II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2023/203 НА КОМИСИЯТА

от 27 октомври 2022 година

за определяне на правила за прилагането на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за управление на рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност за организациите, обхванати от регламенти (ЕС) № 1321/2014, (ЕС) № 965/2012, (ЕС) № 1178/2011, (ЕС) 2015/340 на Комисията, регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията, и за компетентните органи, обхванати от регламенти (ЕС) № 748/2012, (ЕС) № 1321/2014, (ЕС) № 965/2012, (ЕС) № 1178/2011, (ЕС) 2015/340 и (ЕС) № 139/2014 на Комисията, регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията, и за изменение на регламенти (ЕС) № 1178/2011, (ЕС) № 748/2012, (ЕС) № 965/2012, (ЕС) № 139/2014, (ЕС) № 1321/2014, (ЕС) 2015/340 на Комисията и регламенти за изпълнение (ЕС) 2017/373 и (ЕС) 2021/664 на Комисията

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета от 4 юли 2018 г. относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за изменение на регламенти (ЕО) № 2111/2005, (ЕО) № 1008/2008, (ЕС) № 996/2010, (ЕС) № 376/2014 и на директиви 2014/30/ЕС и 2014/53/ЕС на Европейския парламент и на Съвета, и за отмяна на регламенти (ЕО) № 552/2004 и (ЕО) № 216/2008 на Европейския парламент и на Съвета и Регламент (ЕИО) № 3922/91 на Съвета [1], и по-специално член 17, параграф 1, буква б), член 27, параграф 1, буква а), член 31, параграф 1, буква б), член 43, параграф 1), буква б), член 53, параграф 1, буква а) и член 62, параграф 15, буква в) от него,

като има предвид, че:

(1) В съответствие със съществените изисквания, определени в приложение II, точка 3.1, буква б) към Регламент (ЕС) 2018/1139, организациите за управление на поддържането на летателната годност и организациите за техническо обслужване трябва да въведат и поддържат система за управление с цел управление на рисковете за безопасността.

(2) Също така в съответствие със съществените изисквания, определени в приложение IV, точка 3.3, буква б) и точка 5, буква б) към Регламент (ЕС) 2018/1139, организациите за обучение на пилоти, организациите за обучение на кабинен екипаж, авиомедицинските центрове за летателен състав и операторите на летателни тренажори трябва да въведат и поддържат система за управление на рисковете за безопасността.

(3) Освен това в съответствие със съществените изисквания, определени в приложение V, точка 8.1, буква в) към Регламент (ЕС) 2018/1139, операторите на въздухоплавателни средства трябва да въведат и поддържат система за управление с цел управление на рисковете за безопасността.

(4) Също така в съответствие със съществените изисквания, определени в приложение VIII, точка 5.1, буква в) и точка 5.4, буква б) към Регламент (ЕС) 2018/1139, доставчиците на услуги по управление на въздушното движение и аеронавигационно обслужване, доставчиците на обслужване за U-space и единствените доставчици на общо информационно обслужване, както и организациите за обучение и авиомедицинските центрове за ръководители на полети трябва да въведат и поддържат система за управление на рисковете за безопасността.

[1] ОВ L 212, 22.8.2018 г., стр. 1.

(5) Тези рискове за безопасността могат да произтичат от различни източници, като например недостатъци при проектирането и техническото обслужване, аспекти, свързани с възможностите на човека, заплахи за околната среда и за информационната сигурност. Поради това системите за управление, въведени от Агенцията за авиационна безопасност на Европейския съюз („Агенцията“) и националните компетентни органи и организациите, посочени в съображенията по-горе, следва да отчитат не само рисковете за безопасността, произтичащи от случайни събития, но и рисковете за безопасността, произтичащи от заплахи за информационната сигурност, при които съществуващите недостатъци могат да бъдат използвани от злонамерени лица. Тези рискове за информационната сигурност постоянно нарастват в гражданското въздухоплаване, тъй като настоящите информационни системи стават все по-взаимосвързани и все по-често са мишена на злонамерени лица.

(6) Рисковете, свързани с тези информационни системи, не се ограничават до възможни атаки срещу киберпространството, а обхващат и заплахи, които могат да засегнат процесите и процедурите, както и възможностите на човека.

(7) Значителен брой организации вече използват международни стандарти, като например ISO 27001, за да обезпечат сигурността на цифровата информация и цифровите данни. Възможно е обаче тези стандарти да не отговарят напълно на всички особености на гражданското въздухоплаване. Следователно е целесъобразно да се определят изисквания за управление на рисковете за информационната сигурност, които биха могли да имат потенциално въздействие върху авиационната безопасност.

(8) От съществено значение е тези изисквания да обхващат всички области на въздухоплаването и техните връзки, тъй като въздухоплаването представлява система от силно взаимосвързани системи. Поради това те следва да се прилагат за всички организации и компетентни органи, обхванати от регламенти (ЕС) № 748/2012 ([2]), (ЕС) № 1321/2014 ([3]), (ЕС) № 965/2012 ([4]), (ЕС) № 1178/2011 ([5]), (ЕС) 2015/340 ([6]), (ЕС) № 139/2014 ([7]) на Комисията и Регламент за изпълнение (ЕС) 2021/664 на Комисията ([8]), както и за тези, от които вече се изисква да имат система за управление в съответствие със съществуващото законодателство на Съюза в областта на авиационната безопасност. Независимо от това някои организации следва да бъдат изключени от обхвата на настоящия регламент, за да се осигури съответна пропорционалност на по-ниските рискове за информационната сигурност, които те представляват за авиационната система.

(9) Изискванията, определени в настоящия регламент, следва да се прилагат последователно във всички области на въздухоплаването, като същевременно оказват минимално въздействие върху законодателството на Съюза в областта на авиационната безопасност, което вече е приложимо в тези области.

([2]) Регламент (ЕС) № 748/2012 на Комисията от 3 август 2012 г. за определяне на правила за прилагане на сертифициране за летателна годност и за опазване на околната среда на въздухоплавателни средства и свързани с тях продукти, части и оборудване, както и за сертифициране на проектантски и производствени организации (ОВ L 224, 21.8.2012 г., стр. 1).

([3]) Регламент (ЕС) № 1321/2014 на Комисията от 26 ноември 2014 г. относно поддържането на летателната годност на въздухоплавателните средства и авиационните продукти, части и устройства и относно одобряването на организациите и персонала, изпълняващи тези задачи (ОВ L 362, 17.12.2014 г., стр. 1).

([4]) Регламент (ЕС) № 965/2012 на Комисията от 5 октомври 2012 г. за определяне на технически изисквания и административни процедури във връзка с въздушните операции в съответствие с Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета (ОВ L 296, 25.10.2012 г., стр. 1).

([5]) Регламент (ЕС) № 1178/2011 на Комисията от 3 ноември 2011 г. за определяне на технически изисквания и административни процедури във връзка с екипажите на въздухоплавателни средства в гражданското въздухоплаване в съответствие с Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета (ОВ L 311, 25.11.2011 г., стр. 1).

([6]) Регламент (ЕС) 2015/340 на Комисията от 20 февруари 2015 г. за определяне на технически изисквания и административни процедури във връзка със свидетелствата за правоспособност и други свидетелства и сертификати на ръководители на полети съгласно Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета, за изменение на Регламент за изпълнение (ЕС) № 923/2012 на Комисията и за отмяна на Регламент (ЕС) № 805/2011 на Комисията (ОВ L 63, 6.3.2015 г., стр. 1).

([7]) Регламент (ЕС) № 139/2014 на Комисията от 12 февруари 2014 година за определяне на изискванията и административните процедури във връзка с летищата в съответствие с Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета (ОВ L 44, 14.2.2014 г., стр. 1).

([8]) Регламент за изпълнение (ЕС) 2021/664 на Комисията от 22 април 2021 г. относно регулаторната рамка за U-space (ОВ L 139, 23.4.2021 г, стр. 161).

(10) Изискванията, определени в настоящия регламент, не следва да засягат изискванията за информационна сигурност и киберсигурност, определени в точка 1.7 от приложението към Регламент за изпълнение (ЕС) 2015/1998 на Комисията ([9]) и в член 14 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([10]).

(11) Изискванията за сигурност, определени в членове 33—43 от дял V „Сигурност на програмата“ от Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета ([11]) се считат за еквивалентни на изискванията, определени в настоящия регламент, освен по отношение на точка IS.I.OR.230 от приложение II към настоящия регламент, която следва да бъде спазена.

(12) За да се осигури правна сигурност, тълкуването на термина „информационна сигурност“ съгласно определението му в настоящия регламент, което отразява общата му употреба в гражданското въздухоплаване в световен мащаб, следва да се счита за съвместимо с тълкуването на термина „сигурност на мрежите и информационните системи“ съгласно определението в член 4, точка 2 от Директива (ЕС) 2016/1148. Определението за информационна сигурност, използвано за целите на настоящия регламент, не следва да се тълкува като различаващо се от определението за сигурност на мрежите и информационните системи, установено в Директива (ЕС) 2016/1148.

(13) За да се избегне дублиране на правните изисквания, когато организациите, обхванати от настоящия регламент, вече са предмет на изисквания за сигурност, произтичащи от актове на Съюза, посочени в съображения (10) и 11, които по своето действие са равностойни на разпоредбите, установени в настоящия регламент, спазването на тези изисквания за сигурност следва да се счита за съответствие с изискванията, установени в настоящия регламент.

(14) Организациите, обхванати от настоящия регламент, които вече са предмет на изискванията за сигурност, произтичащи от Регламент за изпълнение (ЕС) 2015/1998 или Регламент (ЕС) 2021/696, или и от двата регламента, следва също да отговарят на изискванията на приложение II (част IS.I.OR.230 „Схема за външно докладване във връзка с информационната сигурност“) към настоящия регламент, тъй като и двата регламента не съдържат разпоредби по отношение на външното докладване на инциденти, свързани с информационната сигурност.

(15) С оглед на изчерпателността регламенти (ЕС) № 1178/2011, (ЕС) № 748/2012, (ЕС) № 965/2012, (ЕС) № 139/2014, (ЕС) № 1321/2014, (ЕС) 2015/340 и регламенти за изпълнение (ЕС) 2017/373 ([12]) и (ЕС) 2021/664 следва да бъдат изменени, за да се въведат изискванията за системите за управление на информационната сигурност, предвидени в настоящия регламент, заедно с посочените в него системи за управление, и да се определят изискванията на компетентните органи по отношение на надзора над организациите, прилагащи горепосочените изисквания за управление на информационната сигурност.

(16) С цел да се предостави на организациите достатъчно време, за да осигурят спазването на новите правила и процедури, настоящият регламент следва да започне да се прилага 3 години след влизането му в сила, с изключение на доставчика на аеронавигационно обслужване на Европейската геостационарна служба за навигационно покритие (EGNOS), определен в Регламент за изпълнение (ЕС) 2017/373, когато поради продължаващата акредитация на системата и услугите на EGNOS по отношение на сигурността в съответствие с Регламент (ЕС) 2021/696, той следва да започне да се прилага от 1 януари 2026 г.

(17) Изискванията, определени в настоящия регламент, се основават на Становище № 03/2021 ([13]), издадено от Агенцията в съответствие с член 75, параграф 2, букви б) и в) и член 76, параграф 1 от Регламент (ЕС) 2018/1139.

([9]) Регламент за изпълнение (ЕС) 2015/1998 на Комисията от 5 ноември 2015 г. за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването (ОВ L 299, 14.11.2015 г., стр. 1).

([10]) 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).

([11]) Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета от 28 април 2021 г. за създаване на космическа програма на Съюза и Агенция на Европейския съюз за космическата програма и за отмяна на регламенти (ЕС) № 912/2010, (ЕС) № 1285/2013 и (ЕС) № 377/2014 и на Решение № 541/2014/ЕС (ОВ L 170, 12.5.2021 г., стр. 69).

([12]) Регламент за изпълнение (ЕС) 2017/373 на Комисията от 1 март 2017 г. за определяне на общи изисквания за доставчиците на услуги и надзора при управлението на въздушното движение/аеронавигационното обслужване и други мрежови функции за управление на въздушното движение, за отмяна на Регламент (ЕО) № 482/2008 и на регламенти за изпълнение (ЕС) № 1034/2011, (ЕС) № 1035/2011 и (ЕС) 2016/1377, както и за изменение на Регламент (ЕС) № 677/2011 (ОВ L 62, 8.3.2017 г., стр. 1).

([13]) https://www.easa.europa.eu/document-library/opinions

(18) Изискванията, определени в настоящия регламент, са в съответствие със становището на комитета за прилагане на общите правила за безопасност в областта на гражданското въздухоплаване, създаден с член 127 от Регламент (ЕС) 2018/1139,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет

С настоящия регламент се определят изискванията, на които трябва да отговарят организациите и компетентните органи, за да:

а) идентифицират и управляват рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност, които биха могли да засегнат системите на информационните и комуникационните технологии и данни, използвани за целите на гражданското въздухоплаване;

б) откриват събития, свързани с информационната сигурност, и да идентифицират тези, които се считат за инциденти, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност;

в) реагират на тези инциденти, свързани с информационната сигурност, и да се възстановяват от тях.

Член 2

Приложно поле

1. Настоящият регламент се прилага по отношение на следните организации:

а) организации за техническо обслужване, които са предмет на раздел А от приложение II (част 145) към Регламент (ЕС) № 1321/2014, с изключение на тези, които участват единствено в техническото обслужване на въздухоплавателни средства в съответствие с приложение Vб (част ML) към Регламент (ЕС) № 1321/2014;

б) организации за управление на поддържането на летателната годност (CAMO), които са предмет на раздел А от приложение Vв (част CAMO) към Регламент (ЕС) № 1321/2014, с изключение на тези, които участват единствено в управлението на поддържането на летателната годност на въздухоплавателни средства в съответствие с приложение Vб (част ML) към Регламент (ЕС) № 1321/2014;

в) оператори на въздухоплавателни средства, които са предмет на приложение III (част ORO) към Регламент (ЕС) № 965/2012, с изключение на тези, които участват единствено в експлоатацията на някое от следните въздухоплавателни средства:

i) въздухоплавателно средство ELA 2, както е определено в член 1, параграф 2, буква й) от Регламент (ЕС) № 748/2012;

ii) витлови самолети с един двигател, с максимална оперативна конфигурация на пътническите места от 5 или по-малко места, които не са класифицирани като сложни въздухоплавателни средства с моторна тяга, когато излитат и кацат на едно и също летище или на една и съща експлоатационна площадка и се експлоатират по правилата за визуални полети (VFR) през деня;

iii) вертолети с един двигател, с максимална оперативна конфигурация на пътническите места от 5 или по-малко места, които не са класифицирани като сложни въздухоплавателни средства с моторна тяга, когато излитат и кацат на едно и също летище или на една и съща експлоатационна площадка и се експлоатират по правилата за визуални полети (VFR) през деня.

г) одобрени организации за обучение (ATO), които са предмет на приложение VII (част ORA) към Регламент (ЕС) № 1178/2011, с изключение на тези, които участват единствено в дейности по обучение за въздухоплавателни средства ELA2 съгласно определението в член 1, параграф 2, буква й) от Регламент (ЕС) № 748/2012 или участват единствено в теоретично обучение;

д) авиомедицински центрове за екипажи на въздухоплавателни средства, които са предмет на приложение VII (част ORA) към Регламент (ЕС) № 1178/2011;

е) оператори на летателни тренажори (FSTD), които са предмет на приложение VII (част ORA) към Регламент (ЕС) № 1178/2011, с изключение на тези, които участват единствено в експлоатацията на FSTD за въздухоплавателни средства ELA2 съгласно определението в член 1, параграф 2, буква й) от Регламент (ЕС) № 748/2012;

ж) организации за обучение на ръководители на полети (ATCO TO) и авиомедицински центрове на ATCO, които са предмет на приложение III (част ATCO.OR) към Регламент (ЕС) 2015/340;

з) организации, които са предмет на приложение III (част ATM/ANS.OR) към Регламент за изпълнение (ЕС) 2017/373, с изключение на следните доставчици на услуги:

i) доставчици на аеронавигационно обслужване, които притежават ограничен сертификат в съответствие с точка ATM/ANS.OR.A.010 от посоченото приложение;

ii) доставчици на полетно-информационно обслужване, които декларират своите дейности в съответствие с точка ATM/ANS.OR.A.015 от посоченото приложение;

и) доставчици на обслужване за U-space и единствени доставчици на общо информационно обслужване съгласно Регламент (ЕС) 2021/664.

2. Настоящият регламент се прилага за компетентните органи, включително Агенцията за авиационна безопасност на Европейския съюз („Агенцията“), посочени в член 6 от настоящия регламент и в член 5 от Делегиран регламент (ЕС) 2022/1645 на Комисията ([14]).

3. Настоящият регламент се прилага и за компетентния орган, отговорен за издаването, продължаването, смяната, временното прекратяване или анулирането на лицензи за техническо обслужване на въздухоплавателни средства в съответствие с приложение III (част 66) към Регламент (ЕС) № 1321/2014.

4. Настоящият регламент не засяга изискванията за информационна сигурност и киберсигурност, определени в точка 1.7 от приложението към Регламент за изпълнение (ЕС) 2015/1998 и в член 14 от Директива (ЕС) 2016/1148.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) „информационна сигурност“ означава запазването на поверителността, целостта, автентичността и наличността на мрежите и информационните системи;

(2) „събитие, свързано с информационната сигурност“ означава установено събитие, свързано със система, услуга или мрежа, което показва възможно нарушение на политиката за информационна сигурност или отказ на контрола на информационната сигурност, или неизвестна преди това ситуация, която може да е от значение за информационната сигурност;

(3) „инцидент“ означава всяко събитие, което има действително неблагоприятно въздействие върху сигурността на мрежите и информационните системи съгласно определението в член 4, точка 7 от Директива (ЕС) 2016/1148;

(4) „риск за информационната сигурност“ означава риск за организационните операции на гражданското въздухоплаване, активи, физически лица и други организации, дължащ се на потенциала на събитие, свързано с информационната сигурност. Рисковете за информационната сигурност са свързани с вероятността при дадена заплаха да има възползване от уязвимостта на даден информационен актив или група от информационни активи;

([14]) Делегиран регламент (ЕС) 2022/1645 на Комисията от 14 юли 2022 година за определяне на правила за прилагането на Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета по отношение на изискванията за управление на рисковете за информационната сигурност с потенциално въздействие върху авиационната безопасност за организациите, обхванати от регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014 на Комисията, и за изменение на регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014 на Комисията (ОВ L 248, 26.9.2022 г., стр. 18).

(5) „заплаха“ означава потенциално нарушение на информационната сигурност, което съществува, когато е налице субект, обстоятелство, действие или събитие, които биха могли да причинят вреда;

(6) „уязвимост“ означава недостатък или слабост в актив или система, процедури, проект, изпълнение или мерки за информационна сигурност, с които може да се злоупотреби и които водят до нарушаване на политиката за информационна сигурност.

Член 4

Изисквания към организациите и компетентните органи

1. Организациите, посочени в член 2, параграф 1, отговарят на изискванията на приложение II (част IS.I.OR) към настоящия регламент.

2. Компетентните органи, посочени в член 2, параграфи 2 и 3, отговарят на изискванията на приложение I (част IS.AR) към настоящия регламент.

Член 5

Изисквания, произтичащи от друго законодателство на Съюза

1. Ако организация, посочена в член 2, параграф 1, отговаря на изискванията за сигурност, определени в съответствие с член 14 от Директива (ЕС) 2016/1148, които са равностойни на изискванията, определени в настоящия регламент, спазването на тези изисквания за сигурност се счита за съответствие с изискванията, определени в настоящия регламент.

2. Ако организация, посочена в член 2, параграф 1, е оператор или субект, посочен в националните програми за сигурност на гражданското въздухоплаване на държавите членки, определени в съответствие с член 10 от Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета ([15]), изискванията за киберсигурност, съдържащи се в точка 1.7 от приложението към Регламент за изпълнение (ЕС) 2015/1998, се считат за равностойни на изискванията, определени в настоящия регламент, с изключение на точка IS.I.OR.230 от приложение II към настоящия регламент, която трябва да бъде спазена.

3. Ако организацията, посочена в член 2, параграф 1, е доставчик на аеронавигационно обслужване на Европейската геостационарна служба за навигационно покритие (EGNOS), посочена в Регламент (ЕС) 2021/696, изискванията за сигурност, съдържащи се в членове 33—43 от дял V от посочения регламент, се считат за равностойни на изискванията, определени в настоящия регламент, с изключение на точка IS.I.OR.230 от приложение II към настоящия регламент, която трябва да бъде спазена.

4. Комисията, след консултация с Агенцията и групата за сътрудничество, посочена в член 11 от Директива (ЕС) 2016/1148, може да издаде насоки за оценка дали изискванията, определени в настоящия регламент и в Директива (ЕС) 2016/1148, са равностойни.

Член 6

Компетентен орган

1. Без да се засягат задачите, възложени на Съвета за акредитация на сигурността, посочен в член 36 от Регламент (ЕС) 2021/696, органът, отговарящ за сертифицирането и контрола за спазването на настоящия регламент, е:

а) по отношение на организациите, посочени в член 2, параграф 1, буква а) — компетентният орган, определен в съответствие с приложение II (част 145) към Регламент (ЕС) № 1321/2014;

б) по отношение на организациите, посочени в член 2, параграф 1, буква б) — компетентният орган, определен в съответствие с приложение Vв (част CAMO) към Регламент (ЕС) № 1321/2014;

([15]) Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ L 97, 9.4.2008 г., стр. 72).

в) по отношение на организациите, посочени в член 2, параграф 1, буква в) — компетентният орган, определен в съответствие с приложение III (част ORO) към Регламент (ЕС) № 965/2012;

г) по отношение на организациите, посочени в член 2, параграф 1, букви г)—е) — компетентният орган, определен в съответствие с приложение VII (част ORA) към Регламент (ЕС) № 1178/2011;

д) по отношение на организациите, посочени в член 2, параграф 1, буква ж) — компетентният орган, определен в съответствие с член 6, параграф 2 от Регламент (ЕС) 2015/340;

е) по отношение на организациите, посочени в член 2, параграф 1, буква з) — компетентният орган, определен в съответствие с член 4, параграф 1 от Регламент за изпълнение (ЕС) 2017/373;

ж) по отношение на организациите, посочени в член 2, параграф 1, буква и) — компетентният орган, определен в съответствие с член 14, параграф 1 или 2, според случая, от Регламент за изпълнение (ЕС) 2021/664.

2. За целите на настоящия регламент държавите членки могат да определят независим и автономен субект, който да изпълнява възложената роля и отговорности на компетентните органи, посочени в параграф 1. В този случай се определят мерки за координация между този субект и компетентните органи, както е посочено в параграф 1, за да се осигури ефективен контрол върху всички изисквания, които трябва да бъдат изпълнени от организацията.

3. Агенцията си сътрудничи в пълно съответствие с приложимите правила за пазене на тайна, защита на личните данни и защита на класифицираната информация с Агенцията на Европейския съюз за космическата програма (EUSPA) и със Съвета за акредитация на сигурността, посочен в член 36 от Регламент (ЕС) 2021/696, за да се осигури ефективен контрол върху изискванията, приложими към доставчика на аеронавигационно обслужване на EGNOS.

Член 7

Предоставяне на относима информация на компетентните органи за мрежите и информационните системи (МИС)

Съгласно настоящия регламент компетентните органи информират без неоправдано забавяне единното звено за контакт, определено в съответствие с член 8 от Директива (ЕС) 2016/1148, за всякаква относима информация, включена в уведомленията, подадени съгласно точка IS.I.OR.230 от приложение II към настоящия регламент и точка IS.D.OR.230 от приложение I към Делегиран регламент (ЕС) 2022/1645 от операторите на основни услуги, определени в съответствие с член 5 от Директива (ЕС) 2016/1148.

Член 8

Изменение на Регламент (ЕС) № 1178/2011

Приложения VI (част ARA) и VII (част ORA) към Регламент (ЕС) № 1178/2011 се изменят в съответствие с приложение III към настоящия регламент.

Член 9

Изменение на Регламент (ЕС) № 748/2012

Приложение I (част 21) към Регламент (ЕС) № 748/2012 се изменя в съответствие с приложение IV към настоящия регламент.

Член 10

Изменение на Регламент (ЕС) № 965/2012

Приложения II (част ARO) и III (част ORO) към Регламент (ЕС) № 965/2012 се изменят в съответствие с приложение V към настоящия регламент.

Член 11

Изменение на Регламент (ЕС) № 139/2014

Приложение II (част ADR.AR) към Регламент (ЕС) № 139/2014 се изменя в съответствие с приложение VI към настоящия регламент.

Член 12

Изменение на Регламент (ЕС) № 1321/2014

Приложения II (част 145), III (част 66) и Vв (част CAMO) към Регламент (ЕС) № 1321/2014 се изменят в съответствие с приложение VII към настоящия регламент.

Член 13

Изменение на Регламент (ЕС) 2015/340

Приложения II (част ATCO.AR) и III (част ATCO.OR) към Регламент (ЕС) 2015/340 се изменят в съответствие с приложение VIII към настоящия регламент.

Член 14

Изменение на Регламент за изпълнение (ЕС) 2017/373

Приложения II (част ATM/ANS.AR) и III (част ATM/ANS.OR) към Регламент за изпълнение (ЕС) 2017/373 се изменят в съответствие с приложение IX към настоящия регламент.

Член 15

Изменение на Регламент за изпълнение (ЕС) 2021/664

Регламент за изпълнение (ЕС) 2021/664 се изменя, както следва:

(1) в член 15, параграф 1, буква е) се заменя със следното:

„е) въвежда и поддържа система за управление на сигурността в съответствие с точка ATM/ANS.OR.D.010 от подчаст Г на приложение III към Регламент за изпълнение (ЕС) 2017/373 и система за управление на информационната сигурност в съответствие с приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

(2) в член 18 се добавя следната буква л):

„л) създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203.“;

Член 16

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

Той се прилага от 22 февруари 2026 г.

По отношение на доставчика на аеронавигационно обслужване EGNOS, за който се прилага Регламент за изпълнение (ЕС) 2017/373, той се прилага от 1 януари 2026 г.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 27 октомври 2022 година.

За Комисията

Председател

Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ I

ИНФОРМАЦИОННА СИГУРНОСТ — ИЗИСКВАНИЯ КЪМ ОРГАНА

[ЧАСТ IS.AR]

IS.AR.100 Обхват

IS.AR.200 Система за управление на информационната сигурност (ISMS)

IS.AR.205 Оценка на риска за информационната сигурност

IS.AR.210 Третиране на риска за информационната сигурност

IS.AR.215 Инциденти, свързани с информационната сигурност — откриване, реагиране и възстановяване

IS.AR.220 Възлагане на дейности по управление на информационната сигурност на подизпълнители

IS.AR.225 Изисквания към персонала

IS.AR.230 Водене на документация

IS.AR.235 Постоянно подобряване

IS.AR.100 Обхват

В настоящата част се определят изискванията за управление, на които трябва да отговарят компетентните органи, посочени в член 2, параграф 2 от настоящия регламент.

Изискванията, на които трябва да отговарят тези компетентни органи за изпълнението на своите дейности по сертифициране, надзор и правоприлагане, се съдържат в регламентите, посочени в член 2, параграф 1 от настоящия регламент и в член 2 от Делегиран регламент (ЕС) 2022/1645.

IS.AR.200 Система за управление на информационната сигурност (ISMS)

а) За постигане на целите, посочени в член 1, компетентният орган създава, въвежда и поддържа система за управление на информационната сигурност (ISMS), която гарантира, че компетентният орган:

1. установява политика за информационна сигурност, която определя общите принципи на компетентния орган по отношение на потенциалното въздействие на рисковете за информационната сигурност върху авиационната безопасност;

2. установява и преглежда рисковете за информационната сигурност в съответствие с точка IS.AR.205;

3. определя и прилага мерки за третиране на риска за информационната сигурност в съответствие с точка IS.AR.210;

4. определя и прилага, в съответствие с точка IS.AR.215, необходимите мерки за откриване на събития, свързани с информационната сигурност, идентифицира тези събития, които се считат за инциденти с потенциално въздействие върху авиационната безопасност, реагира на тези инциденти, свързани с информационната сигурност, и се възстановява от тях;

5. спазва изискванията, съдържащи се в точка IS.AR.220, когато възлага на други организации която и да е част от дейностите, описани в точка IS.AR.200;

6. спазва изискванията по отношение на персонала, съдържащи се в точка IS.AR.225;

7. спазва изискванията за водене на документация, съдържащи се в точка IS.AR.230;

8. наблюдава съответствието на собствената си организация с изискванията на настоящия регламент и предоставя обратна информация относно констатациите на лицето, посочено в точка IS.AR.225, буква а), за да се гарантира ефективното изпълнение на коригиращите действия;

9. защитава поверителността на всякаква информация, с която компетентният орган може да разполага във връзка с организациите, подлежащи на неговия надзор, и на информацията, получена чрез схемите за външно докладване на организацията, създадени в съответствие с точка IS.I.OR.230 от приложение II (част IS.I.OR) към настоящия регламент и точка IS.D.OR.230 от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645;

10. уведомява Агенцията за промени, които засягат способността на компетентния орган да изпълнява своите задачи и задължения, както е определено в настоящия регламент;

11. определя и прилага процедури за обмен, по целесъобразност и по практичен и навременен начин, на относима информация с цел подпомагане на други компетентни органи и агенции, както и на организациите, за които се прилага настоящият регламент, да извършват ефективни оценки на риска за сигурността във връзка с техните дейности.

б) За да спазва системно изискванията, посочени в член 1, компетентният орган осъществява процес на постоянно подобряване в съответствие с точка IS.AR.235.

в) Компетентният орган документира всички ключови процеси, процедури, роли и отговорности, необходими за спазване на точка IS.AR.200, буква а), и установява процес за изменение на тази документация.

г) Процесите, процедурите, ролите и отговорностите, установени от компетентния орган с цел спазване на точка IS.AR.200, буква а), съответстват на естеството и сложността на неговите дейности въз основа на оценка на рисковете за информационната сигурност, присъщи на тези дейности, и могат да бъдат интегрирани в други съществуващи системи за управление, които вече са въведени от компетентния орган.

IS.AR.205 Оценка на риска за информационната сигурност

а) Компетентният орган установява всички елементи на собствената си организация, които биха могли да бъдат изложени на рискове за информационната сигурност. Това включва:

1. дейностите, съоръженията и ресурсите на компетентния орган, както и услугите, които компетентният орган експлоатира, предоставя, получава или поддържа;

2. оборудването, системите, данните и информацията, които допринасят за функционирането на елементите, посочени в точка 1.

б) Компетентният орган установява връзките, които собствената му организация има с други организации и които биха могли да доведат до взаимно излагане на рискове за информационната сигурност.

в) По отношение на елементите и връзките, посочени в букви а) и б), компетентният орган установява рисковете за информационната сигурност, които може да имат потенциално въздействие върху авиационната безопасност.

За всеки установен риск компетентният орган:

1. определя нивото на риска съгласно предварително определена класификация, възприета от него;

2. свързва всеки риск и неговото ниво със съответния елемент или връзка, установени в съответствие с букви а) и б).

При предварително определената класификация, посочена в точка 1, се взема предвид потенциалът за възникване на сценария за заплаха и сериозността на последиците от него за безопасността. Посредством тази класификация и като се вземе предвид дали компетентният орган има структуриран и възпроизводим процес на управление на риска за операциите, компетентният орган е в състояние да установи дали рискът е приемлив, или трябва да бъде третиран в съответствие с точка IS.AR.210.

За да се улесни взаимната съпоставимост на оценките на риска, при определянето на нивото на риска съгласно подточка 1 се взема предвид информацията от значение, получена в координация с организациите, посочени в буква б).

г) Компетентният орган преразглежда и актуализира оценката на риска, извършена в съответствие с букви а), б) и в), във всеки от следните случаи:

1. когато има промяна в елементите, които са изложени на рискове за информационната сигурност;

2. когато има промяна във връзките между организацията на компетентния орган и други организации или в рисковете, съобщени от другите организации;

3. когато има промяна в информацията или знанията, използвани за установяване, анализ и класификация на рисковете;

4. когато са извлечени поуки от анализа на инцидентите, свързани с информационната сигурност.

IS.AR.210 Третиране на риска за информационната сигурност

а) Компетентният орган разработва мерки за справяне с неприемливите рискове, установени в съответствие с точка IS.AR.205, прилага ги своевременно и проверява дали те продължават да са ефективни. Тези мерки дават възможност на компетентния орган:

1. да контролира обстоятелствата, които допринасят за действителното възникване на сценария за заплаха;

2. да смекчава последиците за авиационната безопасност, свързани с реализирането на сценария за заплаха;

3. да избягва рисковете.

Тези мерки не трябва да въвеждат нови потенциални неприемливи рискове за авиационната безопасност.

б) Лицето, посочено в точка IS.AR.225, буква а), и другият засегнат персонал на компетентния орган се информират за резултатите от оценката на риска, извършена в съответствие с точка IS.AR.205, съответните сценарии за заплаха и мерките, които трябва да бъдат изпълнени.

Компетентният орган също така информира организациите, с които си взаимодейства в съответствие с точка IS.AR.205, буква б), за всеки риск, който е общ за компетентния орган и организацията.

IS.AR.215 Инциденти, свързани с информационната сигурност — откриване, реагиране и възстановяване

а) Въз основа на резултатите от оценката на риска, извършена в съответствие с точка IS.AR.205, и на резултата от третирането на риска, извършено в съответствие с точка IS.AR.210, компетентният орган прилага мерки за откриване на събития, които показват потенциалното възникване на неприемливи рискове и които може да окажат потенциално въздействие върху авиационната безопасност. Тези мерки за откриване дават възможност на компетентния орган:

1. да установява отклонения от предварително определени базови стойности на функционалните показатели;

2. да задейства предупреждения за начало на подходящи мерки за реагиране в случай на отклонение.

б) Компетентният орган прилага мерки за реагиране на всяко събитие, определено в съответствие с буква а), което би могло да се развие или се е развило в инцидент, свързан с информационната сигурност. Тези мерки за реагиране дават възможност на компетентния орган:

1. да започне да реагира на предупрежденията на собствената си организация, посочени в буква а), подточка 2, като активира предварително определени ресурси и начин на действие;

2. да ограничи разрастването на атаката и да избегне пълното реализиране на сценария за заплаха;

3. да контролира режима на неизправност на засегнатите елементи, определени в точка IS.AR.205, буква а).

в) Компетентният орган прилага мерки, насочени към възстановяване от инциденти, свързани с информационната сигурност, включително спешни мерки, ако е необходимо. Тези мерки за възстановяване дават възможност на компетентния орган:

1. да отстрани състоянието, което е причинило инцидента, или да го ограничи до допустимо ниво;

2. да възстанови безопасното състояние на засегнатите елементи, определени в точка IS.AR.205, буква а), в рамките на период на възстановяване, определен предварително от собствената му организация.

IS.AR.220 Възлагане на дейности по управление на информационната сигурност на подизпълнители

Компетентният орган гарантира, че когато възлага на други организации която и да е част от дейностите, посочени в точка IS.AR.200, дейностите, за които е сключен договор, отговарят на изискванията на настоящия регламент, а организацията подизпълнител работи под негов надзор. Компетентният орган гарантира, че рисковете, свързани с дейностите, възложени на подизпълнители, се управляват по подходящ начин.

IS.AR.225 Изисквания към персонала

Компетентният орган:

а) разполага с лице, което има правомощия да създава и поддържа организационните структури, политики, процеси и процедури, необходими за прилагането на настоящия регламент.

Това лице:

1. има правомощия за пълен достъп до ресурсите, необходими на компетентния орган за изпълнение на всички задачи, изисквани от настоящия регламент;

2. има делегирани правомощия, необходими за изпълнение на възложените му задължения.

б) разполага с процедура, чрез която да се гарантира, че е налице достатъчно персонал за извършване на дейностите, обхванати от настоящото приложение;

в) разполага с процедура, чрез която да се гарантира, че персоналът, посочен в буква б), притежава необходимата компетентност за изпълнение на своите задачи;

г) разполага с процедура, чрез която да се гарантира, че персоналът е запознат с отговорностите, свързани с възложените роли и задачи;

д) гарантира, че самоличността и надеждността на персонала, който има достъп до информационните системи и данните, за които се прилагат изискванията на настоящия регламент, са установени по подходящ начин.

IS.AR.230 Водене на документация

а) Компетентният орган съхранява документация за своите дейности по управление на информационната сигурност.

1. Компетентният орган гарантира, че следните записи са архивирани и проследими:

i) договори за дейностите, посочени в точка IS.AR.200, буква а), подточка 5;

ii) записи на ключовите процеси, посочени в точка IS.AR.200, буква г);

iii) записи на рисковете, установени при оценката на риска, посочена в точка IS.AR.205, заедно със свързаните с тях мерки за третиране на риска, посочени в точка IS.AR.210;

iv) записи на събития, свързани с информационната сигурност, които може да се наложи да бъдат преразгледани, за да се разкрият неоткрити инциденти или уязвимости, свързани с информационната сигурност.

2. Документацията, посочена в подточка 1, i), се съхранява най-малко 5 години след изменението или прекратяването на договора.

3. Записите, посочени в подточка 1, ii) и iii), се съхраняват най-малко за срок от 5 години.

4. Записите, посочени в подточка 1, iv), се съхраняват, докато конкретните събития, свързани с информационната сигурност, бъдат преразгледани в съответствие с периодичността, определена в установена от компетентния орган процедура.

б) Компетентният орган съхранява документация за квалификацията и опита на собствения си персонал, участващ в дейности по управление на информационната сигурност.

1. Данните за квалификацията и опита на персонала се съхраняват, докато лицето работи за компетентния орган, и в продължение на най-малко 3 години след напускането му.

2. По тяхно искане членовете на персонала получават достъп до личните си досиета. Освен това — при поискване от тяхна страна — компетентният орган им предоставя копие от личните им досиета при напускане на компетентния орган.

в) Форматът на документацията се уточнява в процедурите на компетентния орган.

г) Записите се съхраняват по начин, който гарантира защита от повреда, промяна и кражба, като информацията се идентифицира, когато е необходимо, в съответствие с нейното ниво на класификация за сигурност. Компетентният орган гарантира, че записите се съхраняват, като се използват средства за гарантиране на целостта, автентичността и разрешения достъп.

IS.AR.235 Постоянно подобряване

а) Компетентният орган оценява, като използва подходящи показатели за изпълнението, ефективността и зрелостта на собствената си ISMS. Оценката се извършва въз основа на график, предварително определен от компетентния орган, или след инцидент, свързан с информационната сигурност.

б) Ако в резултат на оценката, извършена в съответствие с буква а), бъдат открити недостатъци, компетентният орган предприема необходимите мерки за подобряване, за да гарантира, че ISMS продължава да отговаря на приложимите изисквания, и поддържа рисковете за информационната сигурност на приемливо равнище. Освен това компетентният орган извършва повторна оценка на елементите на ISMS, засегнати от приетите мерки.

ПРИЛОЖЕНИЕ II

ИНФОРМАЦИОННА СИГУРНОСТ — ИЗИСКВАНИЯ КЪМ ОРГАНИЗАЦИЯТА

[ЧАСТ IS.I.OR]

IS.I.OR.100 Обхват

IS.I.OR.200 Система за управление на информационната сигурност (ISMS)

IS.I.OR.205 Оценка на риска за информационната сигурност

IS.I.OR.210 Третиране на риска за информационната сигурност

IS.I.OR.215 Схема за вътрешно докладване във връзка с информационната сигурност

IS.I.OR.220 Инциденти, свързани с информационната сигурност — откриване, реагиране и възстановяване

IS.I.OR.225 Реагиране на констатациите, съобщени от компетентния орган

IS.I.OR.230 Схема за външно докладване във връзка с информационната сигурност

IS.I.OR.235 Възлагане на дейности по управление на информационната сигурност на подизпълнители

IS.I.OR.240 Изисквания към персонала

IS.I.OR.245 Водене на документация

IS.I.OR.250 Ръководство за управление на информационната сигурност (ISMM)

IS.I.OR.255 Промени в системата за управление на информационната сигурност

IS.I.OR.260 Постоянно подобряване

IS.I.OR.100 Обхват

В настоящата част се определят изискванията, на които трябва да отговарят организациите, посочени в член 2, параграф 1 от настоящия регламент.

IS.I.OR.200 Система за управление на информационната сигурност (ISMS)

а) За постигане на целите, посочени в член 1, организацията създава, въвежда и поддържа система за управление на информационната сигурност (ISMS), която гарантира, че организацията:

1. установява политика за информационна сигурност, която определя общите принципи на организацията по отношение на потенциалното въздействие на рисковете за информационната сигурност върху авиационната безопасност;
2. установява и преглежда рисковете за информационната сигурност в съответствие с точка IS.I.OR.205;
3. определя и прилага мерки за третиране на риска за информационната сигурност в съответствие с точка IS.I.OR.210;
4. прилага схема за вътрешно докладване във връзка с информационната сигурност в съответствие с точка IS.I.OR.215;
5. определя и прилага — в съответствие с точка IS.I.OR.220 — необходимите мерки за откриване на събития, свързани с информационната сигурност, установява тези събития, които се считат за инциденти с потенциално въздействие върху авиационната безопасност, с изключение на разрешеното по точка IS.I.OR.205, буква д), реагира на тези инциденти, свързани с информационната сигурност, и се възстановява от тях;

6. изпълнява мерките, за които компетентният орган е уведомил, като незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност;

7. предприема подходящи действия в съответствие с точка IS.I.OR.225 за отстраняване на констатациите, за които компетентният орган я е информирал;

8. прилага схема за външно докладване в съответствие с точка IS.I.OR.230, за да се даде възможност на компетентния орган да предприеме подходящи действия;

9. отговаря на изискванията, съдържащи се в точка IS.I.OR.235, когато възлага на други организации която и да е част от дейностите, посочени в точка IS.I.OR.200;

10. отговаря на изискванията по отношение на персонала, определени в точка IS.I.OR.240;

11. отговаря на изискванията за водене на документация, определени в точка IS.I.OR.245;

12. наблюдава съответствието на организацията с изискванията на настоящия регламент и предоставя обратна информация относно констатациите на отговорния ръководител, за да се гарантира ефективното изпълнение на коригиращите действия;

13. без да се засягат приложимите изисквания за докладване на инциденти, защитава поверителността на всяка информация, която организацията може да е получила от други организации, в съответствие с нейната степен на поверителност.

б) За да спазва системно изискванията, посочени в член 1, организацията осъществява процес на постоянно подобряване в съответствие с точка IS.I.OR.260.

в) Организацията документира в съответствие с точка IS.I.OR.250 всички ключови процеси, процедури, роли и отговорности, необходими за спазване на точка IS.I.OR.200, буква а), и установява процес за изменение на тази документация. Промените в тези процеси, процедури, роли и отговорности се управляват в съответствие с точка IS.I.OR.255.

г) Процесите, процедурите, ролите и отговорностите, установени от организацията с цел спазване на точка IS.I.OR.200, буква а), съответстват на естеството и сложността на нейните дейности въз основа на оценка на рисковете за информационната сигурност, присъщи на тези дейности, и могат да бъдат интегрирани в други съществуващи системи за управление, които вече са въведени от организацията.

д) Без да се засяга задължението за спазване на изискванията за докладване, определени в Регламент (ЕС) № 376/2014, и изискванията, определени в точка IS.I.OR.200, буква а), подточка 13, организацията може да бъде одобрена от компетентния орган да не прилага изискванията, посочени в букви а)—г), и свързаните с тях изисквания, съдържащи се в точки IS.I.OR.205—IS.I.OR.260, ако тя докаже по удовлетворителен за този орган начин, че нейните дейности, съоръжения и ресурси, както и услугите, които експлоатира, предоставя, получава и поддържа, не пораждат рискове за информационната сигурност с потенциално въздействие върху авиационната безопасност нито на самата нея, нито на други организации. Одобрението се основава на документирана оценка на риска за информационната сигурност, извършена от организацията или от трета страна в съответствие с точка IS.I.OR.205 и разгледана и одобрена от нейния компетентен орган.

Поддържането на валидността на това одобрение се преразглежда от компетентния орган след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.

IS.I.OR.205 Оценка на риска за информационната сигурност

а) Организацията установява всички свои елементи, които биха могли да бъдат изложени на рискове за информационната сигурност. Това включва:

1. дейностите, съоръженията и ресурсите на организацията, както и услугите, които организацията експлоатира, предоставя, получава или поддържа;

2. оборудването, системите, данните и информацията, които допринасят за функционирането на елементите, изброени в подточка 1.

б) Организацията установява връзките, които има с други организации и които биха могли да доведат до взаимно излагане на рискове за информационната сигурност.

в) По отношение на елементите и връзките, посочени в букви а) и б), организацията установява рисковете за информационната сигурност, които може да имат потенциално въздействие върху авиационната безопасност. За всеки установен риск организацията:

1. определя нивото на риска съгласно предварително определена класификация, възприета от организацията;

2. свързва всеки риск и неговото ниво със съответния елемент или връзка, установени в съответствие с букви а) и б).

При предварително определената класификация, посочена в подточка 1, се взема предвид потенциалът за възникване на сценария за заплаха и сериозността на последиците от него за безопасността. Въз основа на тази класификация и като се вземе предвид дали организацията има структуриран и възпроизводим процес на управление на риска за операциите, организацията трябва да е в състояние да установи дали рискът е приемлив, или трябва да бъде третиран в съответствие с точка IS.I.OR.210.

За да се улесни взаимната съпоставимост на оценките на риска, при определянето на нивото на риска съгласно подточка 1 се взема предвид съответната информация, получена в координация с организациите, посочени в буква б).

г) Организацията преразглежда и актуализира оценката на риска, извършена в съответствие с букви а), б) и, според случая, с букви в) или д), във всяка от следните ситуации:

1. когато има промяна в елементите, които са изложени на рискове за информационната сигурност;

2. когато има промяна във връзките между организацията и други организации или в рисковете, съобщени от другите организации;

3. когато има промяна в информацията или знанията, използвани за установяване, анализ и класификация на рисковете;

4. когато са извлечени поуки от анализа на инцидентите, свързани с информационната сигурност.

д) Чрез дерогация от буква в) организациите, от които се изисква да спазват подчаст B от приложение III (част ATM/ANS.OR) към Регламент за изпълнение (ЕС) 2017/373, заменят анализа на въздействието върху авиационната безопасност с анализ на въздействието върху техните услуги съгласно оценката на поддържането на безопасността, изисквана по точка ATM/ANS.OR.C.005. Тази оценка на поддържането на безопасността се предоставя на доставчиците на обслужване на въздушното движение, на които те предоставят услуги, а тези доставчици на обслужване на въздушното движение отговарят за оценката на въздействието върху авиационната безопасност.

IS.I.OR.210 Третиране на риска за информационната сигурност

а) Организацията разработва мерки за справяне с неприемливите рискове, установени в съответствие с точка IS.I.OR.205, прилага ги своевременно и проверява дали те продължават да са ефективни. Тези мерки дават възможност на организацията:

1. да контролира обстоятелствата, които допринасят за действителното възникване на сценария за заплаха;

2. да смекчава последиците за авиационната безопасност, свързани с реализирането на сценария за заплаха;

3. да избягва рисковете.

Тези мерки не трябва да въвеждат нови потенциални неприемливи рискове за авиационната безопасност.

б) Лицето, посочено в точка IS.I.OR.240, букви а) и б), и останалият засегнат персонал на организацията се информират за резултатите от оценката на риска, извършена в съответствие с точка IS.I.OR.205, съответните сценарии за заплаха и мерките, които трябва да бъдат предприети.

Организацията също така информира организациите, с които си взаимодейства в съответствие с точка IS.I.OR.205, буква б), за всеки риск, който е общ и за двете организации.

IS.I.OR.215 Схема за вътрешно докладване във връзка с информационната сигурност

а) Организацията създава схема за вътрешно докладване, за да се даде възможност за събиране и оценка на събития, свързани с информационната сигурност, включително такива, които трябва да бъдат докладвани съгласно точка IS.I.OR.230.

б) Тази схема и процесът, посочени в точка IS.I.OR.220, дават възможност на организацията:

1. да определя кои от събитията, докладвани съгласно буква а), се считат за инциденти или уязвимости, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност;

2. да разпознава причините за установените в съответствие с подточка 1 инциденти и уязвимости, свързани с информационната сигурност, както и факторите, допринасящи за тях, и — като част от процеса на управление на риска за информационната сигурност в съответствие с точки IS.I.OR.205 и IS.I.OR.220 — да ги отстранява;

3. да осигурява оценка на цялата известна информация от значение за инцидентите и уязвимостите, свързани с информационната сигурност, установени в съответствие с подточка 1;

4. да гарантира прилагането на метод за вътрешно разпространение на информацията, ако е необходимо.

в) От всяка организация подизпълнител, която може да изложи организацията на рискове за информационната сигурност с потенциално въздействие върху авиационната безопасност, се изисква да ѝ докладва за събития, свързани с информационната сигурност. Тези доклади се представят, като се прилагат процедурите, установени в конкретните договорни споразумения, и се оценяват в съответствие с буква б).

г) При разследвания организацията си сътрудничи с всяка друга организация, която има значителен принос за информационната сигурност на собствените ѝ дейности.

д) Организацията може да обедини тази схема за докладване с други схеми за докладване, които вече прилага.

IS.I.OR.220 Инциденти, свързани с информационната сигурност — откриване, реагиране и възстановяване

а) Въз основа на резултатите от оценката на риска, извършена в съответствие с точка IS.I.OR.205, и на резултата от третирането на риска, извършено в съответствие с точка IS.I.OR.210, организацията прилага мерки за откриване на инциденти и уязвимости, които показват потенциалното възникване на неприемливи рискове и които може да окажат потенциално въздействие върху авиационната безопасност. Тези мерки за откриване дават възможност на организацията:

1. да установява отклонения от предварително определени базови стойности на функционалните показатели;

2. да задейства предупреждения за начало на подходящи мерки за реагиране в случай на отклонение.

б) Организацията прилага мерки за реагиране на всяко събитие, определено в съответствие с буква а), което би могло да се развие или се е развило в инцидент, свързан с информационната сигурност. Тези мерки за реагиране дават възможност на организацията:

1. да започне да реагира на предупрежденията, посочени в буква а), подточка 2, като активира предварително определени ресурси и начин на действие;

2. да ограничи разрастването на атаката и да избегне пълното реализиране на сценария за заплаха;

3. да контролира режима на неизправност на засегнатите елементи, определени в точка IS.I.OR.205, буква а).

в) Организацията прилага мерки, насочени към възстановяване от инциденти, свързани с информационната сигурност, включително спешни мерки, ако е необходимо. Тези мерки за възстановяване дават възможност на организацията:

1. да отстрани състоянието, което е причинило инцидента, или да го ограничи до допустимо ниво;

2. да достигне безопасно състояние на засегнатите елементи, определени в точка IS.I.OR.205, буква а), в рамките на период на възстановяване, определен предварително от организацията.

IS.I.OR.225 Реагиране на констатациите, съобщени от компетентния орган

а) След получаване на уведомлението за констатации, представено от компетентния орган, организацията:

1. установява причината или причините и факторите, които са допринесли за възникване на несъответствието;

2. изготвя план с коригиращи действия;

3. доказва отстраняването на несъответствието по удовлетворителен за компетентния орган начин.

б) Действията, посочени в буква а), се извършват в срока, договорен с компетентния орган.

IS.I.OR.230 Схема за външно докладване във връзка с информационната сигурност

а) Организацията въвежда система за докладване във връзка с информационната сигурност, която отговаря на изискванията, определени в Регламент (ЕС) № 376/2014 и свързаните с него делегирани актове и актове за изпълнение, ако посоченият регламент е приложим за организацията.

б) Без да се засягат задълженията по Регламент (ЕС) № 376/2014, организацията гарантира, че всеки инцидент или уязвимост, свързани с информационната сигурност, които може да представляват значителен риск за авиационната безопасност, се докладват на нейния компетентен орган. Освен това:

1. когато такъв инцидент или уязвимост засяга въздухоплавателно средство или свързана система или компонент, организацията докладва за това и на притежателя на одобрението на проекта;

2. когато такъв инцидент или уязвимост засяга система или съставен елемент, използвани от организацията, тя докладва за това на организацията, отговорна за проектирането на системата или съставния елемент.

в) Организацията докладва условията, посочени в буква б), както следва:

1. на компетентния орган и, ако е приложимо, на притежателя на одобрението на проекта или на организацията, отговорна за проектирането на системата или съставния елемент, се изпраща уведомление веднага щом състоянието стане известно на организацията;

2. на компетентния орган и, ако е приложимо, на притежателя на одобрението на проекта или на организацията, отговорна за проектирането на системата или съставния елемент, се представя доклад във възможно най-кратък срок, но не повече от 72 часа от момента, в който състоянието е станало известно на организацията, освен ако изключителни обстоятелства не попречат на това.

   Докладът се изготвя във формата, определена от компетентния орган, и съдържа цялата информация от значение за състоянието, известна на организацията;

3. на компетентния орган и, ако е приложимо, на притежателя на одобрението на проекта или на организацията, отговорна за проектирането на системата или съставния елемент, се представя доклад за последващите действия, в който се предоставят подробности за действията, които организацията е предприела или възнамерява да предприеме, за да се възстанови от инцидента, и действията, които възнамерява да предприеме, за да предотврати подобни инциденти, свързани с информационната сигурност в бъдеще.

   Докладът за последващите действия се представя веднага след определянето на тези действия и се изготвя във формата, определена от компетентния орган.

IS.I.OR.235 Възлагане на дейности по управление на информационната сигурност на подизпълнители

а) Организацията гарантира, че когато възлага на други организации която и да е част от дейностите, посочени в точка IS.I.OR.200, дейностите, за които е сключен договор, отговарят на изискванията на настоящия регламент, а организацията подизпълнител работи под неин надзор. Организацията гарантира, че рисковете, свързани с дейностите, възложени на подизпълнители, се управляват по подходящ начин.

б) Организацията гарантира, че компетентният орган може да получи достъп при поискване до организацията подизпълнител, за да установи дали се запазва съответствието с приложимите изисквания, определени в настоящия регламент.

IS.I.OR.240 Изисквания към персонала

а) Отговорният ръководител на организацията, определен в съответствие с регламенти (ЕС) № 1321/2014, (ЕС) № 965/2012, (ЕС) № 1178/2011, (ЕС) 2015/340, (ЕС) 2017/373 или Регламент за изпълнение (ЕС) 2021/664, според случая, посочен в член 2, параграф 1 от настоящия регламент, има административни правомощия да гарантира, че всички дейности, изисквани по настоящия регламент, могат да бъдат финансирани и извършени. Това лице:

1. гарантира, че са налице всички необходими ресурси за спазване на изискванията на настоящия регламент;

2. създава и популяризира политиката за информационна сигурност, посочена в точка IS.I.OR.200, буква а), подточка 1;

3. показва основно разбиране на разпоредбите на настоящия регламент.

б) Отговорният ръководител назначава лице или група лица, които да гарантират, че организацията отговаря на изискванията на настоящия регламент, и определя обхвата на техните правомощия. Това лице или група лица докладват пряко на отговорния ръководител и притежават необходимите знания, образование и опит, за да изпълняват своите задължения. В процедурите се определя кой замества дадено лице в случай на продължителното му отсъствие.

в) Отговорният ръководител назначава лице или група лица, които отговарят за управлението на функцията по наблюдение на съответствието, посочена в точка IS.I.OR.200, буква а), подточка 12.

г) Когато организацията споделя организационни структури, политики, процеси и процедури за информационна сигурност с други организации или с области от тяхната собствена организация, които не са част от одобрението или декларацията, отговорният ръководител може да делегира своите дейности на едно общо отговорно лице.

В този случай се установяват мерки за координация между отговорния ръководител на организацията и общото отговорно лице, за да се осигури адекватно интегриране на управлението на информационната сигурност в рамките на организацията.

д) Отговорният ръководител или общото отговорно лице, посочено в буква г), имат административни правомощия да създават и поддържат организационните структури, политики, процеси и процедури, необходими за прилагането на точка IS.I.OR.200.

е) Организацията трябва да въведе процедура, която да гарантира, че тя има достатъчно персонал, който да е на разположение за извършване на дейностите, обхванати от настоящото приложение.

ж) Организацията трябва да въведе процедура, която да гарантира, че персоналът, посочен в буква е), притежава необходимата компетентност за изпълнение на своите задачи.

з) Организацията трябва да въведе процедура, която да гарантира, че персоналът е запознат с отговорностите, свързани с възложените роли и задачи.

и) Организацията гарантира, че самоличността и надеждността на персонала, който има достъп до информационните системи и данните, за които се прилагат изискванията на настоящия регламент, са установени по подходящ начин.

IS.I.OR.245 Водене на документация

а) *Организацията съхранява документация за своите дейности по управление на информационната сигурност.*

1. Организацията гарантира, че следните записи са архивирани и проследими:

i) всяко получено одобрение и всяка свързана с него оценка на риска за информационната сигурност в съответствие с точка IS.I.OR.200, буква д);

ii) договори за дейностите, посочени в точка IS.I.OR.200, буква а), подточка 9;

iii) записи на ключовите процеси, посочени в точка IS.I.OR.200, буква г);

iv) записи на рисковете, установени при оценката на риска, посочена в точка IS.I.OR.205, заедно със свързаните с тях мерки за третиране на риска, посочени в точка IS.I.OR.210;

v) записи на инциденти и уязвимости, свързани с информационната сигурност, докладвани в съответствие със схемите за докладване, посочени в точки IS.I.OR.215 и IS.I.OR.230;

vi) записи на такива събития, свързани с информационната сигурност, които може да се наложи да бъдат преразгледани, за да се разкрият неоткрити инциденти или уязвимости, свързани с информационната сигурност.

2. Записите, посочени в подточка 1, i), се съхраняват най-малко 5 години след изтичане на валидността на одобрението.

3. Документацията, посочена в подточка 1, ii), се съхранява най-малко 5 години след изменението или прекратяването на договора.

4. Записите, посочени в подточка 1, iii), iv) и v), се съхраняват най-малко за срок от 5 години.

5. Записите, посочени в подточка 1, vi), се съхраняват, докато конкретните събития, свързани с информационната сигурност, бъдат преразгледани в съответствие с периодичността, определена в установена от организацията процедура.

б) *Организацията съхранява документация за квалификацията и опита на собствения си персонал, участващ в дейности по управление на информационната сигурност.*

1. Данните за квалификацията и опита на персонала се съхраняват, докато лицето работи за организацията, и в продължение на най-малко 3 години след напускането му.

2. По тяхно искане членовете на персонала получават достъп до личните си досиета. Освен това — при поискване от тяхна страна — организацията им предоставя копие от личните им досиета при напускане на организацията.

в) Форматът на документацията се уточнява в процедурите на организацията.

г) Записите се съхраняват по начин, който гарантира защита от повреда, изменение и кражба, като информацията се идентифицира, когато е необходимо, в съответствие с нейното ниво на класификация за сигурност. Организацията гарантира, че записите се съхраняват, като се използват средства за гарантиране на целостта, автентичността и разрешения достъп.

IS.I.OR.250 Ръководство за управление на информационната сигурност (ISMM)

а) Организацията предоставя на компетентния орган ръководство за управление на информационната сигурност (ISMM) и, когато е приложимо, всички съответни ръководства и процедури, съдържащи:

1. декларация, подписана от отговорния ръководител, в която се потвърждава, че организацията ще работи винаги в съответствие с настоящото приложение и с ISMM. Ако отговорният ръководител не е главният изпълнителен директор на организацията, този главен изпълнителен директор подписва декларацията;

2. длъжността, имената, задълженията, отчетността, отговорностите и правомощията на лицето или лицата, определено/и в точка IS.I.OR.240, букви б) и в);

3. длъжността, имената, задълженията, отчетността, отговорностите и правомощията на общото отговорно лице, определено в точка IS.I.OR.240, буква г), ако е приложимо;

4. политиката за информационна сигурност на организацията, както е посочено в точка IS.I.OR.200, буква а), подточка 1;

5. общо описание на броя и категориите персонал и на въведената система за планиране на наличния персонал съгласно изискванията на точка IS.I.OR.240;

6. длъжността, имената, задълженията, отчетността, отговорностите и правомощията на ключовите лица, отговарящи за изпълнението на точка IS.I.OR.200, включително лицето или лицата, отговарящи за функцията по наблюдение на съответствието, посочена в точка IS.I.OR.200, буква а), подточка 12;

7. органиграма, показваща свързаните вериги на отчетност и отговорност за лицата, посочени в подточки 2 и 6;

8. описание на схемата за вътрешно докладване, посочена в точка IS.I.OR.215;

9. процедурите, определящи начина, по който организацията гарантира спазването на настоящата част, и по-специално:

i) документацията, посочена в точка IS.I.OR.200, буква в);

ii) процедурите, определящи начина, по който организацията контролира всички възложени на подизпълнители дейности, както е посочено в точка IS.I.OR.200, буква а), подточка 9;

iii) процедурата за изменение на ISMM, посочена в буква в);

10. данни за одобрените понастоящем алтернативни начини за постигане на съответствие.

б) Първоначалното издание на ISMM се одобрява и компетентният орган запазва копие от него. ISMM се изменя при необходимост, за да бъде актуално описанието на ISMS на организацията. Копие от всички изменения на ISMM се предоставя на компетентния орган.

в) Измененията на ISMM се управляват съгласно процедура, установена от организацията. Всички изменения, които не са включени в обхвата на посочената процедура, и всички изменения, свързани с промените, посочени в точка IS.I.OR.255, буква б), се одобряват от компетентния орган.

г) Организацията може да интегрира ISMM с други описания на управлението или ръководства, които поддържа, при условие че има ясна препратка, която показва кои части от описанието на управлението или наръчника отговарят на различните изисквания, съдържащи се в настоящото приложение.

IS.I.OR.255 Промени в системата за управление на информационната сигурност

а) Промените в ISMS могат да се управляват и съобщават на компетентния орган по процедура, разработена от организацията. Тази процедура се одобрява от компетентния орган.

б) По отношение на промените в ISMS, които не са обхванати от процедурата, посочена в буква а), организацията подава заявление и получава одобрение, издадено от компетентния орган.

По отношение на тези промени:

1. заявлението се подава преди извършването на такава промяна, за да се даде възможност на компетентния орган да установи дали се запазва съответствието с настоящия регламент и да измени, ако е необходимо, сертификата на организацията и съответните приложени към него условия на одобрението;

2. организацията предоставя на компетентния орган всяка поискана от него информация за оценка на промяната;

3. промяната се прилага само след получаване на официално одобрение от компетентния орган;

4. организацията работи при условията, предписани от компетентния орган при прилагането на такива промени.

IS.I.OR.260 Постоянно подобряване

а) Организацията оценява ефективността и зрелостта на ISMS, като използва подходящи показатели за изпълнение. Тази оценка се извършва въз основа на график, предварително определен от организацията, или след инцидент, свързан с информационната сигурност.

б) Ако в резултат на оценката, извършена в съответствие с буква а), бъдат открити недостатъци, организацията предприема необходимите мерки за подобряване, за да гарантира, че ISMS продължава да отговаря на приложимите изисквания, и поддържа рисковете за информационната сигурност на приемливо равнище. Освен това организацията извършва повторна оценка на елементите на ISMS, засегнати от приетите мерки.

ПРИЛОЖЕНИЕ III

Приложения VI (част ARA) и VII (част ORA) към Регламент (ЕС) № 1178/2011 се изменят, както следва:

(1) приложение VI (част ARA) се изменя, както следва:

а) в точка ARA.GEN.125 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

б) след точка ARA.GEN.135 се вмъква следната точка ARA.GEN.135A:

„**ARA.GEN.135A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка ARA.GEN.125, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

в) в точка ARA.GEN.200 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

г) точка ARA.GEN.205 се изменя, както следва:

i) заглавието се заменя със следното:

„**ARA.GEN.205 Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка ORA.GEN.200A компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка ARA.GEN.200, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

д) в точка ARA.GEN.300 се добавя следната буква ж):

„ж) По отношение на сертифицирането и надзора над съответствието на организацията с точка ORA.GEN.200A, в допълнение към спазването на букви а)—е), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

е) след точка ARA.GEN.330 се вмъква следната точка ARA.GEN.330A:

„**ARA.GEN.330A Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка ARA.GEN.300. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка ARA.GEN.350.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“;

(2) приложение VII (част ORA) се изменя, както следва:

след точка ORA.GEN.200 се вмъква следната точка ORA.GEN.200A:

„**ORA.GEN.200A Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка ORA.GEN.200, организацията създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“

ПРИЛОЖЕНИЕ IV

Приложение I (част 21) към Регламент (ЕС) № 748/2012 се изменя, както следва:

(1) съдържанието се изменя, както следва:

а) след заглавие 21.Б.20 се вмъква следното заглавие:

„21.Б.20A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност“;

б) заглавието на точка 21.Б.30 се заменя със следното:

„21.Б.30 Разпределение на задачите“;

в) след заглавие 21.Б.240 се вмъква следното заглавие:

„21.Б.240A Промени в системата за управление на информационната сигурност“;

г) след заглавие 21.Б.435 се вмъква следното заглавие:

„21.Б.435A Промени в системата за управление на информационната сигурност“;

(2) в точка 21.Б.15 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.D.OR.230 от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645.“;

(3) след точка 21.Б.20 се вмъква следната точка 21.Б.20A:

„**21.Б.20A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка 21.Б.15, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема адекватни мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

(4) в точка 21.Б.25 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

(5) точка 21.Б.30 се изменя, както следва:

а) заглавието се заменя със следното:

„21.Б.30 Разпределение на задачите“;

б) добавя се следната буква в):

„в) За сертифицирането и надзора над съответствието на организацията с точки 21.А.139А и 21.А.239А компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка 21.Б.25, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

(6) в точка 21.Б.221 се добавя следната буква ж):

„ж) По отношение на сертифицирането и надзора над съответствието на организацията с точка 21.А.139А, в допълнение към спазването на букви а)—е), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

(7) след точка 21.Б.240 се вмъква следната точка 21.Б.240А:

„**21.Б.240А Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.D.OR.255, буква а) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка 21.Б.221. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка 21.Б.225.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.D.OR.255, буква б) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“;

(8) в точка 21.Б.431, се добавя следната буква г):

„г) По отношение на сертифицирането и надзора над съответствието на организацията с точка 21.А.239А, в допълнение към съответствието с букви а)—в), компетентният орган трябва да спазва следните принципи:

1. компетентният орган осъществява преглед на връзките и свързаните с тях рискове, определени в съответствие с точка IS.D.OR.205, буква б) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645 от всяка организация, която подлежи на неговия надзор;

2. ако се открият несъответствия във връзките и свързаните с тях рискове, установени от различни организации, компетентният орган ги разглежда заедно със засегнатите организации и, ако е необходимо, прави съответните констатации, за да осигури изпълнението на коригиращи действия;

3. когато документацията, прегледана съгласно подточка 2, разкрива наличието на значителни рискове, свързани с връзки с организации, подлежащи на надзор от друг компетентен орган в рамките на една и съща държава членка, тази информация се съобщава на съответния компетентен орган.“;

(9) след точка 21.Б.435 се вмъква следната точка 21.Б.435А:

„**21.Б.435А Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.D.OR.255, буква а) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка 21.Б.431. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка 21.Б.433.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.D.OR.255, буква б) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“

ПРИЛОЖЕНИЕ V

Приложения II (част ARO) и III (част ORO) към Регламент (ЕС) № 965/2012 се изменят, както следва:

(1) приложение II (част ARO) се изменя, както следва:

а) в точка ARO.GEN.125 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

б) след точка ARO.GEN.135 се вмъква следната точка ARO.GEN.135A:

„**ARO.GEN.135A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка ARO.GEN.125, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

в) в точка ARO.GEN.200 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

г) точка ARO.GEN.205 се изменя, както следва:

i) заглавието се заменя със следното:

„**ARO.GEN.205 Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка ORO.GEN.200A компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка ARO.GEN.200, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

д) в точка ARO.GEN.300 се добавя следната буква ж):

„ж) По отношение на сертифицирането и надзора над съответствието на организацията с точка ORO.GEN.200A, в допълнение към спазването на букви а)—е), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

е) след точка ARO.GEN.330 се вмъква следната точка ARO.GEN.330A:

„**ARO.GEN.330A Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка ARO.GEN.300. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка ARO.GEN.350.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“;

(2) приложение III (част ORO) се изменя, както следва:

след точка ORO.GEN.200 се вмъква следната точка ORO.GEN.200A:

„**ORO.GEN.200A Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка ORO.GEN.200, операторът създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“

ПРИЛОЖЕНИЕ VI

Приложение II (част ADR.AR) към Регламент (ЕС) № 139/2014 се изменя, както следва:

(1) в точка ADR.AR.A.025 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.D.OR.230 от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645.“;

(2) след точка ADR.AR.A.030 се вмъква следната точка ADR.AR.A.030A:

„**ADR.AR.A.030A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка ADR.AR.A.025, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

(3) в точка ADR.AR.B.005 се добавя следната буква г):

„г) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

(4) точка ADR.AR.B.010 се изменя, както следва:

i) заглавието се заменя със следното:

„**ADR.AR.B.010 Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка ADR.OR.D.005A компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка ADR.AR.B.005, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

(5) в точка ADR.AR.C.005 се добавя следната буква е):

„е) По отношение на сертифицирането и надзора над съответствието на организацията с точка ADR.OR.D.005A, в допълнение към спазването на букви а)—д), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

(6) след точка ADR.AR.C.040 се вмъква следната точка ADR.AR.C.040A:

„**ADR.AR.C.040A Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.D.OR.255, буква а) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645, компетентният орган включва прегледа на тези промени в своя продължаващ надзор, в съответствие с принципите, изложени в точка ADR.AR.C.005. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка ADR.AR.C.055.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.D.OR.255, буква б) от приложението (част IS.D.OR) към Делегиран регламент (ЕС) 2022/1645:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“

ПРИЛОЖЕНИЕ VII

Приложения II (част 145), III (част 66) и Vв (част CAMO) към Регламент (ЕС) № 1321/2014 се изменят, както следва:

1. приложение II (част 145) се изменя, както следва:

а) съдържанието се изменя, както следва:

i) след заглавие 145.А.200 се вмъква следното заглавие:

„145.А.200А Система за управление на информационната сигурност“;

ii) след заглавие 145.Б.135 се вмъква следното заглавие:

„145.Б.135А Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност“;

iii) заглавието на точка 145.Б.205 се заменя със следното:

„145.Б.205 Разпределение на задачите“;

iv) след заглавие 145.Б.330 се вмъква следното заглавие:

„145.Б.330А Промени в системата за управление на информационната сигурност“;

б) след точка 145.А.200 се вмъква следната точка 145.А.200А:

„145.А.200А **Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка 145.А.200, организацията за техническо обслужване създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

в) в точка 145.Б.125 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

г) след точка 145.Б.135 се вмъква следната точка 145.Б.135А:

„145.Б.135А **Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка 145.Б.125, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема адекватни мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

д) в точка 145.Б.200 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

е) точка 145.Б.205 се изменя, както следва:

i) заглавието се заменя със следното:

„145.Б.205 **Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка 145.А.200А компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка 145.Б.200, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

ж) в точка 145.Б.300 се добавя следната буква ж):

„ж) По отношение на сертифицирането и надзора над съответствието на организацията с точка 145.А.200А, в допълнение към спазването на букви а)—е), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

з) след точка 145.Б.330 се вмъква следната точка 145.Б.330А:

„145.Б.330А **Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка 145.Б.300. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка 145.Б.350.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“

(2) приложение III (част 66) се изменя, както следва:

а) в съдържанието след заглавие 66.Б.10 се добавя следното заглавие:

„66.Б.15 Система за управление на информационната сигурност“;

б) след точка 66.Б.10 се вмъква следната точка 66.Б.15:

„66.Б.15 **Система за управление на информационната сигурност**

Компетентният орган създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

(3) приложение Vв (част CAMO) се изменя, както следва:

а) съдържанието се изменя, както следва:

i) след заглавие CAMO.A.200 се вмъква следното заглавие:

„CAMO.A.200A Система за управление на информационната сигурност“;

ii) след заглавие CAMO.Б.135 се вмъква следното заглавие:

„CAMO.Б.135A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност“;

iii) заглавието на точка CAMO.Б.205 се заменя със следното:

„CAMO.Б.205 Разпределение на задачите“;

iv) след заглавие CAMO.Б.330 се вмъква следното заглавие:

„CAMO.Б.330A Промени в системата за управление на информационната сигурност“;

б) след точка CAMO.A.200 се вмъква следната точка CAMO.A.200A:

„CAMO.A.200A **Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка CAMO.A.200, организацията създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

в) в точка САМО.Б.125 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

г) след точка САМО.Б.135 се вмъква следната точка САМО.Б.135А:

„САМО.Б.135А **Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка САМО.Б.125, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

д) в точка САМО.Б.200 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

е) точка САМО.Б.205 се изменя, както следва:

i) заглавието се заменя със следното:

„САМО.Б.205 **Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка САМО.А.200А компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка CAMO.Б.200, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

ж) в точка CAMO.Б.300 се добавя следната буква ж):

„ж) По отношение на сертифицирането и надзора над съответствието на организацията с точка CAMO.A.200A, в допълнение към спазването на букви а)—е), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

з) след точка CAMO.Б.330 се вмъква следната точка CAMO.Б.330A:

„CAMO.Б.330A **Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка CAMO.Б.300. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка CAMO.Б.350.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“

ПРИЛОЖЕНИЕ VIII

Приложения II (част ATCO.AR) и III (част ATCO.OR) към Регламент (ЕС) 2015/340 се изменят, както следва:

(1) приложение II (част ATCO.AR) се изменя, както следва:

а) в точка ATCO.AR.A.020 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

б) след точка ATCO.AR.A.025 се вмъква следната точка ATCO.AR.A.025A:

„**ATCO.AR.A.025A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка ATCO.AR.A.020, и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

в) в точка ATCO.AR.Б.001 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

г) точка ATCO.AR.Б.005 се изменя, както следва:

i) заглавието се заменя със следното:

„**ATCO.AR.Б.005 Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка ATCO.OR.B.001A компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка ATCO.AR.Б.001, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

д) в точка ATCO.AR.B.001 се добавя следната буква е):

„е) По отношение на сертифицирането и надзора над съответствието на организацията с точка ATCO.OR.B.001A, в допълнение към спазването на букви а)—д), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

е) след точка ATCO.AR.Д.010 се вмъква следната точка ATCO.AR.Д.010A:

„**ATCO.AR.Д.010A Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка ATCO.AR.B.001. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка ATCO.AR.B.010.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“;

(2) приложение III (част ATCO.OR) се изменя, както следва:

след точка ATCO.OR.B.001 се вмъква следната точка ATCO.OR.B.001A:

„**ATCO.OR.B.001A Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка ATCO.OR.B.001, организацията за обучение създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“

ПРИЛОЖЕНИЕ IX

Приложения II (част ATM/ANS.AR) и III (част ATM/ANS.OR) към Регламент (ЕС) 2017/373 се изменят, както следва:

(1) приложение II (част ATM/ANS.AR) се изменя, както следва:

а) в точка ATM/ANS.AR.A.020 се добавя следната буква в):

„в) Компетентният орган на държавата членка предоставя на Агенцията във възможно най-кратък срок значима за безопасността информация, произтичаща от докладите за информационната сигурност, които е получил съгласно точка IS.I.OR.230 от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203.“;

б) след точка ATM/ANS.AR.A.025 се вмъква следната точка ATM/ANS.AR.A.025A:

„**ATM/ANS.AR.A.025A Незабавна реакция на инцидент или уязвимост, свързани с информационната сигурност, които оказват въздействие върху авиационната безопасност**

а) Компетентният орган прилага система за подходящо събиране, анализиране и разпространяване на информация, свързана с инциденти и уязвимости в областта на информационната сигурност с потенциално въздействие върху авиационната безопасност, които са докладвани от организациите. Това се извършва в сътрудничество с всички други съответни органи, отговарящи за информационната сигурност или киберсигурността в държавата членка, за да се подобри координацията и съвместимостта на схемите за докладване.

б) Агенцията прилага система за подходящ анализ на всяка значима за безопасността информация, получена в съответствие с точка ATM/ANS.AR.A.020, буква в), и без неоправдано забавяне предоставя на държавите членки и на Комисията всякаква информация (включително препоръки или коригиращи действия, които трябва да бъдат предприети), необходима за своевременната им реакция при инцидент или уязвимост, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, включващи продукти, части, немонтирано оборудване, лица или организации, предмет на Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение.

в) При получаване на информацията, посочена в букви а) и б), компетентният орган предприема подходящи мерки за справяне с потенциалното въздействие на инцидента или уязвимостта, свързани с информационната сигурност, върху авиационната безопасност.

г) За мерките, предприети в съответствие с буква в), се съобщава незабавно на всички лица или организации, които ги изпълняват съгласно Регламент (ЕС) 2018/1139 и свързаните с него делегирани актове и актове за изпълнение. Компетентният орган на държавата членка съобщава тези мерки и на Агенцията, а когато са необходими съвместни действия — на компетентните органи на останалите засегнати държави членки.“;

в) в точка ATM/ANS.AR.B.001 се добавя следната буква д):

„д) В допълнение към изискванията, съдържащи се в буква а), системата за управление, създадена и поддържана от компетентния орган, е в съответствие с приложение I (част IS.AR) към Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

г) точка ATM/ANS.AR.B.005 се изменя, както следва:

i) заглавието се заменя със следното:

„**ATM/ANS.AR.B.005 Разпределение на задачите**“;

ii) добавя се следната буква в):

„в) По отношение на сертифицирането и надзора над съответствието на организацията с точка ATM/ANS.OR.B.005A компетентният орган може да възложи задачи на квалифицирани органи в съответствие с буква а) или на всеки съответен орган, отговарящ за информационната сигурност или киберсигурността в държавата членка. При разпределението на задачите компетентният орган гарантира, че:

1. всички аспекти, свързани с авиационната безопасност, се координират и вземат предвид от квалифицирания орган или съответния орган;

2. резултатите от дейностите по сертифициране и надзор, извършени от квалифицирания орган или съответния орган, се интегрират в цялостното досие за сертифициране и надзор на организацията;

3. собствената му система за управление на информационната сигурност, създадена в съответствие с точка ATM/ANS.AR.B.001, буква д), обхваща всички задачи по сертифициране и продължаващ надзор, изпълнявани от негово име.“;

д) в точка ATM/ANS.AR.C.010 се добавя следната буква г):

„г) По отношение на сертифицирането и надзора над съответствието на организацията с точка ATM/ANS.OR.B.005A, в допълнение към спазването на букви а)—в), компетентният орган преразглежда всяко одобрение, издадено съгласно точка IS.I.OR.200, буква д) от настоящия регламент или точка IS.D.OR.200, буква д) от Делегиран регламент (ЕС) 2022/1645, след приложимия цикъл на одит на надзора и всеки път, когато бъдат въведени промени в обхвата на дейностите на организацията.“;

е) след точка ATM/ANS.AR.C.025 се вмъква следната точка ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Промени в системата за управление на информационната сигурност**

а) По отношение на промените, управлявани и съобщени на компетентния орган в съответствие с процедурата, посочена в точка IS.I.OR.255, буква а) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203, компетентният орган включва прегледа на тези промени в своя продължаващ надзор в съответствие с принципите, изложени в точка ATM/ANS.AR.C.010. Ако се установи несъответствие, компетентният орган уведомява организацията за това, изисква допълнителни промени и действа в съответствие с точка ATM/ANS.AR.C.050.

б) По отношение на други промени, за които се изисква заявление за одобрение в съответствие с точка IS.I.OR.255, буква б) от приложение II (част IS.I.OR) към Регламент за изпълнение (ЕС) 2023/203:

1. след като получи заявлението за промяна, компетентният орган проверява съответствието на организацията с приложимите изисквания, преди да издаде одобрението;

2. компетентният орган определя условията, при които организацията може да работи по време на прилагането на промяната;

3. ако се увери, че организацията отговаря на приложимите изисквания, компетентният орган одобрява промяната.“;

(2) приложение III (част ATM/ANS.OR) се изменя, както следва:

а) след точка ATM/ANS.OR.B.005 се вмъква следната точка ATM/ANS.OR.B.005A:

„**ATM/ANS.OR.B.005A Система за управление на информационната сигурност**

В допълнение към системата за управление, посочена в точка ATM/ANS.OR.B.005, доставчикът на услуги създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Регламент за изпълнение (ЕС) 2023/203, за да се осигури правилното управление на рисковете за информационната сигурност, които може да окажат въздействие върху авиационната безопасност.“;

б) точка ATM/ANS.OR.D.010 се заменя със следното:

„**ATM/ANS.OR.D.010 Управление на сигурността**

а) Доставчиците на аеронавигационно обслужване и на услуги по управление на потоците въздушно движение, както и управителният орган на мрежата, изграждат като неразделна част от своята система за управление, изисквана съгласно точка ATM/ANS.OR.B.005, система за управление на сигурността, за да гарантират:

1. сигурността на своите съоръжения и персонал, така че да предотвратят незаконна намеса при предоставянето на услуги;

2. сигурността на оперативните данни, които те получават, генерират или използват по друг начин, така че достъпът до тези данни да бъде ограничен — само за оправомощени лица.

б) В системата за управление на сигурността се определят:

1. процесът и процедурите, свързани с оценяване и ограничаване на риска за сигурността, наблюдението и повишаването на сигурността, прегледите на сигурността и разпространяването на изводите от тези прегледи;

2. средствата за установяване, наблюдение и откриване на пробиви в сигурността и алармиране на персонала с подходящи предупреждения относно сигурността;

3. средствата за контролиране на последиците от нарушенията на сигурността и за определяне на коригиращи действия и процедури за намаляване на риска, за да се предотврати повторно възникване.

в) Доставчиците на аеронавигационно обслужване и на услуги по управление на потоците въздушно движение, както и управителният орган на мрежата, гарантират, че техният персонал е проучен за надеждност, ако е необходимо, и координират със съответните граждански и военни органи гарантирането на сигурността на своите съоръжения, персонал и данни.

г) Аспектите, свързани с информационната сигурност, се управляват в съответствие с точка ATM/ANS.OR.B.005A.“