I

(Резолюции, препоръки и становища)

ПРЕПОРЪКИ

ЕВРОПЕЙСКИ СЪВЕТ ЗА СИСТЕМЕН РИСК

ПРЕПОРЪКА НА ЕВРОПЕЙСКИЯ СЪВЕТ ЗА СИСТЕМЕН РИСК

от 2 декември 2021 година

относно общоевропейската рамка за координация на системни киберинциденти за съответните органи

(ЕССР/2021/17)

(2022/C 134/01)

ГЕНЕРАЛНИЯТ СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪВЕТ ЗА СИСТЕМЕН РИСК,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Споразумението за Европейското икономическо пространство ([1]), и по-специално приложение IX към него,

Като взе предвид Регламент (ЕС) № 1092/2010 на Европейския парламент и на Съвета от 24 ноември 2010 г. за пруденциалния надзор върху финансовата система на Европейския съюз на макроравнище и за създаване на Европейски съвет за системен риск ([2]), и по-специално член 3, параграф 2, буква б) и буква г) и членове16 и 18 от него,

като взе предвид Решение ЕССР/2011/1 на Европейския съвет за системен риск от 20 януари 2011 г. за приемане на процедурен правилник на Европейския съвет за системен риск ([3]), и по-специално членове 18—20 от него,

като има предвид, че:

(1) Както е посочено в съображение 4 от Препоръка ЕССР/2013/1 на Европейския съвет за системен риск ([4]), основната цел на макропруденциалната политика е да допринася за запазването на стабилността на финансовата система като цяло, включително чрез укрепване на устойчивостта на финансовата система и чрез намаляване на натрупването на системни рискове, като по този начин се осигурява устойчив принос на финансовия сектор към икономическия растеж. Европейският съвет за системен риск (ЕССР) отговаря за макропруденциалния надзор на финансовата система в рамките на Съюза. При изпълнението на своя мандат ЕССР следва да допринася за предотвратяването и смекчаването на системните рискове за финансовата стабилност, включително тези, свързани с киберинциденти, и да предлага как тези рискове могат да бъдат смекчени.

(2) Съществените киберинциденти могат да породят системен риск за финансовата система, като се има предвид техният потенциал да нарушават критични финансови услуги и операции. Усилването на първоначалния шок може да възникне или чрез оперативно или финансово разпространение, или чрез подкопаване на доверието във финансовата система. Ако финансовата система не е в състояние да поеме тези шокове, финансовата стабилност ще бъде изложена на риск и тази ситуация може да доведе до системна киберкриза ([5]).

([1]) ОВ L 1, 3.1.1994 г, стр. 3.
([2]) ОВ L 331, 15.12.2010 г., стр. 1.
([3]) ОВ C 58, 24.2.2011 г., стр. 4.
([4]) Препоръка ЕССР/2013/1 на Европейския съвет за системен риск от 4 април 2013 г. относно междинните цели и инструментите на макропруденциалната политика (ОВ C 170, 15.6.2013 г., стр. 1).
([5]) Виж Системен киберриск, ЕССР, февруари 2020 г., достъпен на уебсайта на ЕССР www.esrb.europa.eu.

(3) Постоянно развиващата се картина на киберзаплахи и неотдавнашното увеличаване на съществените киберинциденти са показатели за по-голям риск за финансовата стабилност в Съюза. Пандемията от COVID-19 подчерта значението на ролята, която играе технологията, за да позволи на финансовата система да функционира. Съответните органи и институции трябваше да адаптират своята техническа инфраструктура и рамки за управление на риска към внезапното увеличаване на дистанционната работа, което увеличи цялостното излагане на финансовата система на киберзаплахи и позволи на престъпниците както да изработят нови начини на действие, така и да адаптират съществуващите, за да се възползват от ситуацията ([6]). В този контекст броят на киберинцидентите, докладвани на банковия надзор на ЕЦБ през 2020 г., се е увеличил с 54 % в сравнение с 2019 г ([7])..

(4) Потенциално големият мащаб, скоростта и нивото на разпространение на съществени киберинциденти изискват ефективен отговор от съответните органи, за да се смекчат потенциалните отрицателни последици за финансовата стабилност. Бързата координация и комуникация между съответните органи на равнището на Съюза могат да подпомогнат ранната оценка на въздействието на съществен киберинцидент върху финансовата стабилност, поддържайки доверието във финансовата система и ограничавайки разпространението към други финансови институции и по този начин допринасят за предотвратяване на превръщането на съществен киберинцидент в риск за финансовата стабилност.

(5) Базисният шок възниква по нов начин в сравнение с традиционните финансови и ликвидни кризи, пред които обикновено се изправят съответните органи. Освен финансовите аспекти, цялостната оценка на риска трябва да включва мащаба и въздействието на оперативните смущения, тъй като те могат да повлияят на избора на макропруденциални инструменти. По същия начин финансовата стабилност може да повлияе и върху избора от страна на киберексперти на оперативни смекчаващи средства. Това изисква тясна и бърза координация и открита комуникация с цел, наред с другото, изграждане на ситуационна осведоменост.

(6) Рискът от неуспех на координацията от страна на органите съществува и трябва да бъде преодолян. Съответните органи в Съюза ще трябва да се координират помежду си и с други органи, като Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), с които може обикновено да не си взаимодействат. Тъй като значителен брой финансови институции на Съюза извършват дейност по света, съществен киберинцидент вероятно няма да бъде ограничен до Съюза или може да бъде предизвикан извън Съюза и може да изисква световна координация на отговора.

(7) Съответните органи трябва да бъдат подготвени за тези взаимодействия. В противен случай те могат да рискуват да предприемат несъгласувани действия, които противоречат или застрашават отговорите на други органи. Подобен неуспех на координацията би могъл да усили шока за финансовата система, като доведе до подкопаване на доверието във функционирането на финансовата система, което в най-лошия случай би породило риск за финансовата стабилност ([8]). Поради това следва да се предприемат необходимите стъпки за справяне с риска за финансовата стабилност, произтичащ от неуспеха на координацията в случай на съществен киберинцидент.

(8) В доклада на ЕССР (2021) „Смекчаване на системния киберриск“ ([9]) се установява необходимостта от създаване на общоевропейска рамка за координация на системните киберинциденти (ЕС-РКСКИ) за съответните органи в Съюза. Целта на ЕС-РКСКИ ще бъде да се увеличи нивото на подготвеност на съответните органи, за да се улесни координираният отговор при потенциално съществен киберинцидент. Докладът на ЕССР (2021) „Смекчаване на системния киберриск“ предоставя оценката на ЕССР относно характеристиките на рамката, които биха били необходими *prima facie* за справяне с риска от неуспех на координацията.

(9) Основната цел на настоящата препоръка е да се надгражда върху една от предвидените роли на Европейските надзорни органи (ЕНО) съгласно предложението за регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор ([10]) (наричан по-нататък „РОУЦТ“) — постепенно да позволи ефективен координиран отговор на равнището на Съюза в случай на съществен трансграничен инцидент, свързан с информационните и комуникационните технологии (ИКТ) или свързана с него заплаха, който има системно въздействие върху финансовия сектор на Съюза като цяло. Този процес ще доведе до създаването на ЕС-РКСКИ за съответните органи.

([6]) Виж Оценка на заплахата от организираната престъпност в интернет, Европол, 2020 г., достъпна на уебсайта на Европол www.europol.europa.eu.

([7]) Виж ИТ и киберриск: постоянно предизвикателство, ЕЦБ, 2021 г., достъпно на уебсайта на Банков надзор в ЕЦБ www.bankingsupervision.europa.eu.

([8]) Виж Системен киберриск, ЕССР, февруари 2020 г., достъпен на уебсайта на ЕССР www.esrb.europa.eu.

([9]) Виж Смекчаване на системния киберриск, ЕССР, 2021, предстоящ).

([10]) COM (2020) 595 final.

(10) ЕС-РКСКИ не следва да има за цел да замени съществуващите рамки, а да преодолее всякакви пропуски в координацията и комуникацията между съответните органи и с други органи в Съюза, и други ключови участници на международно равнище. В това отношение следва да се разгледа позиционирането на ЕС-РКСКИ в съществуващата рамка за финансовата криза и рамката на Съюза за киберинциденти. Относно координацията между съответните органи, следва да се разгледат, но не само, ролите и дейностите на групата за сътрудничество в областта на мрежите и информационните системи (МИС) за финансовите субекти съгласно Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([11]), и механизмите за координация, предвидени чрез създаването на съвместно киберзвено, наред с участието на АЕСМИС.

(11) По-специално предложението за започване на подготовката на ЕС-РКСКИ има за цел да подкрепи потенциалните роли на ЕНО, както е предвидено в предложението за РОУЦТ. РОУЦТ предлага „ЕНО, чрез съвместния комитет и в сътрудничество с компетентните органи, Европейската централна банка (ЕЦБ) и ЕССР, могат да създадат механизми, за споделяне на ефективните практики сред финансовите сектори, за да се повишава осведомеността за възникващите ситуации и да се установят общите за секторите уязвими места и рискове, свързани с кибернетичното пространство“ и „могат да разработят симулационни сценарии за управление на кризи и действие при извънредни ситуации в резултат на кибератаки, с цел да се изградят комуникационни канали и постепенно да се създадат условия за ефективни координирани ответни действия на равнище ЕС при мащабен трансграничен инцидент с ИКТ или свързана с него заплаха, които имат системно въздействие върху целия финансов сектор на Съюза“ ([12]). Все още не съществува общоевропейска рамка като ЕС-РКСКИ, и следва да бъде създадена и разработена в контекста на РОУЦТ.

(12) Като се има предвид рискът за финансовата стабилност в Съюза, произтичащ от киберриска, подготвителната работа за постепенното създаване на ЕС-РКСКИ следва, доколкото е възможно, да започне дори преди да е напълно приложима необходимата правна рамка и рамка на политиката за неговото създаване. Тази правна рамка и рамка на политиката ще бъде напълно завършена и финализирана, след като станат приложими съответните разпоредби на РОУЦТ и на делегираните актове към него.

(13) Ефективната комуникация допринася за ситуационната осведоменост сред съответните органи и поради това е необходима предпоставка за координация в целия Съюз по време на съществени киберинциденти. В това отношение следва да бъде определена комуникационната инфраструктура, необходима за координиране на отговора при съществен киберинцидент. Това означава да се посочи видът на информацията, която трябва да бъде споделяна, редовните канали, които да бъдат използвани за обмен на такава информация, и звената за контакт, с които следва да се обменя информация. При обмена на информация трябва да се спазват съществуващите правни изисквания. В допълнение, може да се наложи съответните органи да определят ясен план за действие и протоколи, които да бъдат следвани, за да се гарантира подходяща координация между органите, които участват в планирането на координиран отговор при съществен киберинцидент.

(14) Системна киберкриза ще изисква задействането на пълно сътрудничество на национално равнище и на равнището на Съюза. Поради това може да се предвиди определянето на звена за контакт за ЕНО, ЕЦБ и всяка държава членка измежду съответните ѝ национални органи, които следва да бъдат съобщени на ЕНО, за да се установят основните партньори в схемата за координация на ЕС-РКСКИ, които да бъдат информирани в случай на съществен киберинцидент. Необходимостта от определяне на звена за контакт следва да бъде оценена по време на разработването на ЕС-РКСКИ, като се вземе предвид определеното единно звено за контакт съгласно Директива (ЕС) 2016/1148, което държавите членки са създали относно сигурността на мрежите и информационните системи, за да се гарантира трансгранично сътрудничество с други държави членки и с групата за сътрудничество за МИС ([13]).

(15) Провеждането на учения за управление на кризи и извънредни ситуации би могло да улесни изпълнението на ЕС-РКСКИ и да позволи на органите да оценят готовността и подготовката си за системна киберкриза на равнището на Съюза. Тези учения ще предоставят на органите извлечените поуки и ще дадат възможност за непрекъснато подобряване и развитие на ЕС-РКСКИ.

([11]) 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).

([12]) Виж проекта на член 43 от предложението за РОУЦТ.

([13]) Виж Европейска комисия, Група за сътрудничество за МИС, достъпно на уебсайта на Европейската комисия www.ec.europa.eu.

(16) За развитието на ЕС-РКСКИ е от съществено значение ЕНО да извършат съвместно съответната подготвителна работа, за да разгледат потенциалните ключови елементи на рамката и необходимите ресурси и потребности, за да продължат с нейното разработване. След това ЕНО биха могли да започнат работа по предварителен анализ на всякакви пречки, които биха могли да възпрепятстват ЕНО и възможностите на съответните органи да създадат ЕС-РКСКИ и да споделят съответната информация чрез комуникационни канали в случай на съществен киберинцидент. Такъв анализ би бил важна стъпка за информиране за всички по-нататъшни действия както от законодателен характер или от други подкрепящи инициативи, които Европейската комисия може да предприеме на етапа на изпълнение след РОУЦТ,

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

РАЗДЕЛ 1

ПРЕПОРЪКИ

Препоръка А — Създаване на общоевропейска рамка за координация на системни киберинциденти (ЕС-РКСКИ)

1. Препоръчва се, както е предвидено в предложението на Комисията за регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор (наричан по-долу „РОУЦТ“), европейските надзорни органи (ЕНО), съвместно посредством Съвместния комитет, и заедно с Европейската централна банка (ЕЦБ), Европейския съвет за системен риск (ЕССР) и съответните национални органи, да започнат подготовка за постепенното разработване на ефективен координиран отговор на равнището на Съюза в случай на съществен трансграничен киберинцидент или свързана с него заплаха, които биха могли да имат системно въздействие върху финансовия сектор на Съюза. Подготвителната работа за координиран отговор на равнището на Съюза следва да доведе до постепенното разработване на ЕС-РКСКИ за ЕНО, ЕЦБ, ЕССР и съответните национални органи. Това следва да включва и оценка на необходимите ресурси за ефективното разработване на ЕС-РКСКИ.

2. Препоръчва се ЕНО да предприемат, предвид подпрепоръка А, параграф 1, в консултация с ЕЦБ и ЕССР, картографиране и последващ анализ на настоящите пречки, правните и други оперативни бариери пред ефективното разработване на ЕС-РКСКИ.

Препоръка Б — Създаване на звена за контакт на ЕС-РКСКИ

Препоръчва се ЕНО, ЕЦБ и всяка държава членка да определят измежду съответните си национални органи основно звено за контакт, което да бъде съобщено на ЕНО. Този списък с контакти ще улесни разработването на рамката и, след въвеждането на ЕС-РКСКИ, звената за контакт и ЕССР следва да бъдат информирани в случай на съществен киберинцидент. Следва също така да се предвиди координация между ЕС-РКСКИ и определеното единно звено за контакт съгласно Директива (ЕС) 2016/1148, което държавите членки са създали относно сигурността на мрежите и информационните системи, за да осигури трансгранично сътрудничество с други държави членки и с Групата за сътрудничество в областта на мрежите и информационните системи.

Препоръка В — Подходящи мерки на равнището на Съюза

Въз основа на резултатите от анализите, извършени в съответствие с препоръка А, се препоръчва Комисията да разгледа подходящите мерки, необходими за осигуряване на ефективна координация на отговорите при системни киберинциденти.

РАЗДЕЛ 2

ИЗПЪЛНЕНИЕ

1. **Определения**

За целите на настоящата препоръка се прилагат следните определения:

а) „кибер“ означава свързано с, в рамките на или чрез средата на взаимосвързаната информационна инфраструктура за взаимодействия между лица, процеси, данни и информационни системи ([14]);

([14]) Виж Кибер речник, Съвет за финансова стабилност, 12 ноември 2018 г., достъпен на уебсайта на Съвета за финансова стабилност www.fsb.org.

б) „съществен киберинцидент“ означава инцидент, свързан с ИКТ с потенциално голямо неблагоприятно въздействие върху мрежите и информационните системи, които поддържат критичните функции на финансовите субекти ([15]);

в) „системна киберкриза“ означава съществен киберинцидент, който причинява ниво на сътресение във финансовата система на Съюза, което потенциално води до сериозни отрицателни последици за гладкото функциониране на вътрешния пазар и функционирането на реалната икономика. Такава криза би могла да възникне в резултат на съществен киберинцидент, който причинява шокове по редица канали, включително оперативни, финансови и канали на доверието;

г) „Европейски надзорни органи“ или „ЕНО“ означава Европейският надзорен орган (Европейски банков орган), създаден с Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета ([16]), заедно с Европейския надзорен орган (Европейски орган за застраховане и професионално пенсионно осигуряване), създаден с Регламент (ЕС) № 1094/2010 на Европейския парламент и на Съвета ([17]) и Европейския надзорен орган (Европейски орган за ценни книжа и пазари), създаден с Регламент (ЕС) № 1095/2010 на Европейския парламент и на Съвета ([18]);

д) „Съвместен комитет“ означава Съвместният комитет на европейските надзорни органи, създаден съгласно член 54 от Регламент (ЕС) № 1093/2010, от Регламент (ЕС) № 1094/2010 и от Регламент (ЕС) № 1095/2010;

е) „съответен национален орган“ означава:

1. компетентен или надзорен орган в държава членка, както е посочено в актовете на Съюза, посочени в член 1, параграф 2 от Регламент (ЕС) № 1093/2010, Регламент (ЕС) № 1094/2010 и Регламент (ЕС) № 1095/2010, и всеки друг национален компетентен орган, както е посочено в актовете на Съюза, с които на ЕНО се възлагат задачи;

2. компетентен орган в държава членка, определен в съответствие с:

i. член 4 от Директива № 2013/36/ЕС на Европейския парламент и на Съвета ([19]), без да се засягат специфичните задачи, възложени на ЕЦБ с Регламент (ЕС) № 1024/2013 на Съвета ([20]);

ii. член 22 от Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета ([21]);

iii. член 37 от Директива 2009/110/ЕО на Европейския парламент и на Съвета ([22]);

iv. член 4 от Директива (ЕС) 2019/2034 на Европейския парламент и на Съвета ([23]);

([15]) Виж точка 7 от проекта на член 3 от предложението за РОУЦТ.

([16]) 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).

([17]) 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).

([18]) 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).

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

([20]) 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).

([21]) 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).

([22]) 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).

([23]) Директива (ЕС) 2019/2034 на Европейския парламент и на Съвета от 27 ноември 2019 година 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).

v. член 3, параграф 1, буква дд), първо тире от предложението за регламент на Европейския парламент и на Съвета относно пазарите на криптоактиви и за изменение на Директива (ЕС) 2019/1937 ([24]);

vi. член 11 от Регламент (ЕС) № 909/2014 на Европейския парламент и на Съвета ([25]);

vii. член 22 от Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета ([26]);

viii. член 67 от Директива 2014/65/ЕС на Европейския парламент и на Съвета ([27]);

ix. член 22 от Регламент (ЕС) № 648/2012;

x. член 44 от Директива 2011/61/ЕС на Европейския парламент и на Съвета ([28]);

xi. член 97 от Директива 2009/65/ЕО на Европейския парламент и на Съвета ([29]);

xii. член 30 от Директива 2009/138/ЕО на Европейския парламент и на Съвета ([30]);

xiii. член 12 от Директива (ЕС) 2016/97 на Европейския парламент и на Съвета ([31]);

xiv. член 47 от Директива (ЕС) 2016/2341 на Европейския парламент и на Съвета ([32]);

xv. член 22 от Регламент (ЕС) № 1060/2009 на Европейския парламент и на Съвета ([33]);

xvi. член 3, параграф 2 и член 32 от Директива 2006/43/ЕО на Европейския парламент и на Съвета ([34]);

xvii. член 40 от Регламент (ЕС) № 2016/1011 на Европейския парламент и на Съвета ([35]);

xviii. член 29 от Регламент (ЕС) № 2020/1503 на Европейския парламент и на Съвета ([36]);

([24]) COM (2020) 593 final.

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) 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).

([30]) 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).

([31]) 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).

([32]) 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).

([33]) 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).

([34]) 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).

([35]) 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).

([36]) 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).

3. орган, на когото е възложено приемането и/или активирането на мерки на макропруденциалната политика или изпълнението на други задачи, свързани с финансовата стабилност, като например анализа, който се извършва в подкрепа на другите задачи, свързани с финансовата стабилност, включително, но не само:

   i. определеният орган съгласно Директива 2013/36/ЕС, дял VII, глава 4 или член 458, параграф 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета ([37]);

   ii. макропруденциалният орган с целите, правния режим, задачите, правомощията, инструментите, изискванията за отчетност и другите характеристики, изложени в Препоръка ЕССР/2011/3 на Европейския съвет за системен риск ([38]);

ж) „съответен орган“ означава:

1. ЕНО;

2. ЕЦБ за задачите, които са ѝ възложени в съответствие с членове 4, параграфи 1 и 2 и член 5, параграф 2 от Регламент (ЕС) № 1024/2013;

3. съответен национален орган.

2. **Критерии за изпълнение**

По отношение на изпълнението на настоящата препоръка се прилагат следните критерии:

а) да се обърне дължимото внимание на принципа на предоставяне на информация при необходимост и принципа на пропорционалност, като се вземат предвид целта и съдържанието на всяка препоръка;

б) да се изпълнят специфичните критерии за спазване, изложени в приложението, във връзка с всяка препоръка.

3. **Срок за последващи действия**

В съответствие с член 17, параграф 1 от Регламент (ЕС) № 1092/2010 адресатите трябва да уведомят Европейския парламент, Съвета, Комисията и ЕССР за действията, предприети в отговор на настоящата препоръка, или да обосноват всяко бездействие. От адресатите се изисква да представят такова съобщение при спазване на посочените по-долу срокове:

1. Препоръка А

   а) До 30 юни 2023 г., но не по-рано от шест месеца след влизането в сила на РОУЦТ, от ЕНО се изисква да представят на Европейския парламент, Съвета, Комисията и на ЕССР междинен доклад относно изпълнението на подпрепоръка А, параграф 1.

   б) До 30 юни 2024 г., но не по-рано от осемнадесет месеца след влизането в сила на РОУЦТ, от ЕНО се изисква да представят на Европейския парламент, Съвета, Комисията и на ЕССР окончателен доклад относно изпълнението на подпрепоръка А, параграф 1.

   в) До 30 юни 2025 г., но не по-рано от тридесет месеца след влизането в сила на РОУЦТ, от ЕНО се изисква да представят на Европейския парламент, Съвета, Комисията и на ЕССР доклад относно изпълнението на подпрепоръка А, параграф 2.

2. Препоръка Б

   До 30 юни 2023 г., но не по-рано от шест месеца след влизането в сила на РОУЦТ, от ЕНО, ЕЦБ и държавите членки се изисква да представят на Европейския парламент, Съвета, Комисията и на ЕССР доклад относно изпълнението на препоръка Б.

3. Препоръка В

   а) До 31 декември 2023 г., но не по-рано от 12 месеца след влизането в сила на РОУЦТ, от Комисията се изисква да представи на Европейския парламент, Съвета и на ЕССР доклад относно изпълнението на препоръка В с оглед на междинния доклад на ЕНО в съответствие с подпрепоръка А, параграф 1.

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

([38]) Препоръка ЕССР/2011/3 на Европейския съвет за системен риск от 22 декември 2011 г. относно макропруденциалния мандат на националните органи (ОВ C 41, 14.2.2012 г., стр. 1).

б) До 31 декември 2025 г., но не по-рано от 36 месеца след влизането в сила на РОУЦТ, от Комисията се изисква да представи на Европейския парламент, Съвета и на ЕССР доклад относно изпълнението на препоръка В с оглед на докладите на ЕНО в съответствие с препоръка А.

4. **Наблюдение и оценка**

1. Секретариатът на ЕССР:

а) подпомага адресатите, като осигурява координацията на процеса на докладване и предоставянето на съответните образци, и когато е необходимо, определя процедурата и срока за последващи действия;

б) проверява последващите действия на адресатите, подпомага ги при поискване от тяхна страна и представя докладите за последващите действия на Генералния съвет. Сроковете за започването на оценките са следните:

i) в срок от 12 месеца след влизането в сила на РОУЦТ, по отношение на изпълнението на препоръки А и Б;

ii) в срок от 18 месеца след влизането в сила на РОУЦТ, по отношение на изпълнението на препоръка В;

iii) в срок от 24 месеца след влизането в сила на РОУЦТ, по отношение на изпълнението на препоръка А;

iv) в срок от 36 месеца след влизането в сила на РОУЦТ, по отношение на изпълнението на препоръка А;

v) в срок от 42 месеца след влизането в сила на РОУЦТ, по отношение на изпълнението на препоръка В;

2. Генералният съвет извършва оценка на действията и обосновките, за които са го уведомили адресатите, и ако е уместно, може да реши, че настоящата препоръка не е била спазена и че адресатът не е предоставил подходяща обосновка за бездействието си.

Съставено във Франкфурт на Майн на 2 декември 2021 година.

Ръководител на секретариата на ЕССР,
от името на Генералния съвет на ЕССР,
Francesco MAZZAFERRO

ПРИЛОЖЕНИЕ

КРИТЕРИИ ЗА СПАЗВАНЕ НА ПРЕПОРЪКИТЕ

Препоръка А — Създаване на общоевропейска рамка за координация на системни киберинциденти (ЕС-РКСКИ)

За подпрепоръка А, параграф 1 се определят следните критерии за спазване:

1. При подготовката на ефективен координиран отговор на равнището на Съюза, който следва да доведе до постепенно разработване на ЕС-РКСКИ чрез упражняване на правомощията, предвидени в бъдещия регламент на Европейския парламент и на Съвета относно оперативната устойчивост на цифровите технологии във финансовия сектор (наричан по-нататък „РОУЦТ“), Европейските надзорни органи (ЕНО), действащи чрез Съвместния комитет, и заедно с Европейската централна банка (ЕЦБ), Европейския съвет за системен риск (ЕССР) и съответните национални органи, и след консултации с Агенцията на Европейския съюз за мрежова и информационна сигурност и Комисията, когато счете за необходимо, следва да обмислят включването в предвидената подготовка за ЕС-РКСКИ най-малко на следните аспекти:

   а) анализ на необходимите ресурси за ефективно разработване на ЕС-РКСКИ;

   б) разработване на учения за управление на кризи и извънредни ситуации, включващи сценарии за кибератака, с оглед разработване на канали за комуникация;

   в) разработване на общ речник;

   г) разработване на съгласувана класификация на киберинцидентите;

   д) създаване на сигурни и надеждни канали за обмен на информация, включително резервни системи;

   е) създаване на звена за контакт;

   ж) да се обърне внимание на поверителността при обмена на информация;

   з) инициативи за сътрудничество и обмен на информация с киберразузнаването във финансовия сектор;

   и) разработване на ефективни процеси на активиране и поетапни процеси чрез ситуационна осведоменост;

   й) изясняване на отговорностите на участниците в рамката;

   к) разработване на интерфейси за междусекторна координация и, когато е уместно, за координация с трети държави;

   л) осигуряване на съгласувана комуникация от съответните органи с обществеността за запазване на доверието;

   м) създаване на предварително определени комуникационни линии за своевременна комуникация;

   н) извършване на подходящи учения за тестване на рамката, включително тестване между юрисдикции и координация с трети държави, и оценки, които водят до извлечени поуки и развитие на рамката;

   о) осигуряване на ефективна комуникация и мерки за противодействие срещу дезинформацията.

Препоръка Б — Създаване на звена за контакт на ЕС-РКСКИ

За препоръка Б се определят следните критерии за съответствие:

1. ЕНО, ЕЦБ и всяка държава членка сред съответните си национални органи следва да постигнат съгласие по общ подход за обмен и актуализиране на списъка на определените звена за контакт на ЕС-РКСКИ.

2. Определянето на звено за контакт следва да бъде оценено, като се вземе предвид определеното единно звено за контакт съгласно Директива (ЕС) 2016/1148, което държавите членки са създали по отношение на сигурността на мрежите и информационните системи, за да се гарантира трансгранично сътрудничество с други държави членки и с Групата за сътрудничество в областта на мрежите и информационните системи.

Препоръка В – Промени в правната рамка на Съюза

За препоръка В се определя следният критерий за съответствие:

Комисията следва да обмисли дали са необходими мерки, включително промени в съответното законодателство на Съюза, в резултат на анализа, извършен в съответствие с препоръка А, за да се гарантира, че ЕНО, чрез Съвместния комитет и заедно с ЕЦБ, ЕССР и съответните национални органи, могат да разработят ЕС-РКСКИ в съответствие с подпрепоръка А, параграф 1 и да се гарантира, че ЕНО, ЕЦБ, ЕССР и съответните национални органи, както и други органи, могат да участват в координационни действия и обмен на информация, които са достатъчно подробни и последователни, за да подкрепят ефективен ЕС-РКСКИ.