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

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 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 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.

([1]) ОВ L 212, 22.8.2018 г., стр. 1.

(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 ([2]) и в член 14 от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([3]).

(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.

(12) Организациите, обхванати от настоящия регламент, които вече са предмет на изискванията за сигурност, произтичащи от Регламент за изпълнение (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 за изпълнение (ЕС) 2015/1998 не съдържа разпоредби, свързани с външното докладване на инциденти, свързани с информационната сигурност.

(13) Регламенти (ЕС) № 748/2012 ([4]) и (ЕС) № 139/2014 ([5]) на Комисията 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 ([6]), 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 ([7]),

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

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

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

([7]) ОВ L 123, 12.5.2016 г., стр. 1.

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.

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 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 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;

(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, 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 ([8]), 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.

([8]) 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).

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.

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) 2022/1645 на Комисията (*), за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.

_____

(*) 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)“;

(3) 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) 2022/1645 , 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 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) 2022/1645 на Комисията (*), за да се осигури доброто управление на рисковете за информационната сигурност, които могат да окажат въздействие върху авиационната безопасност.

_____

(*) 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)“;

(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.

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

(1) 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;

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

(3) 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) 2022/1645, 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 се прилага от 16 октомври 2025 г.

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

Съставено в Брюксел на 14 юли 2022 година.

За Комисията
Председател
Ursula VON DER LEYEN

ПРИЛОЖЕНИЕ

ИНФОРМАЦИОННА СИГУРНОСТ — ИЗИСКВАНИЯ КЪМ ОРГАНИЗАЦИЯТА

[ЧАСТ — IS.D.OR]

IS.D.OR.100 Обхват

IS.D.OR.200 Система за управление на информационната сигурност

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

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

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

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

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

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

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

IS.D.OR.240 Изисквания към персонала

IS.D.OR.245 Водене на документация

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

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

IS.D.OR.260 Постоянно подобряване

IS.D.OR.100 Обхват

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

IS.D.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.D.OR.205;

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

4. прилага схема за вътрешно докладване във връзка с информационната сигурност в съответствие с точка IS.D.OR.215;

5. определя и прилага, в съответствие с точка IS.D.OR.220, необходимите мерки за откриване на събития, свързани с информационната сигурност, идентифицира тези събития, които се считат за инциденти с потенциално въздействие върху авиационната безопасност, с изключение на разрешеното по точка IS.D.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.D.OR.225 за отстраняване на констатациите, за които компетентният орган я е информирал;

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

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

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

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

12. наблюдава съответствието на организацията с изискванията на настоящия регламент и предоставя обратна информация относно констатациите на отговорния ръководител или, в случай на проектантски организации, на ръководителя на проектантската организация, 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.D.OR.260.

в) Организацията документира в съответствие с точка IS.D.OR.250 всички ключови процеси, процедури, роли и отговорности, необходими за спазване на точка IS.D.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.D.OR.255.

г) Процесите, процедурите, ролите и отговорностите, установени от организацията с цел спазване на точка IS.D.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, съдържащи се в Регламент (ЕС) № 376/2014 ([1]), и изискванията по точка IS.D.OR.200, буква а), точка 13, на организацията може да бъде издадено одобрение от компетентния орган да не прилага изискванията, посочени в букви а)—г), и свързаните изисквания, съдържащи се в точки IS.D.OR.205—IS.D.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.D.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.D.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 точка 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 могат да имат потенциално въздействие върху авиационната безопасност. За всеки установен риск организацията:

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

([1]) Регламент (ЕС) № 376/2014 на Европейския парламент и на Съвета от 3 април 2014 г. за докладване, анализ и последващи действия във връзка със събития в гражданското въздухоплаване, за изменение на Регламент (ЕС) № 996/2010 на Европейския парламент и на Съвета и за отмяна на Директива 2003/42/ЕО на Европейския парламент и на Съвета и на регламенти (ЕО) № 1321/2007 и (ЕО) № 1330/2007 на Комисията (ОВ L 122, 24.4.2014 г., стр. 18).

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. 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.D.OR.210.

За да се улесни взаимната съпоставимост на оценките на риска, при определянето на нивото на риска съгласно точка 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 в), 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 идентифициране, анализ и класификация на рисковете;

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

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

а) Организацията разработва мерки за справяне с неприемливите рискове, установени в съответствие с точка IS.D.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 смекчи последиците за авиационната безопасност, свързани с реализирането на сценария за заплаха;

3. да избегне рисковете.

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

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

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

IS.D.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.D.OR.230.

б) Тази схема и процесът, посочени в точка IS.D.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 точка 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.D.OR.205 и IS.D.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 точка 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.D.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.D.OR.205, и на резултата от третирането на риска, извършено в съответствие с точка IS.D.OR.210, организацията прилага мерки за откриване на инциденти и уязвимости, които показват потенциалното възникване на неприемливи рискове и които могат 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), точка 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.D.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.D.OR.205, буква а), в рамките на период на възстановяване, определен предварително от организацията.

IS.D.OR.225 Отговор 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. съставя план за 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.D.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. Също така:

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 до 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, отговаряща 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.D.OR.235 Възлагане на дейности по управление на информационната сигурност

а) Организацията гарантира, че когато възлага на други организации която и да е част от дейностите, посочени в точка IS.D.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 съответствие с приложимите изисквания, определени в настоящия регламент.

IS.D.OR.240 Изисквания към персонала

а) Отговорният ръководител на организацията или, в случай на проектантски организации, ръководителят на проектантската организация, определен в съответствие с регламенти (ЕС) № 748/2012 и (ЕС) № 139/2014, както е посочено в член 2, точка 1, букви а) и б) 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.D.OR.200, буква а), точка 1;

3. показва основно разбиране на разпоредбите на настоящия регламент.

б) Отговорният ръководител или, в случай на проектантски организации, ръководителят на проектантската организация, 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 или, в случай на проектантски организации, на ръководителя на проектантската организация, и притежават необходимите знания, образование и опит, за да изпълняват своите отговорности. В процедурите се определя кой замества дадено лице в случай на продължителното му отсъствие.

в) Отговорният ръководител или, в случай на проектантски организации, ръководителят на проектантската организация, назначава лице или група лица, които отговарят за управлението на функцията по наблюдение на съответствието, посочена в точка IS.D.OR.200, буква а), точка 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 или, в случай на проектантски организации, ръководителят на проектантската организация, може да делегира своите дейности на едно общо отговорно лице.

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

д) Отговорният ръководител или ръководителят на проектантската организация, 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.D.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 отчита 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.D.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.D.OR.200, буква д);

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

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

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

v) записи на инциденти и уязвимости, свързани с информационната сигурност, докладвани в съответствие със схемите за докладване, посочени в точки IS.D.OR.215 и IS.D.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 точка 1, подточка i), се съхраняват най-малко 5 години след изтичане на валидността на одобрението.

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

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

5. Записите, посочени в точка 1, подточка vi), се съхраняват, докато конкретните събития, свързани с информационната сигурност, бъдат преразгледани в период, определен 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 или кражба чрез идентифициране на информацията, при необходимост, съгласно нейното ниво на класификация за целите на сигурността. Организацията гарантира, че записите се съхраняват, като се използват средства за гарантиране на целостта, автентичността и разрешения достъп.

IS.D.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 мениджър или, в случай на проектантски организации, от ръководителя на проектантската организация, потвърждаваща, че организацията ще работи по всяко време в съответствие с настоящото приложение и с ISMM. Ако отговорният ръководител или, в случай на проектантски организации, ръководителят на проектантската организация, 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, посочени в точка IS.D.OR.240, букви б) и в);

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

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

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

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

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

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

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

i) точка IS.D.OR.200, буква в) относно документирането;

ii) процедурите, определящи начина, по който организацията контролира всички възложени на подизпълнители дейности, посочени в точка IS.D.OR.200, буква а), точка 9;

iii) процедурата за изменение на ISMM, определена 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.D.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.D.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;
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.D.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.