Съвет на
Европейския съюз

Брюксел, 18 юли 2022 г.
(OR. en)

11468/22

AVIATION 171
DELACT 120

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	14 юли 2022 г.
До:	Генералния секретариат на Съвета
№ док. Ком.:	C(2022) 4882 final
Относно:	ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА от 14.7.2022 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

Приложено се изпраща на делегациите документ C(2022) 4882 final.

Приложение: C(2022) 4882 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 14.7.2022 г.
C(2022) 4882 final

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА

от 14.7.2022 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

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ДЕЛЕГИРАНИЯ АКТ

Актуалната европейска регулаторна рамка за авиационна безопасност съдържа редица изисквания, които имат за цел да намалят вероятността от настъпване на произшествие.

Тази комбинация от изисквания позволява, дори при наличието на грешка и/или пропуск, да не се създава опасна ситуация, която би могла да доведе до произшествие или сериозен инцидент. Следователно произшествие или сериозен инцидент може да възникне само при малко вероятното случайно събитие, при което няколко пропуска се комбинират едновременно и непредвидимо.

Съществува опасение, че може да не е обърнато достатъчно внимание на ситуацията, при която съществуващите недостатъци в различни области се съчетават преднамерено и се използват от злонамерени лица, което вече не представлява случайно събитие. Този риск постоянно нараства в областта на гражданското въздухоплаване с нарастващата взаимносвързаност на настоящите информационни системи.

Вследствие на това е необходимо да се въведат изисквания за управление на рисковете за информационната сигурност, които биха могли да имат потенциално въздействие върху авиационната безопасност.

В конкретния случай на настоящия делегиран акт въведените разпоредби повишават надеждността на системите за управление и процесите и процедурите за докладване, изисквани съгласно приложение II „Съществени изисквания относно летателната годност“ и приложение VII „Съществени изисквания за летища“ към Регламент (ЕС) 2018/1139([1]) за проектантските и производствените организации и за летищните оператори и доставчиците на обслужване по управление на перона.

2. КОНСУЛТАЦИИ ПРЕДИ ПРИЕМАНЕТО НА АКТА

В съответствие с член 128, параграф 4 от Регламент (ЕС) 2018/1139 преди приемането на делегиран акт Комисията се консултира с експерти, определени от всяка държава членка в съответствие с принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество. Проектът на делегирания акт беше представен на групата на експертите по авиационна безопасност, която включва представители на държавите членки, на нейните заседания, проведени на 17 февруари и 29 юни 2022 г. Настоящият делегиран акт се основава на Становище № 03/2021 на ЕААБ, чието съдържание беше публично обсъдено чрез Известие за предложено изменение (NPA) 2019-07 „Управление на рисковете за информационната сигурност“ ([2])(RMT.0720), публикувано от ЕААБ на 27 май 2019 г.

1 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 (ОВ L 212, 22.8.2018 г., стр. 1) (https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:02018R1139-20210725&qid=1654155476436&from=EN).

2 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

3. ПРАВНИ ЕЛЕМЕНТИ НА ДЕЛЕГИРАНИЯ АКТ

С член 19, параграф 1 и член 39, параграф 1 от Регламент (ЕС) 2018/1139 на Комисията се предоставя правомощието да приема делегирани актове в съответствие с член 128 от посочения регламент за определяне на подробни правила по отношение на организациите, отговарящи за проектирането и производството на продукти, части и немонтирано оборудване, както и по отношение на организациите, отговарящи за експлоатацията на летища и за предоставянето на обслужване по управление на перона.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА

от 14.7.2022 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

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([3]), и по-специално член 19, параграф 1, буква ж) и член 39, параграф 1, буква б) 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, проектантските и производствените организации трябва да въведат и поддържат система за управление с цел управление на рисковете за безопасността.

(2) Освен това, в съответствие със съществените изисквания, определени в точки 2.2.1 и 5.2 от приложение VII към Регламент (ЕС) 2018/1139, летищните оператори и организациите, отговарящи за предоставянето на обслужване по управление на перона, трябва да въведат и поддържат система за управление с цел управление на рисковете за безопасността.

(3) Рисковете за безопасността, посочени в съображения 1 и 2, могат да произтичат от различни източници, включително недостатъци при проектирането и техническото обслужване, аспекти, свързани с човешките възможности, заплахи за околната среда и за информационната сигурност. Поради това системите за управление, въведени от организациите, както е посочено в съображения 1 и 2, 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

3 ОВ L 212, 22.8.2018 г., стр. 1.

настоящите информационни системи стават все по-взаимносвързани и все по-често са мишена на злонамерени лица.

(4) 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 ефективността на хората.

(5) Значителен брой организации вече използват международни стандарти, като например ISO 27001, за да обезпечат сигурността на цифровата информация и данни. Възможно е обаче тези стандарти да не отговарят напълно на всички особености на гражданското въздухоплаване.

(6) Следователно е целесъобразно да се определят изисквания за управление на рисковете за информационната сигурност, които биха могли да имат потенциално въздействие върху авиационната безопасност.

(7) От съществено значение е тези изисквания да обхващат различните области на въздухоплаването и техните връзки, тъй като въздухоплаването представлява система от силно взаимносвързани системи. Поради това изискванията следва да се прилагат за всички организации, от които вече се изисква да разполагат със система за управление в съответствие със съществуващото законодателство на Съюза в областта на авиационната безопасност.

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

(9) 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([4]) и в член 14 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета([5]).

(10) Определението за информационна сигурност, използвано за целите на настоящия правен акт, не следва да се тълкува като различаващо се от определението за сигурност на мрежите и информационните системи, установено в Директива (ЕС) 2016/1148.

(11) За да се избегне дублиране на правните изисквания, когато организациите, обхванати от настоящия регламент, вече са предмет на изисквания за сигурност, произтичащи от други актове на Съюза, посочени в съображение 9, 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.

---

[4] 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).

[5] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

(12) Организациите, обхванати от настоящия регламент, които вече са предмет на изискванията за сигурност, произтичащи от Регламент (ЕС) 2015/1998, следва също да отговарят на изискванията на приложение I (част IS.D.OR.230 „Схема за външно докладване във връзка с информационната сигурност“) към настоящия регламент, тъй като Регламент (ЕС) 2015/1998 не съдържа разпоредби, свързани с външното докладване на инциденти, свързани с информационната сигурност.

(13) Регламенти (ЕС) № 748/2012([6]) и (ЕС) № 139/2014([7]) следва да бъдат изменени, за да се установи връзката между системите за управление, предвидени в изброените по-горе регламенти, и изискванията за управление на информационната сигурност, предвидени в настоящия регламент.

(14) С цел да се предостави на организациите достатъчно време, за да осигурят спазването на новите правила и процедури, въведени с настоящия регламент, настоящият регламент следва да започне да се прилага 3 години след датата на влизане в сила.

(15) Изискванията, определени в настоящия регламент, се основават на Становище № 03/2021([8]), издадено от Агенцията в съответствие с член 75, параграф 2, букви б) и в) и член 76, параграф 1 от Регламент (ЕС) 2018/1139.

(16) В съответствие с член 128, параграф 4 от Регламент (ЕС) 2018/1139 Комисията се консултира с експерти, определени от всяка държава членка съгласно принципите, залегнали в Междуинституционалното споразумение от 13 април 2016 г. за по-добро законотворчество([9]),

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет

С настоящия регламент се определят изискванията, на които трябва да отговарят организациите, посочени в член 2, за да 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, и да откриват събития, свързани с информационната сигурност, да идентифицират тези, които се считат за инциденти, свързани с информационната сигурност, с потенциално въздействие върху авиационната безопасност, както и да

---

6 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.

7 Регламент (ЕС) № 139/2014 на Комисията от 12 февруари 2014 г. за определяне на изискванията и административните процедури във връзка с летищата в съответствие с Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета.

8 https://www.easa.europa.eu/document-library/opinions

9 ОВ L 123, 12.5.2016 г., стр. 1.

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

Член 2

Обхват

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

а) производствени и проектантски организации, които са предмет на подчасти Ж и Й на раздел А от приложение I (част 21) към Регламент (ЕС) № 748/2012, с изключение на проектантски и производствени организации, които участват единствено в проектирането и/или производството на въздухоплавателни средства ELA2 съгласно определението в член 1, параграф 2, буква й) от Регламент (ЕС) № 748/2012;

б) летищни оператори и доставчици на обслужване по управление на перона, за които се прилага приложение III — част „Изисквания към организацията“ (част ADR.OR)“ към Регламент (ЕС) № 139/2014([10]).

2. Настоящият регламент не засяга изискванията за информационна сигурност и киберсигурност, определени в точка 1.7 от приложението към Регламент за изпълнение (ЕС) 2015/1998 на Комисията[(11)] и в член 14 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета[(12)].

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 идентифицирано 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;

---

10 Регламент (ЕС) № 139/2014 на Комисията от 12 февруари 2014 г. 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).

11 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).

12 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).

(3) „инцидент“ означава всяко събитие, което има 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;

(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, произтичащи от друго законодателство на Съюза

1. Ако организация, посочена в член 2, отговаря на изискванията за сигурност, определени в член 14 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета, 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, 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([13]), 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.D.OR.230 от приложението към настоящия регламент, която трябва да бъде спазена.

3. Комисията, след консултация с ЕААБ 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.

[13] 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).

Член 5

Компетентен орган

1. Органът, отговарящ за сертифицирането и контрола за спазването на настоящия регламент, е:

   а) по отношение на организациите, посочени в член 2, буква а) — компетентният орган, определен в съответствие с приложение I (част 21) към Регламент (ЕС) № 748/2012;

   б) по отношение на организациите, посочени в член 2, буква б) — компетентният орган, определен в съответствие с приложение III (част ADR.OR) към Регламент (ЕС) № 139/2014.

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 гарантира ефективен контрол върху всички изисквания, които трябва да бъдат изпълнени от организацията.

Член 6

Изменение на Регламент (ЕС) № 748/2012

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

(1) съдържанието се изменя, както следва:

   а) след заглавие 21.A.139 се вмъква следното заглавие:

   „21.A.139A Система за управление на информационната сигурност“;

   б) след заглавие 21.A.239 се вмъква следното заглавие:

   „21.A.239A Система за управление на информационната сигурност“;

(2) след точка 21.A.139 се вмъква следната точка 21.A.139A:

„21.A.139A Система за управление на информационната сигурност

В допълнение към системата за управление на производството, изисквана съгласно точка 21.A.139, производствената организация създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Делегиран регламент (ЕС) 202X/XXXX [До Службата за публикации: моля, въведете референтния номер на настоящия делегиран регламент], за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.“;

(2) след точка 21.A.239 се вмъква следната точка 21.A.239A:

„21.A.239A Система за управление на информационната сигурност

В допълнение към системата за управление на проекта, изисквана съгласно точка 21.A.239, проектантската организация създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Делегиран регламент (ЕС) 202X/XXXX [До Службата за публикации: моля, въведете референтния номер на настоящия делегиран регламент], за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.“.

Член 7

Изменение на Регламент (ЕС) № 139/2014

Приложение III (част ADR.OR) към Регламент (ЕС) № 139/2014([14]) се изменя, както следва:

(1) след точка ADR.OR.D.005 се вмъква следната точка ADR.OR.D.005A:

„ADR.OR.D.005A Система за управление на информационната сигурност

Летищният оператор създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Делегиран регламент (ЕС) 202X/XXXX [До Службата за публикации: моля, въведете референтния номер на настоящия делегиран регламент], за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.“;

(2) точка ADR.OR.D.007 се заменя със следното:

„ADR.OR.D.007 Управление на аеронавигационни данни и аеронавигационна информация

а) Като част от своята система за управление летищният оператор въвежда и поддържа система за управление на качеството, която обхваща следните дейности:

(1) неговите дейности, свързани с аеронавигационните данни;

(2) неговите дейности по предоставяне на аеронавигационна информация.

б) Като част от своята система за управление летищният оператор създава система за управление на сигурността с цел да гарантира сигурността на оперативните данни, които получава, създава или използва по друг начин, така че достъпът до тези оперативни данни да бъде ограничен само до оправомощени лица.

---

14 Регламент (ЕС) № 139/2014 на Комисията от 12 февруари 2014 г. 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).

в) В системата за управление на сигурността се определят следните елементи:

(3) процедурите, свързани с оценката и смекчаването на рисковете за сигурността на данните, наблюдението и подобряването на сигурността, прегледите на сигурността и разпространението на придобития опит;

(4) средствата за откриване на пробиви в сигурността и алармиране на персонала с подходящи предупреждения относно сигурността;

(5) средствата за контролиране на последиците от пробиви в сигурността и за определяне на възстановителни дейности и процедури за намаляване на риска с цел предотвратяването на повторно възникване.

(г) Летищният оператор осигурява проучване за надеждност на своя персонал във връзка със сигурността на аеронавигационните данни.

(д) Аспектите, свързани с информационната сигурност, се управляват в съответствие с точка ADR.OR.D.005A.“;

(3) след точка ADR.OR.F.045 се вмъква следната точка ADR.OR.F.045A:

„ADR.OR.F.045A Система за управление на информационната сигурност

Организацията, отговаряща за предоставянето на обслужване по управление на перона, създава, въвежда и поддържа система за управление на информационната сигурност в съответствие с Делегиран регламент (ЕС) 202X/XXXX [До Службата за публикации: моля, въведете референтния номер на настоящия делегиран регламент], за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.“.

Член 8

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

Той започва да се прилага ***3 години*** *след датата на влизане в сила*.

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

Съставено в Брюксел на 14.7.2022 година.

За Комисията
Председател
Ursula VON DER LEYEN