнамерява да сключи с трети страни доставчици на услуги в областта на ИКТ, или с поддоставчици на ИКТ, установени в трета държава, може да породи рискове за предоставянето на услуги от финансовия субект или рискове за финансовата стабилност въз основа на прегледа на събраната в съответствие с членове 37 и 38 информация;

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

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

— възлагането на подизпълнители се отнася до критични или важни функции на финансовия субект; както и

— водещият надзорник счита, че използването на такова възлагане на подизпълнители представлява ясен и сериозен риск за финансовата стабилност на Съюза или за финансовите субекти, включително за способността на финансовите субекти да спазват надзорните изисквания.

За целите на точка iv) от настоящата буква третите страни доставчици на услуги в областта на ИКТ, като използват образеца, посочен в член 41, параграф 1, буква б), предават на водещия надзорник информацията относно възлагането на подизпълнители.

2. При упражняване на правомощията, посочени в настоящия член, водещият надзорник:

а) осигурява редовна координация в рамките на СМН и по-специално търси съгласувани подходи, когато е целесъобразно, по отношение на надзора над третите страни критичните доставчици на услуги в областта на ИКТ;

б) взема надлежно предвид рамката, установена с Директива (ЕС) 2022/2555, и при необходимост се консултира със съответните компетентни органи, определени и установени в съответствие с посочената директива, с цел избягване на дублиране на технически и организационни мерки, които биха могли да са приложими за третите страни критични доставчици на услуги в областта на ИКТ, съгласно посочената директива;

в) се стреми да сведе до минимум, доколкото е възможно, риска от смущение в услугите, предоставяни от третите страни критични доставчици на услуги в областта на ИКТ, на клиенти, които са субекти извън обхвата на настоящия регламент.

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

Преди да издаде препоръките в съответствие с параграф 1, буква г), водещият надзорник дава възможност на третата страна доставчик на услуги в областта на ИКТ да предостави в срок от 30 календарни дни съответната информация, доказваща очакваното въздействие върху клиентите, които са субекти извън обхвата на настоящия регламент, и когато е целесъобразно, да формулира решения за намаляване на рисковете.

4. Водещият надзорник информира СМН за резултатите от упражняването на правомощията, посочени в параграф 1, букви а) и б). Водещият надзорник предава без ненужно забавяне докладите по параграф 1, буква в) на СМН и на компетентните органи на финансовите субекти, използващи услугите в областта на ИКТ на тази трета страна критичен доставчик на услуги в областта на ИКТ.

5. Третите страни критични доставчици на услуги в областта на ИКТ, сътрудничат добросъвестно на водещия надзорник и му съдействат в изпълнението на задачите му.

6. В случай на пълно или частично неспазване на мерките, които се изисква да бъдат предприети във връзка с изпълнение на правомощията по параграф 1, букви а), б) и в), и след изтичането на срок от най-малко 30 календарни дни, считано от датата, на която третата страна критичен доставчик на услуги в областта на ИКТ, е получила уведомление за съответните мерки, водещият надзорник взема решение за налагане на периодични наказателни плащания, за да принуди третата страна критичен доставчик на услуги в областта на ИКТ, да започне да спазва тези мерки.

7. Периодичните наказателни плащания, посочени в параграф 6, се начисляват ежедневно, докато разпоредбите не започнат да се спазват, но не по-дълго от шест месеца, след като дадената трета страна критичен доставчик на услуги в областта на ИКТ, е бил уведомено за решението за налагането на периодичните наказателни плащания.

8. Размерът на периодичните наказателни плащания се изчислява от датата, посочена в решението за налагането им, и представлява до 1 % от средния дневен световен оборот на третата страна критичен доставчик на услуги в областта на ИКТ, през предходната финансова година. При определяне на размера на наказателното плащане водещият надзорник взема предвид следните критерии относно неспазването на мерките, посочени в параграф 6:

а) тежестта и продължителността на неспазването;

б) дали неспазването е било умишлено или поради небрежност;

в) степента на сътрудничество на третата страна доставчик на услуги в областта на ИКТ с водещия надзорник;

За целите на първа алинея, за да се гарантира последователен подход, водещият надзорник участва в консултации в рамките на СМН.

9. 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.

10. Водещият надзорник оповестява публично всички периодични наказателни плащания, стига такова оповестяване да не застрашава сериозно финансовите пазари, нито да причинява несъразмерно голяма вреда на засегнатите страни.

11. Преди да наложи периодичните наказателни плащания по параграф 6, водещият надзорник дава възможност на представителите на третата страна критичен доставчик 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. Третата страна критичен доставчик на услуги в областта на ИКТ, срещу която е възбудено дело, 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 36

Упражняване на правомощията на водещия надзорник извън Съюза

1. Когато целите на надзора не могат да бъдат постигнати чрез взаимодействие с дъщерното предприятие, създадено за целите на член 31, параграф 12, или чрез упражняване на надзорни дейности в помещения, намиращи се в Съюза, водещият надзорник може да упражнява правомощията, посочени в следните разпоредби, в помещения, разположени в трета държава, които са притежавани или използвани по някакъв начин за целите на предоставянето на услуги на финансови субекти от Съюза от трета страна критичен доставчик на услуги в областта на ИКТ, във връзка с неговите стопански операции, функции или услуги, включително административни, стопански или оперативни офиси, помещения, терени, сгради или други имоти:

а) в член 35, параграф 1, буква а), и

б) в член 35, параграф 1, буква б) в съответствие с член 38, параграф 2, букви а), б) и г) и член 39, параграф 1 и параграф 2, буква а).

Правомощията, посочени в първа алинея, може да бъдат упражнявани при спазване на всяко едно от следните условия:

i) водещият надзорник счита, че извършването на проверка в трета държава е необходимо, за да може той да изпълнява изцяло и ефективно задълженията си съгласно настоящия регламент;

ii) проверката в трета държава е пряко свързана с предоставянето на услуги в областта на ИКТ на финансови субекти в Съюза;

iii) съответната трета страна критичен доставчик на услуги в областта на ИКТ, е дал съгласието си за извършване на проверка в трета държава; както и

iv) съответният орган на въпросната трета държава е бил официално уведомен от водещия надзорник и не е повдигнал възражения.

2. Без да се засяга компетентността на институциите на Съюза и на държавите членки, за целите на параграф 1 ЕБО, ЕОЦКП или ЕОЗППО сключват споразумения за административно сътрудничество със съответния орган на третата държава, за да се даде възможност за безпрепятствено провеждане на проверките на нейна територия от водещия надзорник и определения от него екип за мисията му в тази трета държава. Тези споразумения за сътрудничество не пораждат правни задължения по отношение на Съюза и неговите държави членки, нито възпрепятстват държавите членки и техните компетентни органи да сключват двустранни или многостранни споразумения с въпросните трети държави и техните органи.

В споразуменията за сътрудничество се посочват най-малко следните елементи:

а) процедурите за координиране на надзорните дейности, извършвани съгласно настоящия регламент, и всяко аналогично наблюдение на риска в областта на ИКТ, пораждан от трета страна във финансовия сектор, упражнявано от съответния орган на засегнатата трета държава, включително подробности за предаване на съгласието на този орган, което да позволи на водещия надзорник и определения от него екип да проведат общи разследвания и проверки на място, както е посочено в параграф 1, първа алинея, на територията под негова юрисдикция;

б) механизма за предаване на всяка имаща отношение информация между ЕБО, ЕОЦКП или ЕОЗППО и съответния орган на засегнатата трета държава, по-специално във връзка с информацията, която може да бъде поискана от водещия надзорник съгласно член 37;

в) механизмите за своевременно уведомяване на ЕБО, ЕОЦКП или ЕОЗППО от съответния орган на засегнатата трета държава за случаите, в които за трета страна доставчик на услуги в областта на ИКТ, установена в трета държава и определена като критична съгласно член 31, параграф 1, буква а), се счита, че е нарушила изискванията, които съгласно приложимото право на тази трета държава е длъжна да спазва при предоставянето на услуги на финансови институции на нейна територия, както и приложените корективни мерки и санкции;

г) редовното предаване на актуална информация за промените в нормативната или надзорната уредба във връзка с наблюдението на риска в областта на ИКТ, пораждан от трети страни по отношение на финансовите институции в засегнатата трета държава;

д) подробностите, позволяващи, ако е необходимо, участието на един представител на съответния орган на третата държава в проверките, извършвани от водещия надзорник и определения екип.

3. Когато водещият надзорник не е в състояние да извършва надзорни дейности извън Съюза, съгласно посоченото в параграфи 1 и 2, водещият надзорник:

а) упражнява правомощията си по член 35 въз основа на всички факти и документи, с които разполага;

б) документира и обяснява всяка последица от невъзможността си да извърши предвидените надзорни дейности, както е посочено в настоящия член.

Потенциалните последици, посочени в буква б) от настоящия параграф, се вземат предвид в препоръките на водещия надзорник, издавани съгласно член 35, параграф 1, буква г).

Член 37

Искане за информация

1. Водещият надзорник може с обикновено искане или с решение да поиска от трета страна критичен доставчик на услуги в областта на ИКТ, да му предостави всички необходими за изпълнението на задълженията му по настоящия регламент сведения, включително всички имащи отношение делови или оперативни документи, договори, документация за политиките, одиторски доклади за сигурността на ИКТ, доклади за инцидентите с ИКТ, както и всяка информация за страните, на които третата страна критичен доставчик на услуги в областта на ИКТ е възложила 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 третата страна критичен доставчик 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 с решение 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 35, параграф 6 периодични наказателни плащания при предоставяне на непълна информация или когато такава информация не е предоставена в срока, посочен в буква г) от настоящия параграф;

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

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

5. Водещият надзорник изпраща без забавяне копие от решението, с което се изисква да му се предостави информация, на компетентните органи на финансовите субекти, които ползват услугите на съответната трета страна критичен доставчик на услуги в областта на ИКТ, и на СМН.

Член 38

Общи разследвания

1. С оглед на задачите си по настоящия регламент водещият надзорник, подпомаган от посочения в член 40, параграф 1 съвместен разследващ екип, може при необходимост да извършва разследвания на трети страни критични доставчици на услуги в областта на ИКТ.

2. Водещият надзорник разполага с правомощия:

а) да проверява записи, 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 тези записи, данни, документирани процедури, както и от всякакви други материали;

в) да призовава представителите на трета страна критичен доставчик 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 35, параграф 6 периодични наказателни плащания, в случай че изисканите записи, данни, документирани процедури или други материали, или отговорите на въпросите, зададени на представителите на третата страна доставчик на услуги в областта на ИКТ, не бъдат представени или бъдат непълни.

4. Представителите на третите страни критични доставчици 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 35, параграф 6 периодични наказателни плащания, средствата за правна защита, предвидени в регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (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 ИКТ услугите на дадената трета страна критичен доставчик на услуги в областта на ИКТ, за предвиденото разследване, както и самоличността на оправомощените лица.

Водещият надзорник подава на СМН цялата информация, получена съгласно първа алинея.

Член 39

Проверки

1. С оглед на задачите си по настоящия регламент водещият надзорник, подпомаган от посочения в член 40, параграф 1 съвместен разследващ екип, може да влиза и извършва всички необходими проверки на място във всички търговски помещения, терени или имоти на трети страни доставчици на услуги в областта на ИКТ — седалища, оперативни центрове, допълнителни помещения, както и да извършва проверки извън работното място.

За целите на упражняването на правомощията, посочени в първа алинея, водещият надзорник се консултира със СМН.

2. Длъжностните лица и други лица, упълномощени от водещия надзорник да извършват проверка, имат право:

а) да влизат във всички тези служебни помещения, терени или имоти; и

б) да запечатват всички тези служебни помещения, счетоводни книги или документи за срока и в степента, необходими за проверката.

Ако представителите на дадено трета страна критичен доставчик на услуги в областта на ИКТ, не се подчинят на дадена проверка, длъжностните лица и други лица, упълномощени от водещия надзорник, упражняват правомощията си след представяне на писмено разрешение, в което са посочени предметът и целта на проверката, както и предвидените в член 35, параграф 6 периодични наказателни плащания.

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

5. Преди всяка планирана проверка на място водещият надзорник предизвестява в разумен срок дадената трета страна критичен доставчик 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. Третата страна критичен доставчик на услуги в областта на ИКТ се подчинява на всяка проверка на място, наредена с решение на водещия надзорник. В решението се посочват предметът и целта на проверката, датата, на която тя ще започне, предвидените в член 35, параграф 6 периодични наказателни плащания, средствата за правна защита, предвидени в регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (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 дадена трета страна критичен доставчик на услуги в областта на ИКТ се противопоставя на проверка, разпоредена по реда на настоящия член, водещият надзорник уведомява третата страна критичен доставчик на услуги в областта на ИКТ за последиците от такова противопоставяне, включително за възможността компетентните органи на съответните финансови субекти да изискат от финансовите субекти да прекратят сключените с него договорни споразумения.

Член 40

Текущ надзор

1. При извършването на надзорни дейности, по-специално на общи разследвания или проверки, водещият надзорник се подпомага от съвместен разследващ екип, който се сформира за всяка трета страна критичен доставчик на услуги в областта на ИКТ.

2. Съвместният разследващ екип, посочен в параграф 1, се състои от служители от:

а) ЕНО;

б) съответните компетентни органи, упражняващи надзор на финансовите субекти, на които третата страна критичен доставчик на услуги в областта на ИКТ, предоставя услуги в областта на ИКТ;

в) националния компетентен орган, посочен в член 32, параграф 4, буква д), на доброволен принцип;

г) един национален компетентен орган от държавата членка, в която е установено третата страна критичен доставчик на услуги в областта на ИКТ, на доброволен принцип.

Членовете на съвместния разследващ екип притежават експертен опит в сферата на ИКТ и операционния риск. Работата на съвместния разследващ екип се координира от определен за целта служител на водещия надзорник („координатор на водещия надзорник“).

3. В рамките на 3 месеца след като приключи дадено разследване или проверка и след като се допита до надзорния форум, водещият надзорник приема препоръки, които отправя към третата страна критичен доставчик на услуги в областта на ИКТ, съгласно правомощията, посочени в член 35.

4. Препоръките по параграф 3 се съобщават незабавно на третата страна критичен доставчик на услуги в областта на ИКТ, и на компетентните органи на финансовите субекти, на които той предоставя услуги в областта на ИКТ.

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

Член 41

Хармонизиране на условията за извършване на надзорните дейности

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

а) информацията, която да бъде представена от трета страна доставчик на услуги в областта на ИКТ в заявлението за доброволно искане да бъде определен като критичен по смисъла на член 31, параграф 11;

б) съдържанието, структурата и формата на информацията, която се подава, оповестява или докладва от третите страни доставчици на услуги в областта на ИКТ съгласно член 35, параграф 1, включително образеца за предоставяне на информация за споразуменията за възлагане на подизпълнители;

в) критериите за определяне състава на съвместния проверяващ екип, осигуряващи балансирано участие на служителите на ЕНО и на съответните компетентни органи, тяхното определяне, задачи и работни договорености;

г) оценяването, което по силата на член 42, параграф 3 компетентните органи извършват на мерките, предприети от трети страни критични доставчици на услуги в областта на ИКТ, вследствие на препоръките на водещия надзорник.

2. ЕНО представят тези проекти на регулаторни технически стандарти на Комисията до 17 юли 2024 г.

На Комисията се делегират правомощия да допълни настоящия регламент, като приеме посочените в параграф 1 регулаторни технически стандарти в съответствие с процедурата, предвидена в членове 10—14 от регламенти (ЕС) № 1093/2010, (ЕС) № 1094/2010 и (ЕС) № 1095/2010.

Член 42

Последващи действия на компетентните органи

1. В рамките на 60 календарни дни от получаването на отправените от водещия надзорник по силата на член 35, параграф 1, буква г) препоръки трети страни критични доставчици на услуги в областта на ИКТ, го уведомяват за намерението си да последват въпросните препоръки или представят аргументирано обяснение защо няма да ги последват. Водещият надзорник незабавно предава тази информация на компетентните органи на заинтересованите финансови субекти.

2. Водещият надзорник оповестява публично случаите, когато трета страна критичен доставчик на услуги в областта на ИКТ, не уведоми водещия надзорник в съответствие с параграф 1 или когато предоставеното от третата страна критичен доставчик на услуги в областта на ИКТ, обяснение бъде сметнато за недостатъчно. В публикуваната информация се разкрива самоличността на третата страна критичен доставчик на услуги в областта на ИКТ, както и видът и естеството на неспазването. Тази информация се ограничава до това, което е съществено и пропорционално за целта да се гарантира обществената осведоменост, освен в случаите, когато такова публикуване би могло да причини несъразмерна вреда на засегнатите страни или да застраши сериозно правилното функциониране и целостта на финансовите пазари или стабилността на цялата финансова система на Съюза или на част от нея.

Водещият надзорник уведомява за това публично оповестяване третата страна доставчик на услуги в областта на ИКТ.

3. Компетентните органи информират съответните финансови субекти за рисковете, установени в препоръките, отправени към третите страни критични доставчици на услуги в областта на ИКТ в съответствие с член 35, параграф 1, буква г).

При управлението на риска при ИКТ, пораждан от трета страна финансовите субекти вземат предвид рисковете, посочени в първа алинея.

4. Когато компетентен орган прецени, че даден финансов субект не отчита или не се справя в рамките на управлението на риска при ИКТ, пораждан от трети страни в достатъчна степен със специфичните рискове, посочени в препоръките, той уведомява финансовия субект за възможността да вземе решение в срок от 60 календарни дни от получаването на уведомлението съгласно параграф 6 при липсата на подходящи договорни споразумения, насочени към преодоляване на тези рискове.

5. След получаване на докладите, посочени в член 35, параграф 1, буква в), и преди да вземат решение по параграф 6 от настоящия член, компетентните органи могат доброволно да се консултират с националните компетентни органи, определени или установени в съответствие с Директива (ЕС) 2022/2555, отговарящи за надзора на съществен или важен субект, попадащ в обхвата на посочената директива, който е определен за трета страна критичен доставчик на услуги в областта на ИКТ.

6. Компетентен орган може, като последна мярка, след уведомлението, и ако е приложимо — след консултацията, както е посочено в параграфи 4 и 5 от настоящия член, по силата на член 50 да вземе решение, с което да изиска от финансов субект временно да престане, частично или изцяло, да използва или да внедрява услуга, предоставяна от дадена трета страна критичен доставчик 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 договорни споразумения, сключени с третата страна критичен доставчик на услуги в областта на ИКТ.

7. Ако трета страна критичен доставчик на услуги в областта на ИКТ откаже да приеме препоръките, като се опира на подход, различен от препоръчания от водещия надзорник, и този различен подход може да окаже неблагоприятно въздействие върху голям брой финансови субекти или значителна част от финансовия сектор, изпълняващи критични или важни функции, и ако индивидуалните предупреждения, отправени от компетентните органи, не са довели до последователни подходи за намаляване на потенциалния риск за финансовата стабилност, водещият надзорник може, след консултация с надзорния форум, да излезе по целесъобразност с необвързващи и непублични становища към компетентните органи, за да насърчи съгласувани и конвергентни мерки, свързани с последващи надзорни действия.

8. След получаването на докладите, посочени в член 35, параграф 1, буква в), когато вземат решение съгласно параграф 6 от настоящия член, компетентните органи отчитат вида и размера на риска, на който третата страна критичен доставчик на услуги в областта на ИКТ, не е обърнала внимание, както и доколко сериозно е неспазването, като се отчитат 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 третата страна критичен доставчик 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;

д) дали спирането или прекратяването на договорните споразумения поражда риск за непрекъснатостта на стопанската дейност на финансовия субект, независимо от усилията на финансовия субект да избегне смущения в предоставянето на своите услуги;

е) ако е приложимо, поисканото на доброволен принцип в съответствие с параграф 5 от настоящия член становище на компетентните органи, определени или установени в съответствие с Директива (ЕС) 2022/2555, отговарящи за съществен или важен субект, попадащ в обхвата на посочената директива, който е определен за трета страна критичен доставчик на услуги в областта на ИКТ.

Компетентните органи предоставят на финансовите субекти необходимия срок, за да могат те да адаптират договорните споразумения с третите страни критични доставчици на услуги в областта на ИКТ, за да се избегнат неблагоприятните последици за тяхната оперативна устойчивост на цифровите технологии и да им се даде възможност да приложат изходните стратегии и преходните планове, посочени в член 28.

9. Решението, посочено в параграф 6 от настоящия член, се съобщава на членовете на надзорния форум, посочен в член 32, параграф 4, букви а), б) и в), и на СМН.

Третите страни критични доставчици на услуги в областта на ИКТ, засегнати от решенията по параграф 6, оказват пълно съдействие на засегнатите финансови субекти, по-специално в процеса на спиране на действието или прекратяване на договорните им споразумения.

10. Компетентните органи редовно осведомяват водещия надзорник за предприетите в хода на надзора върху финансовите субекти подходи и мерки, както и за договорните споразумения, сключени от финансовите субекти в случай на частично или цялостно пренебрегване от страна на трети страни, които са критични доставчици на услуги в областта на ИКТ, на отправените от водещия надзорник препоръки.

11. При поискване водещият надзорник може да предостави допълнителни разяснения относно издадените препоръки, за да даде насоки на компетентните органи във връзка с последващите мерки.

Член 43

Такси за упражняване на надзор

1. В съответствие с делегирания акт, посочен в параграф 2 от настоящия член, водещият надзорник начислява на третите страни критични доставчици на услуги в областта на ИКТ, такси, които изцяло покриват необходимите разходи на водещия надзорник във връзка с изпълнението на надзорните задачи съгласно настоящия регламент, включително възстановяването на всички разходи, които могат да бъдат направени в резултат на работата, извършена от съвместния разследващ екип, посочен в член 40, както и разходите за консултации, предоставени от независимите експерти, посочени в член 32, параграф 4, втора алинея, по въпроси, попадащи в обхвата на преките надзорни дейности.

Таксата, която се начислява на трета страна критичен доставчик на услуги в областта на ИКТ, покрива всички разходи, произтичащи от изпълнението на задълженията, предвидени в настоящия раздел, и е съобразена с неговия оборот.

2. На Комисията се предоставя правомощието да приеме делегиран акт в съответствие с член 57, за да допълни настоящия регламент, като определи размера на таксите и начина на плащането им, до 17 юли 2024 г.

Член 44

Международно сътрудничество

1. Без да се засяга член 36, ЕБО, ЕОЦКП и ЕОЗППО могат, в съответствие с член 33 съответно от регламенти (ЕС) № 1093/2010, (ЕС) № 1095/2010 и (ЕС) № 1094/2010 да сключват административни споразумения с регулаторните и надзорните органи на трети държави за насърчаване на международното сътрудничество във връзка с риска в областта на ИКТ, пораждан от трети страни, в различните финансови сектори, по специално чрез разработването на най-добри практики за преглед на практиките и контролните механизми за управление на риска в областта на ИКТ, мерки за ограничаване на риска и реакция при инциденти.

2. На 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 в областта на ИКТ, пораждан от трети страни, и последиците за финансовата стабилност, целостта на пазара, защитата на инвеститорите и функционирането на вътрешния пазар.

ГЛАВА VI

Споразумения за обмен на информация

Член 45

Споразумения за обмен на информация и разузнавателни сведения за киберзаплахи

1. Финансовите субекти могат да обменят помежду си информация и разузнавателни сведения за киберзаплахи, включително 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 при финансовите субекти, по-специално чрез повишаване на осведомеността за киберзаплахите, ограничаване или възпрепятстване на способността на киберзаплахите да се разпространяват, подпомагане на отбранителните способности, на техниките за откриване на заплахи, на стратегиите за ограничаване на риска или на етапите на реакция и възстановяване;

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 съгласно Регламент (ЕС) 2016/679 и насоките за политиката в областта на конкуренцията.

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 обмен на информация, участието на трети страни доставчици на услуги в областта на ИКТ, както и оперативните елементи, включително използването на специални информационни платформи.

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

ГЛАВА VII

Компетентни органи

Член 46

Компетентни органи

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

а) за кредитните институции и за институциите, освободени съгласно Директива 2013/36/ЕС — компетентният орган, определен в съответствие с член 4 от посочената директива, а за кредитните институции, класифицирани като значими в съответствие с член 6, параграф 4 от Регламент (ЕС) № 1024/2013 — ЕЦБ съгласно правомощията и задачите, възложени ѝ с посочения регламент;

б) за платежните институции, включително платежните институции, освободени съгласно Директива (ЕС) 2015/2366, институциите за електронни пари, включително освободените съгласно Директива 2009/110/ЕО, и доставчиците на услуги по предоставяне на информация за сметка, посочени в член 33, параграф 1 от Директива (ЕС) 2015/2366 — компетентният орган, определен в съответствие с член 22 от Директива (ЕС) 2015/2366;

в) за инвестиционните посредници — компетентният орган, определен в съответствие с член 4 от Директива (ЕС) 2019/2034 на Европейския парламент и на Съвета ([38]);

г) за доставчиците на услуги за криптоактиви, лицензирани съгласно Регламента относно пазарите на криптоактиви, и емитентите на токени, обезпечени с активи — компетентният орган, определен съгласно относимата разпоредба от посочения регламент;

д) за централните депозитари на ценни книжа — компетентният орган, определен в съответствие с член 11 от Регламент (ЕС) № 909/2014;

е) за централните контрагенти — компетентният орган, определен в съответствие с член 22 от Регламент (ЕС) № 648/2012;

ж) за местата на търговия и доставчиците на услуги за докладване на данни —компетентният орган, определен съгласно член 67 от Директива 2014/65/ЕС, и компетентният орган, определен в член 2, параграф 1, точка 18 от Регламент (ЕС) № 600/2014;

з) за регистрите на трансакции — компетентният орган, определен в съответствие с член 22 от Регламент (ЕС) № 648/2012;

и) за лицата, управляващи алтернативни инвестиционни фондове — компетентният орган, определен в съответствие с член 44 от Директива 2011/61/ЕС;

й) за управляващите дружества — компетентният орган, определен в съответствие с член 97 от Директива 2009/65/ЕО;

к) за застрахователните и презастрахователните предприятия — компетентният орган, определен в съответствие с член 30 от Директива 2009/138/ЕО;

л) за застрахователните посредници, презастрахователните посредници и посредниците, предлагащи застрахователни продукти като допълнителна дейност — компетентният орган, определен в съответствие с член 12 от Директива (ЕС) 2016/97;

м) за институциите за професионално пенсионно осигуряване — компетентният орган, определен в съответствие с член 47 от Директива (ЕС) 2016/2341;

н) за агенциите за кредитен рейтинг — компетентният орган, определен в съответствие с член 21 от Регламент (ЕО) № 1060/2009;

о) за администраторите на критични бенчмаркове — компетентният орган, определен в съответствие с членове 40 и 41 от Регламент (ЕС) 2016/1011;

([38]) Директива (ЕС) 2019/2034 на Европейския парламент и на Съвета от 27 ноември 2019 г. относно пруденциалния надзор върху инвестиционните посредници и за изменение на директиви 2002/87/ЕО, 2009/65/ЕО, 2011/61/ЕС, 2013/36/ЕС, 2014/59/ЕС и 2014/65/ЕС (ОВ L 314, 5.12.2019 г., стр. 64).

п) за доставчиците на услуги за колективно финансиране — компетентният орган, определен в съответствие с член 29 от Регламент (ЕС) 2020/1503;

р) за регистрите на секюритизации — компетентният орган, определен в съответствие с член 10 и член 14, параграф 1 от Регламент (ЕС) 2017/2402.

Член 47

Сътрудничество със структурите и органите, създадени с Директива (ЕС) 2022/2555

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 съгласно член 14 от Директива (ЕС) 2022/2555, ЕНО и компетентните органи могат да участват в дейностите на групата за сътрудничество по въпроси, засягащи техните надзорни дейности по отношение на финансовите субекти. ЕНО и компетентните органи могат да поискат да бъдат поканени да участват в дейностите на групата за сътрудничество по въпроси, свързани със съществените или важните субекти попадащи в обхвата на Директива (ЕС) 2022/2555, които са определени и като трети страни, които са критични доставчици на услуги в областта на ИКТ, съгласно член 31 от настоящия регламент.

2. Когато е целесъобразно, компетентните органи могат да се консултират и да обменят информация съответно с единните звена за контакт и ЕРИКС, определени и установени в съответствие с Директива (ЕС) 2022/2555.

3. Когато е целесъобразно, компетентните органи могат да искат всякакво относимо техническо становище и съдействие от компетентните органи, определени или създадени в съответствие с Директива (ЕС) 2022/2555, и да установяват договорености за сътрудничество, които да позволяват създаването на ефективни и бързи механизми за координация.

4. В договореностите по параграф 3 от настоящия член могат, наред с другото, да се уточнят процедурите за координиране на надзорните дейности по отношение съответно на съществените или важните субекти, попадащи в обхвата на Директива (ЕС) 2022/2555 които са определени като трети страни, които са критични доставчици на услуги в областта на ИКТ, съгласно член 31 от настоящия регламент, включително за провеждането, в съответствие с националното право, на разследвания и проверки на място, както и за механизмите за обмен на информация между компетентните органи по настоящия регламент и компетентните органи, определени и установени в съответствие с посочената директива, което включва достъп до информацията, поискана от тези органи.

Член 48

Сътрудничество между органите

1. Компетентните органи си сътрудничат тясно помежду си, и когато е приложимо — с водещия надзорник.

2. Компетентните органи и водещият надзорник обменят своевременно помежду си цялата имаща отношение информация относно третите страни критични доставчици на услуги в областта на ИКТ, необходима за изпълнението на съответните им задължения съгласно настоящия регламент, по-специално във връзка с идентифицираните рискове, подходите и мерките, предприети като част от надзорните задачи на водещия надзорник.

Член 49

Симулации, комуникация и сътрудничество сред финансовите сектори

1. ЕНО, чрез съвместния комитет и в сътрудничество с компетентните органи, националните органи за преструктуриране, посочени в член 3 от Директива 2014/59/ЕС, ЕЦБ, Единният съвет за преструктуриране — когато се касае за информация, отнасяща се до субектите, попадащи в обхвата на Регламент (ЕС) № 806/2014, ЕССР и ENISA, ако е приложимо, могат да създадат механизми за споделяне на ефективните практики сред финансовите сектори, за да се повишава ситуационната осведоменост и да се набележат 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 равнището на Съюза при съществен трансграничен инцидент с ИКТ или свързана с него заплаха със системно въздействие върху целия финансов сектор на Съюза.

Ако е необходимо, при тези симулации може да се тества и зависимостта на финансовия сектор от други икономически сектори.

2. Компетентните органи, ЕНО и ЕЦБ си сътрудничат тясно и обменят информация с оглед на задълженията си по членове 47—54. 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 50

Административни санкции и коригиращи мерки

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

2. Правомощията по параграф 1 включват най-малко следните правомощия:

а) 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) извършване на проверки на място или разследвания, които включват, но не се ограничават до:

i) призоваването на представителите на финансовите субекти да дават устно или писмено обяснение на факти или документи, свързани с предмета и целта на разследването, и записване на отговорите;

ii) интервюирането на всякакви други физически или юридически лица, които дадат съгласие за това, с цел да бъде събрана информация, свързана с предмета на разследването;

в) изискване за прилагане на корективни и коригиращи мерки при нарушения на изискванията на настоящия регламент.

3. Без да се засяга правото им да налагат наказателноправни санкции в съответствие с член 52, държавите членки въвеждат при нарушение на настоящия регламент подходящи административни санкции и коригиращи 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 коригиращи мерки при нарушение на настоящия регламент:

а) разпореждане, с което от физическото или юридическото лице се изисква да спре действието, с което нарушава настоящия регламент и да се въздържа от повтаряне на това действие;

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

в) приемане на всякакви мерки, включително с парично измерение, за да се осигури непрекъснатото 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, включително на публични изявления, в които се посочва самоличността — при физически лица или наименованието — при юридически лица, както и естеството на нарушението.

5. Когато параграф 2, буква в) и параграф 4 се прилагат спрямо юридически лица, държавите членки оправомощават компетентните органи да прилагат административните санкции и коригиращите 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 гарантират, че всяко решение за налагане на посочените в параграф 2, буква в) административни санкции или коригиращи мерки е надлежно мотивирано и полежи на обжалване.

Член 51

Упражняване на правомощията за налагане на административни санкции и коригиращи мерки

1. Компетентните органи упражняват съгласно националната си правна уредба посочените в член 50 правомощия за налагане на административни санкции и коригиращи мерки, ако е целесъобразно, както следва:

а) пряко;

б) в сътрудничество с други органи;

в) на своя отговорност, като оправомощават други органи; или

г) като отнасят въпросите пред компетентните съдебни органи.

2. Когато определят вида и размера на налаганите по силата на член 50 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, включително, 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 физическо или юридическо лице на реализираната печалба или избегнатата загуба;

ж) предишните нарушения на отговорното физическо или юридическо лице.

Член 52

Наказателноправни санкции

1. Държавите членки могат да решат да не въвеждат правила за административни санкции или коригиращи 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, гарантират въвеждането на 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 53

Задължения за уведомяване

Държавите членки уведомяват Комисията, ЕОЦКП, ЕБО и ЕОЗППО относно законовите, подзаконовите и административните разпоредби за прилагане на настоящата глава, включително относно всички приложими наказателноправни разпоредби, до 17 януари 2025 г. При всяко последващо изменение на тези разпоредби държавите членки своевременно уведомяват Комисията, ЕОЦКП, ЕБО и ЕОЗППО.

Член 54

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, включваща рискове по отношение на защитата на личните данни, 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 ако въпросното публикуване би било непропорционално на наложената санкция, ако е била намалена.

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 свързана 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 само за времето, необходимо за прилагането на настоящия член. Този срок не може да надвишава пет години след публикуването.

Член 55

Професионална тайна

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

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

3. Информацията, представляваща професионална тайна, включително обменът на информация между компетентните органи по настоящия регламент и компетентните органи, определени или установени в съответствие с Директива (ЕС) 2022/2555, не се разкрива на никое друго лице или орган, освен по силата на разпоредбите на правото на Съюза или на националното право.

4. Цялата обменяна между компетентните органи съгласно 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 професионалната тайна, освен в случаите, когато компетентният орган посочи в момента на предаването ѝ, че тя може да бъде разкрита, или когато разкриването ѝ се налага за процесуални цели.

Член 56

Защита на данните

1. ЕНО и компетентните органи имат право да обработват лични данни само когато това е необходимо за целите на изпълнението на техните съответни задължения и задачи съгласно настоящия регламент, по-специално във връзка с разследване, проверка, искане за информация, съобщаване, публикуване, оценка, сверяване, оценяване и изготвяне на планове за надзор. Личните данни се обработват в съответствие с Регламент (ЕС) 2016/679 или Регламент (ЕС) 2018/1725, според това кой от тях е приложим.

2. Ако в други секторни актове не е предвидено друго, личните данни, посочени в параграф 1, се съхраняват до изпълнението на приложимите надзорни задължения и при всички случаи за максимален срок от 15 години, освен в случай на висящо съдебно производство, изискващо по-нататъшно съхранение на тези данни.

ГЛАВА VIII

Делегирани актове

Член 57

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 31, параграф 6 и член 43, параграф 2, се предоставя на Комисията за срок от пет години, считано от 17 януари 2024 г. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

3. Делегирането на правомощия, посочено в член 31, параграф 6 и член 43, параграф 2, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. Оттеглянето поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна дата, посочена в решението. То не засяга действителността на делегираните актове, които вече са в сила.

4. Преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество.

5. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

6. Делегиран акт, приет съгласно член 31, параграф 6 и член 43, параграф 2, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от три месеца след нотифицирането на същия акт на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Посоченият срок може да се удължи с три месеца по инициатива на Европейския парламент или на Съвета.

ГЛАВА IX

Преходни и заключителни разпоредби

Раздел I

Член 58

Клауза за преглед

1. До 17 януари 2028 г., след като се допита, по целесъобразност, до ЕБО, ЕОЦКП, ЕОЗППО и ЕССР, Комисията извършва преглед и представя доклад на Европейския парламент и на Съвета, придружен, ако е целесъобразно, от законодателно предложение. Прегледът включва най-малко следното:

а) критериите по член 31, параграф 2 за определяне на третите страни критични доставчици на услуги в областта на ИКТ;

б) доброволния характер на уведомяването за значителни киберзаплахи, посочени в член 19;

в) режима, посочен в член 31, параграф 12, и правомощията на водещия надзорник, предвидени в член 35, параграф 1, буква г), точка iv), първо тире, с цел да се оцени ефективността на тези разпоредби по отношение на осигуряването на ефективен надзор на установените в трета държава трети страни критични доставчици на услуги в областта на ИКТ, както и необходимостта от създаване на дъщерно предприятие в Съюза.

За целите на първата алинея от настоящата буква прегледът включва анализ на режима, посочен в член 31, параграф 12, включително на условията за достъп на финансовите субекти от Съюза до услуги от трети държави и наличността на такива услуги на пазара на Съюза, и взема предвид други събития на пазарите на услугите, обхванати от настоящия регламент, практическия опит на финансовите субекти и органите за финансов надзор по отношение на прилагането и съответно надзора на този режим, както и всички съответни промени в нормативната и надзорната област, които настъпват на международно равнище.

г) целесъобразността на включването в обхвата на настоящия регламент на финансовите субекти, посочени в член 2, параграф 3, буква д), като се използват автоматизирани системи за продажба, с оглед на бъдещото развитие на пазара във връзка с използването на такива системи;

д) функционирането и ефективността на СМН в подкрепа на съгласуваността на надзора и ефикасността на обмена на информация в рамките на надзорната рамка.

2. В контекста на прегледа на Директива (ЕС) 2015/2366 Комисията оценява необходимостта от повишаване на киберустойчивостта на платежните системи и дейностите по обработване на плащания и целесъобразността от разширяването на обхвата на настоящия регламент, така че да включва операторите на платежни системи и субектите, участващи в дейности по обработване на плащания. В светлината на тази оценка Комисията представя, като част от прегледа на Директива (ЕС) 2015/2366, доклад на Европейския парламент и на Съвета не по-късно от 17 юли 2023 г.

Въз основа на посочения доклад за преглед и след консултация с ЕБО, ЕЦБ и ЕССР Комисията може да представи, ако е целесъобразно и като част от законодателното предложение, което може да приеме съгласно член 108, втори параграф от Директива (ЕС) 2015/2366, предложение, с което да се гарантира, че всички оператори на платежни системи и субекти, участващи в дейности по обработване на плащания, са обект на подходящ надзор, като същевременно се отчита съществуващият надзор от страна на централната банка.

3. До 17 януари 2026 г. Комисията, след консултация с ЕНО и Комитета на европейските органи за надзор на одита, извършва преглед и представя доклад на Европейския парламент и на Съвета, придружен, ако е целесъобразно, от законодателно предложение относно целесъобразността от засилени изисквания към регистрираните одитори и одиторските дружества по отношение на оперативната устойчивост на цифровите технологии чрез включването на регистрираните одитори и одиторските дружества в обхвата на настоящия регламент или чрез изменения на Директива 2006/43/ЕО на Европейския парламент и на Съвета ([39]).

Раздел II

Изменения

Член 59

Изменения на Регламент (ЕО) № 1060/2009

Регламент (ЕО) № 1060/2009 се изменя, както следва:

1) В приложение I, раздел А, точка 4 първата 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) 2022/2554 на Европейския парламент и на Съвета (*).

_____

(*) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).“;

2) В приложение III точка 12 се заменя със следното:

„12. Агенцията за кредитен рейтинг нарушава член 6, параграф 2, във връзка с раздел А, точка 4 от приложение I, ако не разполага с надеждни административни или счетоводни процедури, с механизми за вътрешен контрол, с ефективни процедури за оценка на риска, или с ефективни контролни или защитни механизми за управление на системите на ИКТ в съответствие с Регламент (ЕС) 2022/2554; или ако не прилага или не поддържа процедурите за вземане на решение или организационните структури, изисквани съгласно посочената точка.“

Член 60

Изменения на Регламент (ЕС) № 648/2012

Регламент (ЕС) № 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, включително системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета (*).

_____

(*) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).;“

([39]) Директива 2006/43/ЕО на Европейския парламент и на Съвета от 17 май 2006 г. относно задължителния одит на годишните счетоводни отчети и консолидираните счетоводни отчети, за изменение на Директиви 78/660/ЕИО и 83/349/ЕИО на Съвета и за отмяна на Директива 84/253/ЕИО на Съвета (ОВ L 157, 9.6.2006 г., стр. 87).

б) параграф 6 се заличава.

2) Член 34 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1. ЦК създава, прилага и поддържа адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофи, в които са включени политика за непрекъснатост на дейността на ИКТ и планове за реакция и възстановяване на ИКТ, въведени и изпълнявани съгласно Регламент (ЕС) 2022/2554, с цел да осигури поддържането на своите функции, своевременното възстановяване на операциите и изпълнението на задълженията на ЦК.“

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

„3. С цел да се гарантира последователното прилагане на настоящия член ЕОЦКП, след консултации с членовете на ЕСЦБ, разработва проекти на регулаторни технически стандарти за определяне на минималното съдържание и минималните изисквания на политиката за непрекъснатост на дейността и на плана за възстановяване при катастрофа, като се изключват политиката за непрекъснатост на дейността на ИКТ и плановете за възстановяване на ИКТ.“

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

„3. С цел осигуряване на еднообразното прилагане на настоящия член ЕОЦКП разработва проекти на регулаторни технически стандарти, в които се определят детайлите на посоченото в параграф 1 заявление за регистрация, като тези технически детайли не съдържат изисквания относно управлението на риска в областта на 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, включително системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2022/2554.

2. Регистърът на трансакции създава, прилага и поддържа адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофа, в които са включени политика за непрекъснатост на дейността на ИКТ и планове за реакция и възстановяване на ИКТ, създадени в съответствие с Регламент (ЕС) 2022/2554, които имат за цел да осигурят поддържането на неговите функции, своевременното възстановяване на операциите и изпълнението на задълженията на регистъра на трансакции.“

5) В член 80 параграф 1 се заличава.

6) В приложение I раздел II се изменя, както следва:

а) букви а) и б) се заменят със следното:

„а) регистър на трансакции нарушава член 79, параграф 1, ако не идентифицира източниците на операционен риск или не сведе до минимум тези рискове чрез разработването на подходящи системи, механизми за контрол и процедури, включително системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2022/2554;

б) регистър на трансакции нарушава член 79, параграф 2, ако не създаде, не прилага или не поддържа адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофа, изготвени в съответствие с Регламент (ЕС) 2022/2554, с които се цели осигуряване на поддържането на неговите функции, своевременното възобновяване на операциите и изпълнението на задълженията на регистъра на трансакции;“;

б) буква в) се заличава.

7) Приложение III се изменя, както следва:

а) раздел II се изменя, както следва:

i) буква в) се заменя със следното:

„в) ЦК от ниво 2 нарушава член 26, параграф 3, ако не поддържа или не прилага организационна структура, която осигурява непрекъснатост и нормално функциониране при изпълнението на неговите услуги и дейности, или ако не използва подходящи и пропорционални системи, ресурси или процедури, включително системи на ИКТ, управлявани в съответствие с Регламент (ЕС) 2022/2554.“;

ii) буква е) се заличава;

б) в раздел III буква а) се заменя със следното:

„а) ЦК от ниво 2 нарушава член 34, параграф 1, ако не създаде, не прилага или не поддържа адекватна политика за непрекъснатост на дейността и план за реакция и възстановяване, създадени в съответствие с Регламент (ЕС) 2022/2554, с които се цели да се осигури поддържане на неговите функции, своевременно възстановяване на операциите и изпълнение на задълженията на ЦК, и позволяват най-малко възстановяването на всички трансакции към момента на смущението, за да може ЦК да продължи по надежден начин дейността си и да приключи сетълмента на определената дата;“.

Член 61

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) 2022/2554 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, включително до управляваните от него системи за сетълмент на ценни книжа.

_____

(*) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).“

2) Параграф 2 се заличава.

3) Параграфи 3 и 4 се заменят със следното:

„3. С оглед на запазването на своите функции, своевременното възобновяване на операциите 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, адекватна политика за непрекъснатост на дейността и план за възстановяване от катастрофа, в които са включени политика за непрекъснатост на дейността на ИКТ и планове за реакция и възстановяване на ИКТ, установени съгласно Регламент (ЕС) 2022/2554.

4. В посочения в параграф 3 план се очертава как се възстановяват всички трансакции и позиции на участниците към момента на смущението, 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 смущението се възобновява функционирането на критичните информационни системи, както е предвидено в член 12, параграфи 5 и 7 от Регламент (ЕС) 2022/2554.“

4) Параграф 6 се заменя със следното:

„6. ЦДЦК установява, наблюдава и управлява рисковете, които пораждат за операциите му ключовите 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 без забавяне компетентния орган и съответните органи за всички оперативни инциденти, произтичащи от такива рискове, без тук да се включват рисковете в областта на ИКТ.“;

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

„7. 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, различни от рисковете в областта на ИКТ, и методите за тестване на тези рискове, както и за тяхното преодоляване или свеждане до минимум, включително политиките за непрекъснатост на дейността и плановете за възстановяване от катастрофа, посочени в параграфи 3 и 4, както и методите за тяхната оценка.“

Член 62

Изменения на Регламент (ЕС) № 600/2014

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

1) Член 27ж се изменя, както следва:

а) параграф 4 се заменя със следното:

„4. ОМП отговаря на изискванията относно сигурността на мрежовите и информационните системи, определени в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета (*).

_____

(*) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).“;

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

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

2) Член 27з се изменя, както следва:

а) параграф 5 се заменя със следното:

„5. ДКД отговаря на изискванията относно сигурността на мрежовите и информационните системи, определени в Регламент (ЕС) 2022/2554.“;

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 заменя със следното:

„3. ОМД отговаря на изискванията относно сигурността на мрежовите и информационните системи, определени в Регламент (ЕС) 2022/2554.“;

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

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

Член 63

Изменение на Регламент (ЕС) 2016/1011

В член 6 от Регламент (ЕС) 2016/1011 се добавя следният параграф:

„6. Администраторите на критични бенчмаркове 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 съгласно Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета (*).

_____

(*) Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1).“

Член 64

Влизане в сила и прилагане

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

Прилага се от 17 януари 2025 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Страсбург на 14 декември 2022 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
R. METSOLA	M. BEK