II

(Nelegislatívne akty)

NARIADENIA

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2023/203

z 27. októbra 2022,

ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139, pokiaľ ide o požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 1321/2014, (EÚ) č. 965/2012, (EÚ) č. 1178/2011, (EÚ) 2015/340, vykonávacie nariadenia Komisie (EÚ) 2017/373 a (EÚ) 2021/664, a pre príslušné orgány, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012, (EÚ) č. 1321/2014, (EÚ) č. 965/2012, (EÚ) č. 1178/2011, (EÚ) 2015/340, vykonávacie nariadenia Komisie (EÚ) 2017/373, (EÚ) č. 139/2014 a (EÚ) 2021/664, a ktorým sa menia nariadenia Komisie (EÚ) č. 1178/2011, (EÚ) č. 748/2012, (EÚ) č. 965/2012, (EÚ) č. 139/2014, (EÚ) č. 1321/2014, (EÚ) 2015/340 a vykonávacie nariadenia Komisie (EÚ) 2017/373 a (EÚ) 2021/664

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1139 zo 4. júla 2018 o spoločných pravidlách v oblasti civilného letectva, ktorým sa zriaďuje Agentúra Európskej únie pre bezpečnosť letectva a ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 2111/2005, (ES) č. 1008/2008, (EÚ) č. 996/2010, (EÚ) č. 376/2014 a smernice Európskeho parlamentu a Rady 2014/30/EÚ a 2014/53/EÚ a zrušujú nariadenia Európskeho parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nariadenie Rady (EHS) č. 3922/91 ([1]), a najmä na jeho článok 17 ods. 1 písm. b), článok 27 ods. 1 písm. a), článok 31 ods. 1 písm. b), článok 43 ods. 1 písm. b), článok 53 ods. 1 písm. a) a článok 62 ods. 15 písm. c),

keďže:

(1) V súlade so základnými požiadavkami stanovenými v bode 3.1 písm. b) prílohy II k nariadeniu (EÚ) 2018/1139 majú organizácie pre riadenie zachovania letovej spôsobilosti a organizácie vykonávajúce údržbu zaviesť a udržiavať systém riadenia na riadenie bezpečnostných rizík.

(2) Okrem toho v súlade so základnými požiadavkami stanovenými v bode 3.3 písm. b) a bode 5 písm. b) prílohy IV k nariadeniu (EÚ) 2018/1139 majú výcvikové organizácie pre pilotov, výcvikové organizácie pre palubných sprievodcov, poverené letecké zdravotnícke zariadenia pre posádku a prevádzkovatelia výcvikových zariadení na simuláciu letu zaviesť a udržiavať systém riadenia na riadenie bezpečnostných rizík.

(3) Okrem toho v súlade so základnými požiadavkami stanovenými v bode 8.1 písm. c) prílohy V k nariadeniu (EÚ) 2018/1139 majú leteckí prevádzkovatelia zaviesť a udržiavať systém riadenia na riadenie bezpečnostných rizík.

(4) Okrem toho v súlade so základnými požiadavkami stanovenými v bode 5.1 písm. c) a bode 5.4 písm. b) prílohy VIII k nariadeniu (EÚ) 2018/1139 majú poskytovatelia manažmentu letovej prevádzky a leteckých navigačných služieb, poskytovatelia služieb U-space a jednotliví poskytovatelia spoločných informačných služieb a výcvikové organizácie a poverené letecké zdravotnícke zariadenia pre riadiacich letovej prevádzky zaviesť a udržiavať systém riadenia na riadenie bezpečnostných rizík.

([1]) Ú. v. EÚ L 212, 22.8.2018, s. 1.

(5) Uvedené bezpečnostné riziká môžu pochádzať z rôznych zdrojov, ako sú projekčné a údržbové nedostatky, aspekty ľudskej výkonnosti, environmentálne hrozby a hrozby pre informačnú bezpečnosť. V systémoch riadenia zavedených Agentúrou Európskej únie pre bezpečnosť letectva (ďalej len „agentúra“) a národnými príslušnými orgánmi a organizáciami uvedenými v odôvodneniach by sa preto mali zohľadňovať nielen bezpečnostné riziká vyplývajúce z náhodných udalostí, ale aj bezpečnostné riziká vyplývajúce z hrozieb pre informačnú bezpečnosť, pri ktorých môžu jednotlivci so zlým úmyslom existujúce nedostatky zneužiť. Tieto riziká v oblasti informačnej bezpečnosti v prostredí civilného letectva neustále narastajú, keďže súčasné informačné systémy sú čoraz viac prepojené a čoraz viac sa stávajú cieľom aktérov so zlými úmyslami.

(6) Riziká spojené s týmito informačnými systémami sa neobmedzujú len na možné útoky na kybernetický priestor, ale zahŕňajú aj hrozby, ktoré môžu ovplyvniť procesy a postupy, ako aj výkonnosť ľudí.

(7) Značný počet organizácií už používa medzinárodné normy, ako napríklad ISO 27001, s cieľom riešiť zabezpečenie digitálnych informácií a údajov. Uvedené normy nezohľadňujú v plnej miere všetky osobitosti civilného letectva. Preto je vhodné stanoviť požiadavky na riadenie rizík v oblasti informačnej bezpečnosti, ktoré by mohli mať vplyv na bezpečnosť letectva.

(8) Je nevyhnutné, aby sa uvedené požiadavky vzťahovali na všetky oblasti letectva a ich rozhrania, keďže letectvo je vysoko prepojeným systémom systémov. Preto by sa mali uplatňovať na všetky organizácie a príslušné orgány, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012 ([2]), (EÚ) č. 1321/2014 ([3]), (EÚ) č. 965/2012 ([4]), (EÚ) č. 1178/2011 ([5]), (EÚ) 2015/340 ([6]), (EÚ) č. 139/2014 ([7]) a vykonávacie nariadenie Komisie (EÚ) 2021/664 ([8]), a to aj na tie, ktoré sú už povinné mať systém riadenia v súlade s existujúcimi právnymi predpismi Únie v oblasti bezpečnosti letectva. Niektoré organizácie by však mali byť vylúčené z rozsahu pôsobnosti tohto nariadenia, aby sa zabezpečila primeraná proporcionalita k nižším rizikám v oblasti informačnej bezpečnosti, ktoré predstavujú pre systém letectva.

(9) Požiadavky stanovené v tomto nariadení by mali zabezpečiť dôsledné vykonávanie vo všetkých oblastiach letectva, pričom by mali mať minimálny vplyv na právne predpisy Únie v oblasti bezpečnosti letectva, ktoré sa už v týchto oblastiach uplatňujú.

([2]) Nariadenie Komisie (EÚ) č. 748/2012 z 3. augusta 2012 stanovujúce vykonávacie pravidlá osvedčovania letovej spôsobilosti a environmentálneho osvedčovania lietadiel a prislúchajúcich výrobkov, častí a zariadení, ako aj osvedčovania projekčných a výrobných organizácií (Ú. v. EÚ L 224, 21.8.2012, s. 1).

([3]) Nariadenie Komisie (EÚ) č. 1321/2014 z 26. novembra 2014 o zachovaní letovej spôsobilosti lietadiel a výrobkov, súčastí a zariadení leteckej techniky a o schvaľovaní organizácií a personálu zapojených do týchto činností (prepracované znenie) (Ú. v. EÚ L 362, 17.12.2014, s. 1).

([4]) Nariadenie Komisie (EÚ) č. 965/2012 z 5. októbra 2012, ktorým sa ustanovujú technické požiadavky a administratívne postupy týkajúce sa leteckej prevádzky podľa nariadenia Európskeho parlamentu a Rady (ES) č. 216/2008 (Ú. v. EÚ L 296, 25.10.2012, s. 1).

([5]) Nariadenie Komisie (EÚ) č. 1178/2011 z 3. novembra 2011, ktorým sa ustanovujú technické požiadavky a administratívne postupy týkajúce sa posádky civilného letectva podľa nariadenia Európskeho parlamentu a Rady (ES) č. 216/2008 (Ú. v. EÚ L 311, 25.11.2011, s. 1).

([6]) Nariadenie Komisie (EÚ) 2015/340 z 20. februára 2015, ktorým sa stanovujú technické požiadavky a administratívne postupy týkajúce sa preukazov a osvedčení riadiacich letovej prevádzky podľa nariadenia Európskeho parlamentu a Rady (ES) č. 216/2008 a ktorým sa mení vykonávacie nariadenie Komisie (EÚ) č. 923/2012 a zrušuje nariadenie Komisie (EÚ) č. 805/2011 (Ú. v. EÚ L 63, 6.3.2015, s. 1).

([7]) Nariadenie Komisie (EÚ) č. 139/2014 z 12. februára 2014, ktorým sa stanovujú technické požiadavky a administratívne postupy týkajúce sa letísk podľa nariadenia Európskeho parlamentu a Rady (ES) č. 216/2008 (Ú. v. EÚ L 44, 14.2.2014, s. 1).

([8]) Vykonávacie nariadenie Komisie (EÚ) 2021/664 z 22. apríla 2021 o regulačnom rámci pre priestor U-space (Ú. v. EÚ L 139, 23.4.2021, s. 161).

(10) Požiadavkami stanovenými v tomto nariadení by nemali byť dotknuté požiadavky na informačnú bezpečnosť a kybernetickú bezpečnosť stanovené v bode 1.7 prílohy k vykonávaciemu nariadeniu Komisie (EÚ) 2015/1998 ([9]) a v článku 14 smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([10]).

(11) Bezpečnostné požiadavky stanovené v článkoch 33 až 43 hlavy V „Bezpečnosť VPÚ“ nariadenia Európskeho parlamentu a Rady (EÚ) 2021/696 ([11]) sa považujú za rovnocenné s požiadavkami stanovenými v tomto nariadení s výnimkou ustanovenia IS.I.OR.230 prílohy II k tomuto nariadeniu, ktoré by sa mali dodržiavať.

(12) S cieľom zabezpečiť právnu istotu by sa výklad pojmu „informačná bezpečnosť“ vymedzeného v tomto nariadení, ktorý vyjadruje jeho bežné používanie v civilnom letectve na celom svete, mal považovať za konzistentný s výkladom pojmu „bezpečnosť sietí a informačných systémov“ v zmysle článku 4 ods. 2 smernice (EÚ) 2016/1148. Vymedzenie pojmu informačnej bezpečnosti použité na účely tohto nariadenia by sa nemalo vykladať odlišne od vymedzenia pojmu bezpečnosti sietí a informačných systémov stanoveného v smernici (EÚ) 2016/1148.

(13) S cieľom zabrániť duplicite právnych požiadaviek, ak organizácie, na ktoré sa vzťahuje toto nariadenie, už podliehajú bezpečnostným požiadavkám vyplývajúcim z aktov Únie uvedených v odôvodneniach (10) a 11, ktorých účinky sú rovnocenné s ustanoveniami tohto nariadenia, súlad s uvedenými bezpečnostnými požiadavkami by sa mal považovať za súlad s požiadavkami stanovenými v tomto nariadení.

(14) Organizácie, na ktoré sa vzťahuje toto nariadenie a ktoré už podliehajú bezpečnostným požiadavkám vyplývajúcim z vykonávacieho nariadenia (EÚ) 2015/1998 alebo nariadenia (EÚ) 2021/696 alebo z oboch, by mali spĺňať aj požiadavky prílohy II (časť IS.I.OR.230 „Systém externého nahlasovania informačnej bezpečnosti“) k tomuto nariadeniu, keďže žiadne nariadenie neobsahuje ustanovenia týkajúce sa externého nahlasovania incidentov v oblasti informačnej bezpečnosti.

(15) V záujme úplnosti by sa nariadenia (EÚ) č. 1178/2011, (EÚ) č. 748/2012, (EÚ) č. 965/2012, (EÚ) č. 139/2014, (EÚ) č. 1321/2014, (EÚ) 2015/340 a vykonávacie nariadenia (EÚ) 2017/373 ([12]) a (EÚ) 2021/664 mali zmeniť s cieľom zaviesť požiadavky na systém riadenia informačnej bezpečnosti stanovené v tomto nariadení spolu so systémami riadenia, ktoré sú v ňom stanovené, a stanoviť požiadavky príslušných orgánov, pokiaľ ide o dohľad nad organizáciami, ktoré vykonávajú uvedené požiadavky na riadenie informačnej bezpečnosti.

(16) S cieľom poskytnúť organizáciám dostatočný čas na zabezpečenie súladu s novými pravidlami a postupmi by sa toto nariadenie malo začať uplatňovať tri roky po nadobudnutí jeho účinnosti, s výnimkou poskytovateľa leteckých navigačných služieb Európskej prekryvnej služby geostacionárnej navigácie (EGNOS) vymedzenej vo vykonávacom nariadení (EÚ) 2017/373, v prípade ktorého by sa z dôvodu prebiehajúcej bezpečnostnej akreditácie systému a služieb EGNOS v súlade s nariadením (EÚ) 2021/696 toto nariadenie malo začať uplatňovať od 1. januára 2026.

(17) Požiadavky stanovené v tomto nariadení vychádzajú zo stanoviska č. 03/2021 ([13]) vydaného agentúrou v súlade s článkom 75 ods. 2 písm. b) a c) a článkom 76 ods. 1 nariadenia (EÚ) 2018/1139.

([9]) Vykonávacie nariadenie Komisie (EÚ) 2015/1998 z 5. novembra 2015, ktorým sa stanovujú podrobné opatrenia na vykonávanie spoločných základných noriem bezpečnostnej ochrany letectva (Ú. v. EÚ L 299, 14.11.2015, s. 1).

([10]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

([11]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/696 z 28. apríla 2021, ktorým sa zriaďuje Vesmírny program Únie a Agentúra Európskej únie pre vesmírny program a ktorým sa zrušujú nariadenia (EÚ) č. 912/2010, (EÚ) č. 1285/2013 a (EÚ) č. 377/2014 a rozhodnutie č. 541/2014/EÚ (Ú. v. EÚ L 170, 12.5.2021, s. 69).

([12]) Vykonávacie nariadenie Komisie (EÚ) 2017/373 z 1. marca 2017, ktorým sa stanovujú spoločné požiadavky na poskytovateľov manažmentu letovej prevádzky/leteckých navigačných služieb a na ostatné funkcie siete manažmentu letovej prevádzky, ktorým sa zrušuje nariadenie (ES) č. 482/2008, vykonávacie nariadenia (EÚ) č. 1034/2011, (EÚ) č. 1035/2011 a (EÚ) 2016/1377 a ktorým sa mení nariadenie (EÚ) č. 677/2011 (Ú. v. EÚ L 62, 8.3.2017, s. 1).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) Požiadavky stanovené v tomto nariadení sú v súlade so stanoviskom Výboru pre uplatňovanie spoločných bezpečnostných pravidiel v oblasti civilného letectva zriadeného článkom 127 nariadenia (EÚ) 2018/1139,

PRIJALA TOTO NARIADENIE:

Článok 1

Predmet úpravy

Týmto nariadením sa stanovujú požiadavky, ktoré musia spĺňať organizácie a príslušné orgány, aby:

a) identifikovali a riadili riziká v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva, ktoré by mohli ovplyvniť systémy informačných a komunikačných technológií a údaje používané na účely civilného letectva;

b) odhalili udalosti v oblasti informačnej bezpečnosti a identifikovali tie udalosti, ktoré sa považujú za incidenty informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva;

c) reagovali na uvedené incidenty informačnej bezpečnosti a zotavili sa z nich.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa uplatňuje na tieto organizácie:

a) organizácie vykonávajúce údržbu, na ktoré sa vzťahuje oddiel A prílohy II (časť 145) k nariadeniu (EÚ) č. 1321/2014, s výnimkou tých, ktoré sa podieľajú výlučne na údržbe lietadiel v súlade s prílohou Vb (časť ML) k nariadeniu (EÚ) č. 1321/2014;

b) organizácie pre riadenie zachovania letovej spôsobilosti (CAMO), na ktoré sa vzťahuje oddiel A prílohy Vc (časť CAMO) k nariadeniu (EÚ) č. 1321/2014, s výnimkou tých, ktoré sa podieľajú výlučne na riadení zachovania letovej spôsobilosti lietadiel v súlade s prílohou Vb (časť ML) k nariadeniu (EÚ) č. 1321/2014;

c) leteckí prevádzkovatelia, na ktorých sa vzťahuje príloha III (časť ORO) k nariadeniu (EÚ) č. 965/2012, s výnimkou prevádzkovateľov, ktorí sa podieľajú výlučne na prevádzke ktoréhokoľvek z týchto zariadení:

   i) lietadlo ELA2 vymedzené v článku 1 ods. 2 písm. j) nariadenia (EÚ) č. 748/2012;

   ii) jednomotorové vrtuľové letúny s maximálnou prevádzkovou konfiguráciou sedadiel pre päť alebo menej cestujúcich, ktoré nie sú klasifikované ako zložité motorové lietadlá, pri vzlete a pristátí na tom istom letisku alebo mieste prevádzky a pri prevádzke podľa pravidiel letu za viditeľnosti (VFR) počas dňa;

   iii) jednomotorové vrtuľníky s maximálnou prevádzkovou konfiguráciou sedadiel pre päť alebo menej cestujúcich, ktoré nie sú klasifikované ako zložité motorové lietadlá, pri vzlete a pristátí na tom istom letisku alebo mieste prevádzky a pri prevádzke podľa VFR počas dňa;

d) organizácie schválené na výcvik (ATO), na ktoré sa vzťahuje príloha VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011, s výnimkou tých, ktoré sa podieľajú výlučne na výcvikových činnostiach lietadiel ELA2 vymedzených v článku 1 ods. 2 písm. j) nariadenia (EÚ) č. 748/2012, alebo ktoré sa podieľajú výlučne na teoretickom výcviku;

e) poverené letecké zdravotnícke zariadenia pre posádky, na ktoré sa vzťahuje príloha VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011;

f) prevádzkovatelia výcvikových zariadení na simuláciu letu (FSTD), na ktorých sa vzťahuje príloha VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011, s výnimkou tých, ktorí sa podieľajú výlučne na prevádzke FSTD pre lietadlá ELA2 podľa vymedzenia v článku 1 ods. 2 písm. j) nariadenia (EÚ) č. 748/2012;

g) výcvikové organizácie pre riadiacich letovej prevádzky (ATCO TO) a poverené letecké zdravotnícke zariadenia pre riadiacich letovej prevádzky, na ktoré sa vzťahuje príloha III (časť ATCO.OR) k nariadeniu (EÚ) 2015/340;

h) organizácie, na ktoré sa vzťahuje príloha III (časť ATM/ANS.OR) k vykonávaciemu nariadeniu (EÚ) 2017/373, okrem týchto poskytovateľov služieb:

i) poskytovatelia leteckých navigačných služieb, ktorí sú držiteľmi obmedzeného osvedčenia v súlade s ustanovením ATM/ANS.OR.A.010 uvedenej prílohy;

ii) poskytovatelia letových informačných služieb, ktorí podávajú vyhlásenia o svojich činnostiach v súlade s ustanovením ATM/ANS.OR.A.015 uvedenej prílohy;

i) poskytovatelia služieb U-space a jednotliví poskytovatelia spoločných informačných služieb, na ktorých sa vzťahuje vykonávacie nariadenie (EÚ) 2021/664.

2. Toto nariadenie sa vzťahuje na príslušné orgány vrátane Agentúry Európskej únie pre bezpečnosť letectva (ďalej len „agentúra“) uvedené v článku 6 tohto nariadenia a v článku 5 delegovaného nariadenia Komisie (EÚ) 2022/1645 ([14]).

3. Toto nariadenie sa vzťahuje aj na príslušný orgán zodpovedný za vydávanie, zachovanie platnosti, zmenu, pozastavenie platnosti alebo zrušenie preukazov spôsobilosti technika údržby lietadiel v súlade s prílohou III (časť 66) k nariadeniu (EÚ) č. 1321/2014.

4. Týmto nariadením nie sú dotknuté požiadavky na informačnú bezpečnosť a kybernetickú bezpečnosť stanovené v bode 1.7 prílohy k vykonávaciemu nariadeniu (EÚ) 2015/1998 a v článku 14 smernice (EÚ) 2016/1148.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „informačná bezpečnosť“ je zachovanie dôvernosti, integrity, pravosti a dostupnosti sietí a informačných systémov;

2. „udalosť v oblasti informačnej bezpečnosti“ je identifikovaný výskyt stavu systému, služby alebo siete, ktorý naznačuje možné porušenie politiky informačnej bezpečnosti alebo zlyhanie kontrol informačnej bezpečnosti, alebo predtým neznámej situácie, ktorá môže byť relevantná pre informačnú bezpečnosť;

3. „incident“ je každá udalosť, ktorá má skutočný nepriaznivý vplyv na bezpečnosť sietí a informačných systémov v zmysle vymedzenia v článku 4 ods. 7 smernice (EÚ) 2016/1148;

4. „riziko v oblasti informačnej bezpečnosti“ je riziko pre organizačnú prevádzku civilného letectva, aktíva, jednotlivcov a iné organizácie z dôvodu možného výskytu udalosti v oblasti informačnej bezpečnosti. Riziká v oblasti informačnej bezpečnosti sú spojené s potenciálom, že hrozby využijú zraniteľnosti informačného aktíva alebo skupiny informačných aktív;

([14]) Delegované nariadenie Komisie (EÚ) 2022/1645 zo 14. júla 2022, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1139, pokiaľ ide o požiadavky na riadenie rizík v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva pre organizácie, na ktoré sa vzťahujú nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014, a ktorým sa mení nariadenia Komisie (EÚ) č. 748/2012 a (EÚ) č. 139/2014 (Ú. v. EÚ L 248, 26.9.2022, s. 18).

5. „hrozba“ je potenciálne porušenie informačnej bezpečnosti, ktoré existuje v prípade subjektu, okolnosti, konania alebo udalosti, ktoré by mohli spôsobiť škodu;

6. „zraniteľnosť“ je chyba alebo slabá stránka aktíva alebo systému, postupov, projektu, vykonávania alebo opatrení informačnej bezpečnosti, ktoré môžu byť zneužité a viesť k porušeniu politiky informačnej bezpečnosti.

Článok 4

Požiadavky na organizácie a príslušné orgány

1. Organizácie uvedené v článku 2 ods. 1 musia spĺňať požiadavky prílohy II (časť IS.I.OR) k tomuto nariadeniu.

2. Organizácie uvedené v článku 2 ods. 2 a 3 musia spĺňať požiadavky prílohy I (časť IS.AR) k tomuto nariadeniu.

Článok 5

Požiadavky vyplývajúce z iných právnych predpisov Únie

1. Ak organizácia uvedená v článku 2 ods. 1 spĺňa bezpečnostné požiadavky stanovené v súlade s článkom 14 smernice (EÚ) 2016/1148, ktoré sú rovnocenné s požiadavkami stanovenými v tomto nariadení, súlad s týmito bezpečnostnými požiadavkami sa považuje za súlad s požiadavkami stanovenými v tomto nariadení.

2. Ak je organizácia uvedená v článku 2 ods. 1 prevádzkovateľom alebo subjektom uvedeným vo vnútroštátnych programoch bezpečnostnej ochrany civilného letectva členských štátov stanovených v súlade s článkom 10 nariadenia Európskeho parlamentu a Rady (ES) č. 300/2008 ([15]), požiadavky kybernetickej bezpečnosti uvedené v bode 1.7 prílohy k vykonávaciemu nariadeniu (EÚ) 2015/1998 sa považujú za rovnocenné s požiadavkami stanovenými v tomto nariadení, s výnimkou ustanovenia IS.I.OR.230 prílohy II k tomuto nariadeniu, ktoré sa musí dodržiavať ako také.

3. Ak je organizácia uvedená v článku 2 ods. 1 poskytovateľom leteckých navigačných služieb Európskej prekryvnej služby geostacionárnej navigácie (EGNOS) uvedenej v nariadení (EÚ) 2021/696, bezpečnostné požiadavky uvedené v článkoch 33 až 43 hlavy V uvedeného nariadenia sa považujú za rovnocenné s požiadavkami stanovenými v tomto nariadení, s výnimkou ustanovenia IS.I.OR.230 prílohy II k tomuto nariadeniu, ktoré sa musí dodržiavať ako také.

4. Po konzultácii s agentúrou a skupinou pre spoluprácu uvedenou v článku 11 smernice (EÚ) 2016/1148 môže Komisia vydať usmernenia na posúdenie rovnocennosti požiadaviek stanovených v tomto nariadení a smernici (EÚ) 2016/1148.

Článok 6

Príslušný orgán

1. Bez toho, aby boli dotknuté úlohy zverené rade pre bezpečnostnú akreditáciu (SAB) uvedenej v článku 36 nariadenia (EÚ) 2021/696, orgánom zodpovedným za osvedčovanie súladu s týmto nariadením a dohľad nad ním je:

a) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. a), príslušný orgán určený v súlade s prílohou II (časť 145) k nariadeniu (EÚ) č. 1321/2014;

b) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. b), príslušný orgán určený v súlade s prílohou Vc (časť CAMO) k nariadeniu (EÚ) č. 1321/2014;

([15]) Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).

c) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. c), príslušný orgán určený v súlade s prílohou III (časť ORO) k nariadeniu (EÚ) č. 965/2012;

d) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. d) až f), príslušný orgán určený v súlade s prílohou VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011;

e) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. g), príslušný orgán určený v súlade s článkom 6 ods. 2 nariadenia (EÚ) 2015/340;

f) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. h), príslušný orgán určený v súlade s článkom 4 ods. 1 vykonávacieho nariadenia (EÚ) 2017/373;

g) vzhľadom na organizácie uvedené v článku 2 ods. 1 písm. i), príslušný orgán určený v súlade s článkom 14 ods. 1 alebo 2 vykonávacieho nariadenia (EÚ) 2021/664.

2. Členské štáty môžu na účely tohto nariadenia určiť nezávislý a autonómny subjekt, ktorý bude plniť pridelené úlohy a povinnosti príslušných orgánov uvedených v odseku 1. V takom prípade sa stanovia koordinačné opatrenia medzi týmto subjektom a príslušnými orgánmi podľa odseku 1 s cieľom zabezpečiť účinný dohľad nad všetkými požiadavkami, ktoré má organizácia spĺňať.

3. Agentúra spolupracuje s Agentúrou Európskej únie pre vesmírny program (EUSPA) a SAB uvedenou v článku 36 nariadenia (EÚ) 2021/696 v plnom súlade s platnými pravidlami o mlčanlivosti, ochrane osobných údajov a ochrane utajovaných skutočností s cieľom zabezpečiť účinný dohľad nad požiadavkami vzťahujúcimi sa na poskytovateľa leteckých navigačných služieb EGNOS.

Článok 7

Predkladanie relevantných informácií príslušným orgánom NIS

Príslušné orgány podľa tohto nariadenia bez zbytočného odkladu informujú jednotné kontaktné miesto určené v súlade s článkom 8 smernice (EÚ) 2016/1148 o všetkých relevantných informáciách uvedených v oznámeniach predložených podľa ustanovenia IS.I.OR.230 prílohy II k tomuto nariadeniu a ustanovenia IS.D.OR.230 prílohy I k delegovanému nariadeniu (EÚ) 2022/1645 prevádzkovateľmi základných služieb identifikovanými v súlade s článkom 5 smernice (EÚ) 2016/1148.

Článok 8

Zmena nariadenia (EÚ) č. 1178/2011

Príloha VI (časť ARA) a príloha VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011 sa menia v súlade s prílohou III k tomuto nariadeniu.

Článok 9

Zmena nariadenia (EÚ) č. 748/2012

Príloha I (časť 21) k nariadeniu (EÚ) č. 748/2012 sa mení v súlade s prílohou IV k tomuto nariadeniu.

Článok 10

Zmena nariadenia (EÚ) č. 965/2012

Príloha II (časť ARO) a príloha III (časť ORO) k nariadeniu (EÚ) č. 965/2012 sa menia v súlade s prílohou V k tomuto nariadeniu.

Článok 11

Zmena nariadenia (EÚ) č. 139/2014

Príloha II (časť ADR.AR) k nariadeniu (EÚ) č. 139/2014 sa mení v súlade s prílohou VI k tomuto nariadeniu.

Článok 12

Zmena nariadenia (EÚ) č. 1321/2014

Prílohy II (časť 145), III (časť 66) a Vc (časť CAMO) k nariadeniu (EÚ) č. 1321/2014 sa menia v súlade s prílohou VII k tomuto nariadeniu.

Článok 13

Zmena nariadenia (EÚ) 2015/340

Prílohy II (časť ATCO.AR) a III (časť ATCO.OR) k nariadeniu (EÚ) 2015/340 sa menia v súlade s prílohou VIII k tomuto nariadeniu.

Článok 14

Zmena vykonávacieho nariadenia (EÚ) 2017/373

Prílohy II (časť ATM/ANS.AR) a III (časť ATM/ANS.OR) k vykonávaciemu nariadeniu (EÚ) 2017/373 sa menia v súlade s prílohou IX k tomuto nariadeniu.

Článok 15

Zmena vykonávacieho nariadenia (EÚ) 2021/664

Vykonávacie nariadenie (EÚ) 2021/664 sa mení takto:

1. V článku 15 ods. 1 sa písmeno f) nahrádza takto:

„f) zaviedli a udržiavajú systém riadenia bezpečnostnej ochrany v súlade s ustanovením ATM/ANS.OR.D.010 v podčasti D prílohy III k vykonávaciemu nariadeniu (EÚ) 2017/373 a systém riadenia informačnej bezpečnosti v súlade s prílohou II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203;“.

2. V článku 18 sa dopĺňa toto písmeno l):

„l) zriadia, vykonávajú a udržiavajú systém riadenia informačnej bezpečnosti v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

Článok 16

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Uplatňuje sa od 22. februára 2026.

Pokiaľ však ide o prípad poskytovateľa leteckých navigačných služieb EGNOS, na ktorého sa vzťahuje vykonávacie nariadenie (EÚ) 2017/373, uplatňuje sa od 1. januára 2026.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 27. októbra 2022

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

INFORMAČNÁ BEZPEČNOSŤ – POŽIADAVKY NA ORGÁNY

[ČASŤ IS.AR]

IS.AR.100. Rozsah pôsobnosti

IS.AR.200. Systém riadenia informačnej bezpečnosti (ISMS)

IS.AR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

IS.AR.210. Riešenie rizika v oblasti informačnej bezpečnosti

IS.AR.215. Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a zotavenie

IS.AR.220. Zadávanie činností riadenia informačnej bezpečnosti

IS.AR.225. Požiadavky na personál

IS.AR.230. Vedenie záznamov

IS.AR.235. Neustále zlepšovanie

IS.AR.100. Rozsah pôsobnosti

V tejto časti sa stanovujú požiadavky riadenia, ktoré musia spĺňať príslušné orgány uvedené v článku 2 ods. 2 tohto nariadenia.

Požiadavky, ktoré musia tieto príslušné orgány spĺňať pri vykonávaní svojich činností osvedčovania, dohľadu a presadzovania predpisov, sú súčasťou nariadení uvedených v článku 2 ods. 1 tohto nariadenia a v článku 2 delegovaného nariadenia (EÚ) 2022/1645.

IS.AR.200. Systém riadenia informačnej bezpečnosti (ISMS)

a) Na dosiahnutie cieľov stanovených v článku 1 príslušný orgán zriadi, vykonáva a udržiava systém riadenia informačnej bezpečnosti (ISMS), ktorý zabezpečí, aby príslušný orgán:

1. stanovil politiku v oblasti informačnej bezpečnosti, v ktorej určí celkové zásady príslušného orgánu, pokiaľ ide o potenciálny vplyv rizík v oblasti informačnej bezpečnosti na bezpečnosť letectva;

2. identifikoval a preskúmal riziká v oblasti informačnej bezpečnosti v súlade s ustanovením IS.AR.205;

3. určil a vykonával opatrenia na riešenie rizík v oblasti informačnej bezpečnosti v súlade s ustanovením IS.AR.210;

4. vymedzil a vykonával v súlade s ustanovením IS.AR.215 opatrenia potrebné na odhaľovanie udalostí v oblasti informačnej bezpečnosti, identifikoval tie, ktoré sa považujú za incidenty s potenciálnym vplyvom na bezpečnosť letectva, a reagoval na uvedené incidenty v oblasti informačnej bezpečnosti a aby sa z uvedených incidentov zotavil;

5. spĺňal požiadavky uvedené v ustanovení IS.AR.220 pri zadávaní akejkoľvek časti činností uvedených v ustanovení IS.AR.200 iným organizáciám;

6. spĺňal požiadavky na personál uvedené v ustanovení IS.AR.225;

7. spĺňal požiadavky na vedenie záznamov uvedené v ustanovení IS.AR.230;

8. monitoroval súlad svojej vlastnej organizácie s požiadavkami tohto nariadenia a poskytoval spätnú väzbu k zisteniam osobe uvedenej v ustanovení IS.AR.225 písm. a) s cieľom zabezpečiť účinné vykonávanie nápravných opatrení;

9. chránil dôvernosť všetkých informácií, ktoré môže mať príslušný orgán v súvislosti s organizáciami, ktoré podliehajú jeho dohľadu, a informácií získaných prostredníctvom systémov externého nahlasovania organizácie zriadených v súlade s ustanovením IS.I.OR.230 prílohy II (časť IS.I.OR) k tomuto nariadeniu a ustanovením IS.D.OR.230 prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645;

10. informoval agentúru o zmenách, ktoré majú vplyv na schopnosť príslušného orgánu plniť si úlohy a plniť si povinnosti vymedzené v tomto nariadení;

11. určil a vykonával postupy na výmenu relevantných informácií podľa potreby a praktickým a včasným spôsobom s cieľom pomôcť ostatným príslušným orgánom a agentúram, ako aj organizáciám, na ktoré sa vzťahuje toto nariadenie, vykonávať účinné posúdenia bezpečnostných rizík v súvislosti s ich činnosťami.

b) V záujme nepretržitého plnenia požiadaviek uvedených v článku 1 musí príslušný orgán zaviesť postup neustáleho zlepšovania v súlade s ustanovením IS.AR.235.

c) Príslušný orgán musí dokumentovať všetky kľúčové procesy, postupy, úlohy a zodpovednosti požadované na dosiahnutie súladu s ustanovením IS.AR.200 písm. a) a zaviesť postup zmeny tejto dokumentácie.

d) Procesy, postupy, úlohy a zodpovednosti stanovené príslušným orgánom s cieľom dosiahnuť súlad s ustanovením IS.AR.200 písm. a) musia zodpovedať povahe a zložitosti jeho činností na základe posúdenia rizík v oblasti informačnej bezpečnosti, ktoré sú vlastné týmto činnostiam, a môžu byť začlenené do iných existujúcich systémov riadenia, ktoré už príslušný orgán zaviedol.

IS.AR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

a) Príslušný orgán identifikuje všetky prvky svojej vlastnej organizácie, ktoré by mohli byť vystavené rizikám v oblasti informačnej bezpečnosti. To zahŕňa:

1. činnosti, zariadenia a zdroje príslušného orgánu, ako aj služby, ktoré príslušný orgán prevádzkuje, poskytuje, prijíma alebo udržiava;

2. vybavenie, systémy, údaje a informácie, ktoré prispievajú k fungovaniu prvkov uvedených v bode 1.

b) Príslušný orgán identifikuje rozhrania, ktoré má jeho vlastná organizácia s inými organizáciami a ktoré by mohli viesť k vzájomnému vystaveniu rizikám v oblasti informačnej bezpečnosti.

c) Pokiaľ ide o prvky a rozhrania uvedené v písmenách a) a b), príslušný orgán identifikuje riziká v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.

Za každé identifikované riziko príslušný orgán:

1. priradí úroveň rizika podľa vopred určenej klasifikácie stanovenej príslušným orgánom;

2. spojí každé riziko a jeho úroveň so zodpovedajúcim prvkom alebo rozhraním určeným v súlade s písmenami a) a b).

Vo vopred určenej klasifikácii uvedenej v bode 1 sa zohľadňuje možnosť výskytu scenára ohrozenia a závažnosť jeho bezpečnostných dôsledkov. Prostredníctvom tejto klasifikácie a s prihliadnutím na to, či príslušný orgán disponuje štruktúrovaným a opakovateľným procesom riadenia rizík pre prevádzku, musí byť príslušný orgán schopný stanoviť, či je riziko prijateľné alebo či je potrebné s ním zaobchádzať v súlade s ustanovením IS.AR.210.

S cieľom uľahčiť vzájomnú porovnateľnosť posúdení rizík sa pri priraďovaní úrovne rizika podľa bodu 1 zohľadňujú príslušné informácie získané v koordinácii s organizáciami uvedenými v písmene b).

d) Príslušný orgán preskúma a aktualizuje posúdenie rizika vykonané v súlade s písmenami a), b) a c) v ktoromkoľvek z týchto prípadov:

1. došlo k zmene prvkov, ktoré sú vystavené rizikám v oblasti informačnej bezpečnosti;

2. došlo k zmene v rozhraniach medzi organizáciou príslušného orgánu a inými organizáciami alebo v rizikách oznámených inými organizáciami;

3. došlo k zmene informácií alebo poznatkov použitých na identifikáciu, analýzu a klasifikáciu rizík;

4. analýza incidentov v oblasti informačnej bezpečnosti priniesla poznatky.

IS.AR.210. Riešenie rizika v oblasti informačnej bezpečnosti

a) Príslušný orgán vypracuje opatrenia na riešenie neprijateľných rizík identifikovaných v súlade s ustanovením IS.AR.205, včas ich vykoná a skontroluje, či si zachovávajú účinnosť. Tieto opatrenia umožnia príslušnému orgánu:

1. kontrolovať okolnosti, ktoré prispievajú k skutočnému výskytu scenára ohrozenia;

2. znížiť dôsledky pre bezpečnosť letectva spojené s realizáciou scenára ohrozenia;

3. vyhýbať sa rizikám.

Týmito opatreniami sa nesmú zavádzať žiadne nové možné neprijateľné riziká pre bezpečnosť letectva.

b) Osoba uvedená v ustanovení IS.AR.225 písm. a) a iný dotknutý personál príslušného orgánu musia byť informovaní o výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.AR.205, zodpovedajúcich scenároch ohrozenia a opatreniach, ktoré sa majú vykonať.

Príslušný orgán musí informovať aj organizácie, s ktorými má rozhranie v súlade s ustanovením IS.AR.205 písm. b), o akomkoľvek spoločnom riziku pre príslušný orgán a organizáciu.

IS.AR.215. Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a zotavenie

a) Na základe výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.AR.205 a výsledku riešenia rizík vykonaného v súlade s ustanovením IS.AR.210 musí príslušný orgán zaviesť opatrenia na odhaľovanie udalostí, ktoré naznačujú možnú realizáciu neprijateľných rizík a ktoré môžu mať vplyv na bezpečnosť letectva. Uvedené opatrenia na odhaľovanie umožnia príslušnému orgánu:

1. identifikovať odchýlky od vopred stanovenej základnej funkčnej výkonnosti;

2. spúšťať upozornenia na aktiváciu vhodných reakčných opatrení v prípade akejkoľvek odchýlky.

b) Príslušný orgán musí zaviesť opatrenia s cieľom reagovať na všetky podmienky udalosti identifikované v súlade s písmenom a), ktoré sa môžu vyvinúť alebo sa vyvinuli do incidentu v oblasti informačnej bezpečnosti. Uvedené reakčné opatrenia umožnia príslušnému orgánu:

1. iniciovať reakciu jeho vlastnej organizácie na varovania uvedené v písmene a) bode 2 aktivovaním vopred stanovených zdrojov a priebehu činností;

2. obmedziť šírenie útoku a zabrániť úplnej realizácii scenára ohrozenia;

3. regulovať poruchový režim dotknutých prvkov vymedzených v ustanovení IS.AR.205 písm. a).

c) Príslušný orgán musí zaviesť opatrenia zamerané na zotavenie po incidentoch v oblasti informačnej bezpečnosti vrátane núdzových opatrení, ak je to potrebné. Uvedené opatrenia na zotavenie umožnia príslušnému orgánu:

1. odstrániť stav spôsobený incidentom, alebo ho obmedziť na prípustnú úroveň;

2. obnoviť bezpečný stav dotknutých prvkov vymedzených v ustanovení IS.AR.205 písm. a) v rámci času na zotavenie, ktorý predtým vymedzila jeho vlastná organizácia.

IS.AR.220. Zadávanie činností riadenia informačnej bezpečnosti

Príslušný orgán zabezpečí, aby pri zazmluvňovaní akejkoľvek časti činností uvedených v ustanovení IS.AR.200 s inými organizáciami boli zazmluvnené činnosti v súlade s požiadavkami tohto nariadenia a aby zazmluvnená organizácia pracovala pod jeho dohľadom. Príslušný orgán zabezpečí, aby riziká spojené so zazmluvnenými činnosťami boli primerane riadené.

IS.AR.225. Požiadavky na personál

Príslušný orgán musí:

a) mať osobu, ktorá má právomoc zriadiť a udržiavať organizačné štruktúry, politiky, procesy a postupy potrebné na vykonávanie tohto nariadenia.

Táto osoba musí:

1. mať právomoc v plnej miere pristupovať k zdrojom, ktoré príslušný orgán potrebuje na vykonávanie všetkých úloh, ktoré sa vyžadujú v tomto nariadení;

2. byť držiteľom delegovania právomoci potrebného na plnenie pridelených povinností;

b) mať zavedený postup na zabezpečenie dostatočného počtu zamestnancov v službe na vykonávanie činností, na ktoré sa vzťahuje táto príloha;

c) mať zavedený postup na zabezpečenie toho, aby zamestnanci uvedení v písmene b) mali potrebnú spôsobilosť na plnenie svojich úloh;

d) mať zavedený postup na zabezpečenie toho, aby zamestnanci uznali povinnosti spojené s pridelenými rolami a úlohami;

e) zabezpečiť, aby bola náležite stanovená totožnosť a dôveryhodnosť pracovníkov, ktorí majú prístup k informačným systémom a údajom, na ktoré sa vzťahujú požiadavky tohto nariadenia.

IS.AR.230. Vedenie záznamov

a) Príslušný orgán vedie záznamy o svojich činnostiach riadenia informačnej bezpečnosti.

1. Príslušný orgán zabezpečí archiváciu a vysledovateľnosť týchto záznamov:

i) zmluvy o činnostiach uvedených v ustanovení IS.AR.200 písm. a) bode 5;

ii) záznamy o kľúčových procesoch uvedených v ustanovení IS.AR.200 písm. d);

iii) záznamy o rizikách identifikovaných v posúdení rizika uvedenom v ustanovení IS.AR.205 spolu so súvisiacimi opatreniami na riešenie rizík uvedenými v ustanovení IS.AR.210;

iv) záznamy o udalostiach v oblasti informačnej bezpečnosti, ktoré možno bude potrebné prehodnotiť, aby sa odhalili nezistené incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti.

2. Záznamy uvedené v bode 1 podbode i) sa uchovávajú aspoň 5 rokov po zmene alebo vypovedaní zmluvy.

3. Záznamy uvedené v bode 1 podbode ii) a iii) sa uchovávajú najmenej 5 rokov.

4. Záznamy uvedené v bode 1 podbode iv) sa uchovávajú dovtedy, kým sa uvedené udalosti v oblasti informačnej bezpečnosti opätovne neposúdia v súlade s periodicitou vymedzenou v postupe stanovenom príslušným orgánom.

b) Príslušný orgán vedie záznamy o kvalifikácii a skúsenostiach svojich vlastných zamestnancov zapojených do činností riadenia informačnej bezpečnosti.

1. Záznamy o kvalifikácii a skúsenostiach zamestnancov sa uchovávajú, pokiaľ daná osoba pracuje pre príslušný orgán, a najmenej 3 roky po tom, čo osoba opustila príslušný orgán.

2. Zamestnancom sa na ich žiadosť poskytne prístup k ich individuálnym záznamom. Okrem toho im príslušný orgán na ich žiadosť poskytne kópiu individuálnych záznamov pri odchode z príslušného orgánu.

c) Formát týchto záznamov sa stanoví v postupoch príslušného orgánu.

d) Záznamy sa uchovávajú spôsobom, ktorým sa zabezpečí ochrana pred poškodením, pozmeňovaním a krádežou, pričom informácie sa v prípade potreby identifikujú na základe ich stupňa utajenia.information being identified, when required, according to its security classification level. Príslušný orgán zabezpečí, aby sa záznamy uchovávali s použitím prostriedkov na zabezpečenie integrity, pravosti a oprávneného prístupu.

IS.AR.235. Neustále zlepšovanie

a) Príslušný orgán s použitím primeraných ukazovateľov výkonnosti posúdi účinnosť a vyspelosť svojho vlastného ISMS. Toto posúdenie sa vykonáva na základe vopred určeného harmonogramu, ktorý stanoví príslušný orgán, alebo v nadväznosti na incident v oblasti informačnej bezpečnosti.

b) Ak sa po posúdení vykonanom v súlade s písmenom a) zistia nedostatky, príslušný orgán prijme potrebné opatrenia na zlepšenie s cieľom zabezpečiť, aby ISMS naďalej spĺňal príslušné požiadavky a udržiaval riziká v oblasti informačnej bezpečnosti na prijateľnej úrovni. Okrem toho príslušný orgán opätovne posúdi tie prvky ISMS, ktorých sa týkajú prijaté opatrenia.

PRÍLOHA II

INFORMAČNÁ BEZPEČNOSŤ – ORGANIZAČNÉ POŽIADAVKY

[ČASŤ IS.I.OR]

IS.I.OR.100. Rozsah pôsobnosti

IS.I.OR.200. Systém riadenia informačnej bezpečnosti (ISMS)

IS.I.OR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

IS.I.OR.210. Riešenie rizika v oblasti informačnej bezpečnosti

IS.I.OR.215. Systém interného nahlasovania informačnej bezpečnosti

IS.I.OR.220. Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a obnova

IS.I.OR.225. Reakcia na zistenia oznámené príslušným orgánom

IS.I.OR.230. Systém externého nahlasovania informačnej bezpečnosti

IS.I.OR.235. Zadávanie činností riadenia informačnej bezpečnosti

IS.I.OR.240. Požiadavky na personál

IS.I.OR.245. Vedenie záznamov

IS.I.OR.250. Príručka riadenia informačnej bezpečnosti (ISMM)

IS.I.OR.255. Zmeny systému riadenia informačnej bezpečnosti

IS.I.OR.260. Neustále zlepšovanie

IS.I.OR.100. Rozsah pôsobnosti

V tejto časti sa stanovujú požiadavky, ktoré musia spĺňať organizácie uvedené v článku 2 ods. 1 tohto nariadenia.

IS.I.OR.200. Systém riadenia informačnej bezpečnosti (ISMS)

a) Na dosiahnutie cieľov stanovených v článku 1 organizácia zriadi, vykonáva a udržiava systém riadenia informačnej bezpečnosti (ISMS), ktorý zabezpečí, aby organizácia:

   1. stanovila politiku v oblasti informačnej bezpečnosti, v ktorej určí celkové zásady organizácie, pokiaľ ide o potenciálny vplyv rizík v oblasti informačnej bezpečnosti na bezpečnosť letectva;
   2. identifikovala a preskúmala riziká v oblasti informačnej bezpečnosti v súlade s ustanovením IS.I.OR.205;
   3. určila a vykonávala opatrenia na riešenie rizík v oblasti informačnej bezpečnosti v súlade s ustanovením IS.I.OR.210;
   4. zaviedla systém interného nahlasovania informačnej bezpečnosti v súlade s ustanovením IS.I.OR.215;
   5. vymedzila a vykonávala v súlade s ustanovením IS.I.OR.220 opatrenia potrebné na odhaľovanie udalostí v oblasti informačnej bezpečnosti, identifikovala tie udalosti, ktoré sa považujú za incidenty s potenciálnym vplyvom na bezpečnosť letectva, s výnimkou prípadov povolených v ustanovení IS.I.OR.205 písm. e), a reagovala na uvedené incidenty v oblasti informačnej bezpečnosti a aby sa z uvedených incidentov zotavila;

6. vykonávala opatrenia, ktoré oznámil príslušný orgán ako okamžitú reakciu na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva;

7. prijímala vhodné opatrenia v súlade s ustanovením IS.I.OR.225 s cieľom riešiť zistenia oznámené príslušným orgánom;

8. vykonávala systém externého nahlasovania v súlade s ustanovením IS.I.OR.230 s cieľom umožniť príslušnému orgánu prijať vhodné opatrenia;

9. spĺňala požiadavky uvedené v ustanovení IS.I.OR.235 pri zadávaní akejkoľvek časti činností uvedených v ustanovení IS.I.OR.200 iným organizáciám;

10. spĺňala požiadavky na personál určené v ustanovení IS.I.OR.240;

11. spĺňala požiadavky na vedenie záznamov určené v ustanovení IS.I.OR.245;

12. monitorovala súlad organizácie s požiadavkami tohto nariadenia a poskytovala zodpovednému manažérovi spätnú väzbu o zisteniach s cieľom zabezpečiť účinné vykonávanie nápravných opatrení;

13. bez toho, aby boli dotknuté príslušné požiadavky na nahlasovanie incidentov, chránila dôvernosť všetkých informácií, ktoré organizácia mohla získať od iných organizácií, podľa úrovne ich citlivosti.

b) V záujme nepretržitého plnenia požiadaviek uvedených v článku 1 musí organizácia zaviesť postup neustáleho zlepšovania v súlade s ustanovením IS.I.OR.260.

c) Organizácia musí v súlade s ustanovením IS.I.OR.250 dokumentovať všetky kľúčové procesy, postupy, úlohy a zodpovednosti požadované na dosiahnutie súladu s ustanovením IS.I.OR.200 písm. a) a zaviesť postup zmeny tejto dokumentácie. Zmeny týchto procesov, postupov, úloh a zodpovedností sa riadia v súlade s ustanovením IS.I.OR.255.

d) Procesy, postupy, úlohy a zodpovednosti stanovené organizáciou s cieľom dosiahnuť súlad s ustanovením IS.I.OR.200 písm. a) musia zodpovedať povahe a zložitosti jej činností na základe posúdenia rizík v oblasti informačnej bezpečnosti, ktoré sú vlastné týmto činnostiam, a môžu byť začlenené do iných existujúcich systémov riadenia, ktoré už organizácia zaviedla.

e) Bez toho, aby bola dotknutá povinnosť dodržiavať požiadavky na podávanie správ stanovené v nariadení (EÚ) č. 376/2014 a požiadavky stanovené v ustanovení IS.I.OR.200 písm. a) bode 13, môže príslušný orgán dať organizácii súhlas s nevykonávaním požiadaviek uvedených v písmenách a) až d) a príslušných požiadaviek uvedených v ustanoveniach IS.I.OR.205 až IS.I.OR.260, ak preukáže k spokojnosti uvedeného orgánu, že jej činnosti, zariadenia a zdroje, ako aj služby, ktoré prevádzkuje, poskytuje, prijíma a udržiava, nepredstavujú žiadne riziká v oblasti informačnej bezpečnosti s potenciálnym vplyvom na bezpečnosť letectva, a to ani pre seba, ani pre iné organizácie. Tento súhlas musí vychádzať zo zdokumentovaného posúdenia rizika v oblasti informačnej bezpečnosti, ktoré organizácia alebo tretia strana vykoná v súlade s ustanovením IS.I.OR.205 a ktoré preskúma a schváli jej príslušný orgán.

Zachovanie platnosti tohto súhlasu preskúma príslušný orgán na základe príslušného cyklu auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.

IS.I.OR.205. Posúdenie rizika v oblasti informačnej bezpečnosti

a) Organizácia identifikuje všetky svoje prvky, ktoré by mohli byť vystavené rizikám v oblasti informačnej bezpečnosti. To zahŕňa:

1. činnosti, zariadenia a zdroje organizácie, ako aj služby, ktoré organizácia prevádzkuje, poskytuje, prijíma alebo udržiava;

2. vybavenie, systémy, údaje a informácie, ktoré prispievajú k fungovaniu prvkov uvedených v bode 1.

b) Organizácia identifikuje rozhrania, ktoré má s inými organizáciami a ktoré by mohli viesť k vzájomnému vystaveniu rizikám v oblasti informačnej bezpečnosti.

c) Pokiaľ ide o prvky a rozhrania uvedené v písmenách a) a b), organizácia identifikuje riziká v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva. Za každé identifikované riziko organizácia:

1. priradí úroveň rizika podľa vopred určenej klasifikácie stanovenej organizáciou;

2. spojí každé riziko a jeho úroveň so zodpovedajúcim prvkom alebo rozhraním určeným v súlade s písmenami a) a b).

Vo vopred určenej klasifikácii uvedenej v bode 1 sa zohľadňuje možnosť výskytu scenára ohrozenia a závažnosť jeho bezpečnostných dôsledkov. Na základe tejto klasifikácie a s prihliadnutím na to, či organizácia disponuje štruktúrovaným a opakovateľným procesom riadenia rizík pre prevádzku, musí byť organizácia schopná stanoviť, či je riziko prijateľné alebo či je potrebné s ním zaobchádzať v súlade s ustanovením IS.I.OR.210.

S cieľom uľahčiť vzájomnú porovnateľnosť posúdení rizík sa pri priraďovaní úrovne rizika podľa bodu 1 zohľadňujú príslušné informácie získané v koordinácii s organizáciami uvedenými v písmene b).

d) Organizácia preskúma a aktualizuje posúdenie rizika vykonané v súlade s písmenami a), b) a prípadne c) alebo e) v ktorejkoľvek z týchto situácií:

1. došlo k zmene prvkov, ktoré sú vystavené rizikám v oblasti informačnej bezpečnosti;

2. došlo k zmene v rozhraniach medzi organizáciou a inými organizáciami alebo v rizikách oznámených inými organizáciami;

3. došlo k zmene informácií alebo poznatkov použitých na identifikáciu, analýzu a klasifikáciu rizík;

4. analýza incidentov v oblasti informačnej bezpečnosti priniesla poznatky.

e) Odchylne od písmena c) organizácie, od ktorých sa vyžaduje súlad s podčasťou C prílohy III (časť ATM/ANS.OR) k vykonávaciemu nariadeniu (EÚ) 2017/373, nahradia analýzu vplyvu na bezpečnosť letectva analýzou vplyvu na svoje služby v zmysle podporného posúdenia bezpečnosti požadovaného v ustanovení ATM/ANS.OR.C.005. Toto podporné posúdenie bezpečnosti sa sprístupní poskytovateľom letových prevádzkových služieb, ktorým poskytujú služby, a títo poskytovatelia letových prevádzkových služieb sú zodpovední za hodnotenie vplyvu na bezpečnosť letectva.

IS.I.OR.210. Riešenie rizika v oblasti informačnej bezpečnosti

a) Organizácia vypracuje opatrenia na riešenie neprijateľných rizík identifikovaných v súlade s ustanovením IS.I.OR.205, včas ich vykoná a skontroluje, či si zachovávajú účinnosť. Tieto opatrenia umožnia organizácii:

1. kontrolovať okolnosti, ktoré prispievajú k skutočnému výskytu scenára ohrozenia;

2. znížiť dôsledky na bezpečnosť letectva spojené s realizáciou scenára ohrozenia;

3. vyhýbať sa rizikám.

Týmito opatreniami sa nesmú zavádzať žiadne nové možné neprijateľné riziká pre bezpečnosť letectva.

b) Osoba uvedená v ustanovení IS.I.OR.240 písm. a) a b) a iný dotknutý personál organizácie musia byť informovaní o výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.I.OR.205, zodpovedajúcich scenároch ohrozenia a opatreniach, ktoré sa majú vykonať.

Organizácia musí informovať aj organizácie, s ktorými má rozhranie v súlade s ustanovením IS.I.OR.205 písm. b), o akomkoľvek spoločnom riziku pre obe organizácie.

IS.I.OR.215. Systém interného nahlasovania informačnej bezpečnosti

a) Organizácia zriadi systém interného nahlasovania s cieľom umožniť zhromažďovanie a hodnotenie udalostí v oblasti informačnej bezpečnosti vrátane udalostí, ktoré sa majú nahlasovať podľa ustanovenia IS.I.OR.230.

b) Systém a proces uvedený v ustanovení IS.I.OR.220 musia umožniť organizácii:

1. identifikovať, ktoré z udalostí nahlásených podľa písmena a) sa považujú za incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva;

2. identifikovať príčiny a faktory prispievajúce k incidentom a zraniteľnostiam v oblasti informačnej bezpečnosti identifikovaným v súlade s bodom 1 a riešiť ich ako súčasť procesu riadenia rizík v oblasti informačnej bezpečnosti v súlade s ustanoveniami IS.I.OR.205 a IS.I.OR.220;

3. zabezpečiť hodnotenie všetkých známych relevantných informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti identifikovaných v súlade s bodom 1;

4. zabezpečiť zavedenie metódy interného šírenia informácií podľa potreby.

c) Každá zazmluvnená organizácia, ktorá môže vystaviť organizáciu rizikám v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, je povinná nahlásiť organizácii udalosti v oblasti informačnej bezpečnosti. Uvedené správy sa predkladajú s použitím postupov stanovených v osobitných zmluvných dojednaniach a vyhodnocujú sa v súlade s písmenom b).

d) Organizácia spolupracuje pri vyšetrovaniach s akoukoľvek inou organizáciou, ktorá významne prispieva k informačnej bezpečnosti svojich vlastných činností.

e) Organizácia môže zlúčiť tento systém nahlasovania s inými systémami nahlasovania, ktoré už zaviedla.

IS.I.OR.220 Incidenty v oblasti informačnej bezpečnosti – odhaľovanie, reakcia a zotavenie

a) Na základe výsledku posúdenia rizika vykonaného v súlade s ustanovením IS.I.OR.205 a výsledku riešenia rizík vykonaného v súlade s ustanovením IS.I.OR.210 musí organizácia zaviesť opatrenia na odhaľovanie incidentov a zraniteľností, ktoré naznačujú možnú realizáciu neprijateľných rizík a ktoré môžu mať vplyv na bezpečnosť letectva. Uvedené opatrenia na odhaľovanie umožnia organizácii:

1. identifikovať odchýlky od vopred stanovenej základnej funkčnej výkonnosti;

2. spúšťať upozornenia na aktiváciu vhodných reakčných opatrení v prípade akejkoľvek odchýlky.

b) Organizácia musí zaviesť opatrenia s cieľom reagovať na všetky podmienky udalosti identifikované v súlade s písmenom a), ktoré sa môžu vyvinúť alebo sa vyvinuli do incidentu v oblasti informačnej bezpečnosti. Uvedené opatrenia reakcie umožnia organizácii:

1. iniciovať reakciu na varovania uvedené v písmene a) bode 2 aktivovaním vopred stanovených zdrojov a priebehu činností;

2. obmedziť šírenie útoku a zabrániť úplnej realizácii scenára ohrozenia;

3. regulovať poruchový režim dotknutých prvkov vymedzených v ustanovení IS.I.OR.205 písm. a).

c) Organizácia musí zaviesť opatrenia zamerané na obnovu po incidentoch v oblasti informačnej bezpečnosti vrátane núdzových opatrení, ak je to potrebné. Uvedené opatrenia na obnovu umožnia organizácii:

1. odstrániť stav spôsobený incidentom, alebo ho obmedziť na prípustnú úroveň;

2. dosiahnuť bezpečný stav dotknutých prvkov vymedzených v ustanovení IS.I.OR.205 písm. a) v rámci času na zotavenie, ktorý predtým vymedzila organizácia.

IS.I.OR.225. Reakcia na zistenia oznámené príslušným orgánom

a) Po prijatí oznámenia o zisteniach, ktoré predložil príslušný orgán, musí organizácia:

1. určiť hlavnú príčinu alebo príčiny nesúladu a faktory prispievajúce k nesúladu;

2. stanoviť plán nápravných opatrení;

3. preukázať nápravu nesúladu k spokojnosti príslušného orgánu.

b) Opatrenia uvedené v písmene a) sa vykonajú v lehote dohodnutej s príslušným orgánom.

IS.I.OR.230. Systém externého nahlasovania informačnej bezpečnosti

a) Organizácia musí zaviesť systém nahlasovania informačnej bezpečnosti, ktorý je v súlade s požiadavkami stanovenými v nariadení (EÚ) č. 376/2014 a jeho delegovaných a vykonávacích aktoch, ak sa uvedené nariadenie vzťahuje na organizáciu.

b) Bez toho, aby boli dotknuté povinnosti stanovené v nariadení (EÚ) č. 376/2014, organizácia zabezpečí, aby sa akýkoľvek incident alebo zraniteľnosť v oblasti informačnej bezpečnosti, ktoré môžu predstavovať závažné riziko pre bezpečnosť letectva, nahlásil jej príslušnému orgánu. Okrem toho:

1. ak takýto incident alebo zraniteľnosť ovplyvňuje lietadlo alebo súvisiaci systém či komponent, organizácia to musí nahlásiť aj držiteľovi schválenia projektu;

2. ak takýto incident alebo zraniteľnosť ovplyvňuje systém alebo komponent používaný organizáciou, organizácia to nahlási organizácii zodpovednej za projekt systému alebo komponentu.

c) Organizácia nahlasuje podmienky uvedené v písmene b) takto:

1. oznámenie sa predloží príslušnému orgánu a v prípade potreby držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu hneď, ako sa organizácia dozvie o týchto podmienkach;

2. správa sa predloží príslušnému orgánu a prípadne držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu, a to čo najskôr, najneskôr však do 72 hodín od momentu, keď sa organizácia dozvedela o podmienkach, pokiaľ tomu nebránia výnimočné okolnosti.

   Správa sa vypracuje v podobe určenej príslušným orgánom a obsahuje všetky relevantné informácie o podmienkach, ktoré sú organizácii známe;

3. príslušnému orgánu a prípadne držiteľovi schválenia projektu alebo organizácii zodpovednej za projekt systému alebo komponentu sa predloží kontrolná správa, v ktorej sa uvedú podrobnosti o opatreniach, ktoré organizácia prijala alebo plánuje prijať na zotavenie sa z incidentu, a opatrenia, ktoré má v úmysle prijať na zabránenie podobným incidentom v oblasti informačnej bezpečnosti v budúcnosti.

   Kontrolná správa sa predloží ihneď po určení týchto opatrení a vypracuje sa v podobe, ktorú určí príslušný orgán.

IS.I.OR.235. Zadávanie činností riadenia informačnej bezpečnosti

a) Organizácia zabezpečí, aby pri zazmluvňovaní akejkoľvek časti činností uvedených v ustanovení IS.I.OR.200 s inými organizáciami boli zazmluvnené činnosti v súlade s požiadavkami tohto nariadenia a aby zazmluvnená organizácia pracovala pod jej dohľadom. Organizácia zabezpečí, aby riziká spojené so zazmluvnenými činnosťami boli primerane riadené.

b) Organizácia zabezpečí príslušnému orgánu na jeho žiadosť prístup k zazmluvnenej organizácii s cieľom určiť, či naďalej spĺňa príslušné požiadavky stanovené v tomto nariadení.

IS.I.OR.240. Požiadavky na personál

a) Zodpovedný manažér organizácie určený v súlade s nariadeniami (EÚ) č. 1321/2014, (EÚ) č. 965/2012, (EÚ) č. 1178/2011, (EÚ) 2015/340, vykonávacím nariadením (EÚ) 2017/373 alebo vykonávacím nariadením (EÚ) 2021/664, ako sa uvádza v článku 2 ods. 1 tohto nariadenia, má podnikovú právomoc zabezpečiť, aby všetky činnosti požadované v tomto nariadení mohli byť financované a vykonávané. Táto osoba:

1. zabezpečuje, aby boli k dispozícii všetky potrebné zdroje na splnenie požiadaviek tohto nariadenia;

2. stanovuje a presadzuje politiku informačnej bezpečnosti uvedenú v ustanovení IS.I.OR.200 písm. a) bode 1;

3. preukáže základné znalosti o tomto nariadení.

b) Zodpovedný manažér vymenuje osobu alebo skupinu osôb, aby sa zabezpečilo, že organizácia spĺňa požiadavky tohto nariadenia, a vymedzí rozsah ich právomocí. Uvedená osoba alebo skupina osôb podlieha priamo zodpovednému manažérovi a musí mať primerané znalosti, prax a skúsenosti na plnenie svojich povinností. V postupoch sa určí, kto zastupuje určitú osobu v prípade dlhodobej neprítomnosti uvedenej osoby.

c) Zodpovedný manažér vymenuje osobu alebo skupinu osôb, ktoré budú zodpovedné za riadenie funkcie monitorovania súladu podľa ustanovenia IS.I.OR.200 písm. a) bodu 12.

d) Ak organizácia zdieľa organizačné štruktúry, politiky, procesy a postupy v oblasti informačnej bezpečnosti s inými organizáciami alebo oblasťami svojej vlastnej organizácie, ktoré nie sú súčasťou schválenia alebo vyhlásenia, zodpovedný manažér môže delegovať svoje činnosti na spoločnú zodpovednú osobu.

V takom prípade sa stanovia koordinačné opatrenia medzi zodpovedným manažérom organizácie a spoločnou zodpovednou osobou s cieľom zabezpečiť primeranú integráciu riadenia informačnej bezpečnosti v rámci organizácie.

e) Zodpovedný manažér alebo spoločná zodpovedná osoba uvedená v písmene d) majú podnikovú právomoc zriadiť a udržiavať organizačné štruktúry, politiky, procesy a postupy potrebné na vykonávanie ustanovenia IS.I.OR.200.

f) Organizácia musí mať zavedený postup na zabezpečenie dostatočného počtu zamestnancov v službe na vykonávanie činností, na ktoré sa vzťahuje táto príloha.

g) Organizácia musí mať zavedený postup na zabezpečenie toho, aby zamestnanci uvedení v písmene f) mali potrebnú spôsobilosť na plnenie svojich úloh.

h) Organizácia musí mať zavedený postup na zabezpečenie toho, aby zamestnanci uznali povinnosti spojené s pridelenými rolami a úlohami.

i) Organizácia zabezpečí, aby bola náležite stanovená totožnosť a dôveryhodnosť pracovníkov, ktorí majú prístup k informačným systémom a údajom, na ktoré sa vzťahujú požiadavky tohto nariadenia.

IS.I.OR.245. Vedenie záznamov

a) *Organizácia vedie záznamy o svojich činnostiach riadenia informačnej bezpečnosti.*

1. Organizácia zabezpečí archiváciu a vysledovateľnosť týchto záznamov:

i) každé prijaté schválenie a akékoľvek súvisiace posúdenie rizika v oblasti informačnej bezpečnosti v súlade s ustanovením IS.I.OR.200 písm. e);

ii) zmluvy o činnostiach uvedených v ustanovení IS.I.OR.200 písm. a) bode 9;

iii) záznamy o kľúčových procesoch uvedených v ustanovení IS.I.OR.200 písm. d);

iv) záznamy o rizikách identifikovaných v posúdení rizika uvedenom v ustanovení IS.I.OR.205 spolu so súvisiacimi opatreniami na riešenie rizík uvedenými v ustanovení IS.I.OR.210;

v) záznamy o incidentoch a zraniteľnostiach v oblasti informačnej bezpečnosti nahlásených v súlade so systémami nahlasovania uvedenými v ustanoveniach IS.I.OR.215 a IS.I.OR.230;

vi) záznamy o tých udalostiach v oblasti informačnej bezpečnosti, ktoré možno bude potrebné prehodnotiť, aby sa odhalili nezistené incidenty alebo zraniteľnosti v oblasti informačnej bezpečnosti.

2. Záznamy uvedené v bode 1 podbode i) sa uchovávajú aspoň 5 rokov po uplynutí platnosti schválenia.

3. Záznamy uvedené v bode 1 podbode ii) sa uchovávajú aspoň 5 rokov po zmene alebo vypovedaní zmluvy.

4. Záznamy uvedené v bode 1 podbode iii), iv) a v) sa uchovávajú najmenej 5 rokov.

5. Záznamy uvedené v bode 1 podbode vi) sa uchovávajú dovtedy, kým sa uvedené udalosti v oblasti informačnej bezpečnosti opätovne neposúdia v súlade s periodicitou vymedzenou v postupe stanovenom organizáciou.

b) *Organizácia vedie záznamy o kvalifikácii a skúsenostiach svojich vlastných zamestnancov zapojených do činností riadenia informačnej bezpečnosti.*

1. Záznamy o kvalifikácii a skúsenostiach zamestnancov sa uchovávajú, pokiaľ daná osoba pracuje pre organizáciu, a najmenej 3 roky po tom, čo osoba opustila organizáciu.

2. Zamestnancom sa na ich žiadosť poskytne prístup k ich individuálnym záznamom. Okrem toho im organizácia na ich žiadosť poskytne kópiu individuálnych záznamov pri odchode z organizácie.

c) Formát týchto záznamov sa stanoví v postupoch organizácie.

d) Záznamy sa uchovávajú spôsobom, ktorým sa zabezpečí ochrana pred poškodením, pozmeňovaním a krádežou, pričom informácie sa v prípade potreby identifikujú na základe ich stupňa utajenia.information being identified, when required, according to its security classification level. Organizácia zabezpečí, aby sa záznamy uchovávali s použitím prostriedkov na zabezpečenie integrity, pravosti a oprávneného prístupu.

IS.I.OR.250. Príručka riadenia informačnej bezpečnosti (ISMM)

a) Organizácia sprístupní príslušnému orgánu príručku riadenia informačnej bezpečnosti (ISMM) a prípadne všetky súvisiace príručky a postupy, na ktoré sa odkazuje, obsahujúcu:

1. vyhlásenie podpísané zodpovedným manažérom, ktorým sa potvrdzuje, že organizácia bude vždy pracovať v súlade s touto prílohou a ISMM. Ak zodpovedný manažér nie je výkonným riaditeľom organizácie, vyhlásenie podpíše výkonný riaditeľ;

2. titul(-y), meno(-á), úlohy, zodpovednosť, povinnosti a právomoci osoby alebo osôb určených v ustanovení IS.I.OR.240 písm. b) a c);

3. prípadne titul, meno, úlohy, zodpovednosť, povinnosti a právomoci spoločnej zodpovednej osoby určenej v ustanovení IS.I.OR.240 písm. d);

4. politiku informačnej bezpečnosti organizácie, ako sa uvádza v ustanovení IS.I.OR.200 písm. a) bode 1;

5. všeobecný opis počtu a kategórie zamestnancov a zavedeného systému na plánovanie dostupnosti personálu, ako sa vyžaduje v ustanovení IS.I.OR.240;

6. titul(-y), meno(-á), úlohy, zodpovednosť, povinnosti a právomoci kľúčových osôb zodpovedných za vykonávanie ustanovenia IS.I.OR.200 vrátane osoby alebo osôb zodpovedných za funkciu monitorovania súladu uvedenú v ustanovení IS.I.OR.200 písm. a) bode 12;

7. organizačnú schému znázorňujúcu súvisiace reťazce zodpovednosti a povinností osôb uvedených v bodoch 2 a 6;

8. opis schémy interného nahlasovania uvedenej v ustanovení IS.I.OR.215;

9. postupy, ktoré špecifikujú, ako organizácia zabezpečuje súlad s touto časťou, a najmä:

i) dokumentáciu uvedenú v ustanovení IS.I.OR.200 písm. c);

ii) postupy, ktorými sa vymedzuje, ako organizácia kontroluje akékoľvek zazmluvnené činnosti uvedené v ustanovení IS.I.OR.200 písm. a) bode 9;

iii) postup zmeny ISMM uvedený v písmene c);

10. podrobné údaje o v súčasnosti schválenom náhradnom spôsobe dosiahnutia súladu.

b) Prvé vydanie ISMM schvaľuje a jej kópiu si ponechá príslušný orgán. ISMM sa podľa potreby zmení tak, aby bola naďalej aktuálnym opisom ISMS organizácie. Príslušnému orgánu sa poskytne kópia všetkých zmien ISMM.

c) Zmeny ISMM sa riadia postupom, ktorý stanovuje organizácia. Všetky zmeny, ktoré nepatria do rozsahu pôsobnosti tohto postupu, a akékoľvek zmeny týkajúce sa zmien uvedených v ustanovení IS.I.OR.255 písm. b) schvaľuje príslušný orgán.

d) Organizácia môže zlúčiť ISMM s inými príručkami riadenia alebo manuálmi, ktorých je držiteľom, za predpokladu, že uvedie jasný odkaz označujúci časti príručky riadenia alebo manuálu, ktoré zodpovedajú rôznym požiadavkám obsiahnutým v tejto prílohe.

IS.I.OR.255. Zmeny systému riadenia informačnej bezpečnosti

a) Zmeny ISMS sa môžu riadiť a oznamovať príslušnému orgánu v rámci postupu, ktorý vypracuje organizácia. Tento postup musí schváliť príslušný orgán.

b) Pokiaľ ide o zmeny ISMS, na ktoré sa nevzťahuje postup uvedený v písmene a), organizácia musí požiadať o schválenie vydané príslušným orgánom a získať ho.

Pokiaľ ide o tieto zmeny:

1. žiadosť musí podať skôr, než uskutoční akúkoľvek takúto zmenu, aby sa príslušnému orgánu umožnilo stanoviť, či sa zachováva súlad s týmto nariadením, a v prípade potreby zmeniť osvedčenie organizácie a súvisiace podmienky schválenia, ktoré sú jeho prílohou;

2. organizácia musí sprístupniť príslušnému orgánu všetky informácie, ktoré si vyžiada na posúdenie zmeny;

3. zmena sa vykoná až po získaní formálneho schválenia od príslušného orgánu;

4. organizácia musí počas vykonávania takýchto zmien fungovať za podmienok predpísaných príslušným orgánom.

IS.I.OR.260. Neustále zlepšovanie

a) Organizácia s použitím primeraných ukazovateľov výkonnosti posúdi účinnosť a vyspelosť ISMS. Toto posúdenie sa vykonáva na základe harmonogramu, ktorý vopred stanoví organizácia, alebo v nadväznosti na incident v oblasti informačnej bezpečnosti.

b) Ak sa po posúdení vykonanom v súlade s písmenom a) zistia nedostatky, organizácia prijme potrebné opatrenia na zlepšenie s cieľom zabezpečiť, aby ISMS naďalej spĺňal príslušné požiadavky a udržiaval riziká v oblasti informačnej bezpečnosti na prijateľnej úrovni. Okrem toho organizácia opätovne posúdi tie prvky ISMS, ktorých sa týkajú prijaté opatrenia.

PRÍLOHA III

Prílohy VI (časť ARA) a VII (časť ORA) k nariadeniu (EÚ) č. 1178/2011 sa menia takto:

1. Príloha VI (časť ARA) sa mení takto:

a) V ustanovení ARA.GEN.125 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

b) Za ustanovenie ARA.GEN.135 sa vkladá toto ustanovenie ARA.GEN.135A:

„**ARA.GEN.135A Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením ARA.GEN.125 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

c) V ustanovení ARA.GEN.200 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

d) Ustanovenie ARA.GEN.205 sa mení takto:

i) Nadpis sa nahrádza takto:

„**ARA.GEN.205 Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením ORA.GEN.200A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením ARA.GEN.200 písm. e) zahŕňal všetky úlohy osvedčovania a zachovávania dohľadu vykonávané v jeho mene.“

e) V ustanovení ARA.GEN.300 sa dopĺňa toto písmeno g):

„g) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením ORA.GEN.200A, príslušný orgán okrem súladu s písmenami a) až f) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“;

f) Za ustanovenie ARA.GEN.330 sa vkladá toto ustanovenie ARA.GEN.330A:

„**ARA.GEN.330A Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho zachovávania dohľadu v súlade so zásadami stanovenými v ustanovení ARA.GEN.300. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením ARA.GEN.350.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

2. Príloha VII (časť ORA) sa mení takto:

Za ustanovenie ORA.GEN.200 sa vkladá toto ustanovenie ORA.GEN.200A:

„**ORA.GEN.200A Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení ORA.GEN.200 musí organizácia zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

PRÍLOHA IV

Príloha I (časť 21) k nariadeniu (EÚ) č. 748/2012 sa mení takto:

1. Obsah sa mení takto:

   a) Za nadpis 21.B.20 sa vkladá tento nadpis:

   „21.B.20A. Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva“.

   b) Nadpis ustanovenia 21.B.30 sa nahrádza takto:

   „21.B.30. Prideľovanie úloh“;

   c) Za nadpis 21.B.240 sa vkladá tento nadpis:

   „21.B.240A. Zmeny systému riadenia informačnej bezpečnosti“;

   d) Za nadpis 21.B.435 sa vkladá tento nadpis:

   „21.B.435A. Zmeny systému riadenia informačnej bezpečnosti“.

2. V ustanovení 21.B.15 sa dopĺňa toto písmeno c):

   „c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.D.OR.230 prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645.“

3. Za ustanovenie 21.B.20 sa vkladá toto ustanovenie 21.B.20A:

„**21.B.20A. Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením 21.B.15 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

4. V ustanovení 21.B.25 sa dopĺňa toto písmeno e):

   „e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia zavedený a udržiavaný príslušným orgánom v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

5. Ustanovenie 21.B.30 sa mení takto:

a) Nadpis sa nahrádza takto:

„**21.B.30. Prideľovanie úloh“;**

b) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanoveniami 21.A.139A a 21.A.239A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením 21.B.25 písm. e) zahŕňal všetky úlohy osvedčovania a zachovania dohľadu vykonávané v jeho mene.“

6. V ustanovení 21.B.221 sa dopĺňa toto písmeno g):

„g) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením 21.A.139A, príslušný orgán okrem súladu s písmenami a) až f) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

7. Za ustanovenie 21.B.240 sa vkladá toto ustanovenie 21.B.240A:

„**21.B.240A. Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.D.OR.255 písm. a) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení 21.B.221. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením 21.B.225.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.D.OR.255 písm. b) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

8. V ustanovení 21.B.431 sa dopĺňa toto písmeno d):

„d) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením 21.A.239A, okrem súladu s písmenami a) až c) musí príslušný orgán dodržiavať tieto zásady:

1. príslušný orgán preskúma rozhrania a súvisiace riziká, ktoré v súlade s ustanovením IS.D.OR.205 písm. b) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645 identifikovala každá organizácia podliehajúca jeho dohľadu;

2. ak sa vo vzájomných rozhraniach a súvisiacich rizikách, ktoré identifikovali rôzne organizácie, zistia nezrovnalosti, príslušný orgán ich preskúma s dotknutými organizáciami a v prípade potreby upozorní na primerané zistenia s cieľom zabezpečiť vykonanie nápravných opatrení;

3. ak sa preskúmaním dokumentácie podľa bodu 2 odhalí existencia významných rizík spojených s rozhraniami s organizáciami, ktoré podliehajú dohľadu iného príslušného orgánu v rámci toho istého členského štátu, tieto informácie sa oznámia zodpovedajúcemu príslušnému orgánu.“

9. Za ustanovenie 21.B.435 sa vkladá toto ustanovenie 21.B.435A:

„**21.B.435A. Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.D.OR.255 písm. a) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení 21.B.431. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením 21.B.433.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.D.OR.255 písm. b) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

PRÍLOHA V

Prílohy II (časť ARO) a III (časť ORO) k nariadeniu (EÚ) č. 965/2012 sa menia takto:

1. Príloha II (časť ARO) sa mení takto:

a) V ustanovení ARO.GEN.125 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

b) Za ustanovenie ARO.GEN.135 sa vkladá toto ustanovenie ARO.GEN.135A:

„**ARO.GEN.135A Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením ARO.GEN.125 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

c) V ustanovení ARO.GEN.200 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

d) Ustanovenie ARO.GEN.205 sa mení takto:

i) Nadpis sa nahrádza takto:

„**ARO.GEN.205 Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením ORO.GEN.200A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením ARO.GEN.200 písm. e) zahŕňal všetky úlohy osvedčovania a trvalého dohľadu vykonávané v jeho mene.“

e) V ustanovení ARO.GEN.300 sa dopĺňa toto písmeno g):

„g) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením ORO.GEN.200A, príslušný orgán okrem súladu s písmenami a) až f) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

f) Za ustanovenie ARO.GEN.330 sa vkladá toto ustanovenie ARO.GEN.330A:

„**ARO.GEN.330A Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení ARO.GEN.300. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením ARO.GEN.350.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

2. Príloha III (časť ORO) sa mení takto:

Za ustanovenie ORO.GEN.200 sa vkladá toto ustanovenie ORO.GEN.200A:

„**ORO.GEN.200A Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení ORO.GEN.200 musí prevádzkovateľ zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

PRÍLOHA VI

Príloha II (časť ADR.AR) k nariadeniu (EÚ) č. 139/2014 sa mení takto:

1. V ustanovení ADR.AR.A.025 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.D.OR.230 prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645.“

2. Za ustanovenie ADR.AR.A.030 sa vkladá toto ustanovenie ADR.AR.A.030A:

„**ADR.AR.A.030A. Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením ADR.AR.A.025 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

3. V ustanovení ADR.AR.B.005 sa dopĺňa toto písmeno d):

„d) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

4. Ustanovenie ADR.AR.B.010 sa mení takto:

i) Nadpis sa nahrádza takto:

„**ADR.AR.B.010. Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením ADR.OR.D.005A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením ADR.AR.B.005 písm. e) zahŕňal všetky úlohy osvedčovania a zachovávania dohľadu vykonávané v jeho mene.“

5. V ustanovení ADR.AR.C.005 sa dopĺňa toto písmeno f):

„f) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením ADR.OR.D.005A, príslušný orgán okrem súladu s písmenami a) až e) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

6. Za ustanovenie ADR.AR.C.040 sa vkladá toto ustanovenie ADR.AR.C.040A:

„**ADR.AR.C.040A. Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.D.OR.255 písm. a) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení ADR.AR.C.005. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením ADR.AR.C.055.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.D.OR.255 písm. b) prílohy (časť IS.D.OR) k delegovanému nariadeniu (EÚ) 2022/1645:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

PRÍLOHA VII

Prílohy II (časť 145), III (časť 66) a Vc (časť CAMO) k nariadeniu (EÚ) č. 1321/2014 sa menia takto:

1. Príloha II (časť 145) sa mení takto:

a) Obsah sa mení takto:

i) Za nadpis 145.A.200 sa vkladá tento nadpis:

„145.A.200A. Systém riadenia informačnej bezpečnosti“;

ii) Za nadpis 145.B.135 sa vkladá tento nadpis:

„145.B.135A. Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva“;

iii) Nadpis ustanovenia 145.B.205 sa nahrádza takto:

„145.B.205. Prideľovanie úloh“;

iv) Za nadpis 145.B.330 sa vkladá tento nadpis:

„145.B.330A. Zmeny systému riadenia informačnej bezpečnosti“;

b) Za ustanovenie 145.A.200 sa vkladá tento článok 145.A.200A:

„145.A.200A. **Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení 145.A.200 musí organizácia vykonávajúca údržbu zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“;

c) V ustanovení 145.B.125 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“;

d) Za ustanovenie 145.B.135 sa vkladá toto ustanovenie 145.B.135A:

„145.B.135A. **Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením 145.B.125 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“;

e) V ustanovení 145.B.200 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia zavedený a udržiavaný príslušným orgánom v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“;

f) Ustanovenie 145.B.205 sa mení takto:

i) Nadpis sa nahrádza takto:

„145.B.205. **Prideľovanie úloh**“;

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením 145.A.200A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením 145.B.200 písm. e) zahŕňal všetky úlohy osvedčovania a nepretržitého dohľadu vykonávané v jeho mene.“;

g) V ustanovení 145.B.300 sa dopĺňa toto písmeno g):

„g) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením 145.A.200A, príslušný orgán okrem súladu s písmenami a) až f) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“;

h) Za ustanovenie 145.B.330 sa vkladá toto ustanovenie 145.B.330A:

„145.B.330A. **Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení 145.B.300. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením 145.B.350.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

2. Príloha III (časť 66) sa mení takto:

a) V obsahu sa za nadpis 66.B.10 vkladá tento nadpis:

„66.B.15. Systém riadenia informačnej bezpečnosti“.

b) Za ustanovenie 66.B.10 sa vkladá toto ustanovenie 66.B.15:

„66.B.15. **Systém riadenia informačnej bezpečnosti**

Príslušný orgán zriadi, zavedie a udržiava systém riadenia informačnej bezpečnosti v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

3. Príloha Vc (časť CAMO) sa mení takto:

a) Obsah sa mení takto:

i) Za nadpis CAMO.A.200 sa vkladá tento nadpis:

„CAMO.A.200A Systém riadenia informačnej bezpečnosti“.

ii) Za nadpis CAMO.B.135 sa vkladá tento nadpis:

„CAMO.B.135A Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva“.

iii) Nadpis ustanovenia CAMO.B.205 sa nahrádza takto:

„CAMO.B.205 Prideľovanie úloh“.

iv) Za nadpis CAMO.B.330 sa vkladá tento nadpis:

„CAMO.B.330A Zmeny systému riadenia informačnej bezpečnosti“.

b) Za ustanovenie CAMO.A.200 sa vkladá toto ustanovenie CAMO.A.200A:

„CAMO.A.200A **Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení CAMO.A.200 musí organizácia zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

c) V ustanovení CAMO.B.125 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

d) Za ustanovenie CAMO.B.135 sa vkladá toto ustanovenie CAMO.B.135A:

„CAMO.B.135A **Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti, ktoré dostala v súlade s ustanovením CAMO.B.125 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

e) V ustanovení CAMO.B.200 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

f) Ustanovenie CAMO.B.205 sa mení takto:

i) Nadpis sa nahrádza takto:

„CAMO.B.205 **Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením CAMO.A.200A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením CAMO.B.200 písm. e) zahŕňal všetky úlohy osvedčovania a trvalého dohľadu vykonávané v jeho mene.“

g) V ustanovení CAMO.B.300 sa dopĺňa toto písmeno g):

„g) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením CAMO.A.200A, príslušný orgán okrem súladu s písmenami a) až f) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

h) Za ustanovenie CAMO.B.330 sa vkladá toto ustanovenie CAMO.B.330A:

„CAMO.B.330A **Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení CAMO.B.300. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením CAMO.B.350.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

PRÍLOHA VIII

Prílohy II (časť ATCO.AR) a III (časť ATCO.OR) k nariadeniu (EÚ) 2015/340 sa menia takto:

1. Príloha II (časť ATCO.AR) sa mení takto:

a) V ustanovení ATCO.AR.A.020 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

b) Za ustanovenie ATCO.AR.A.025 sa vkladá toto ustanovenie ATCO.AR.A.025A:

„**ATCO.AR.A.025A. Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti prijatých v súlade s ustanovením ATCO.AR.A.020, a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

c) V ustanovení ATCO.AR.B.001 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

d) Ustanovenie ATCO.AR.B.005 sa mení takto:

i) Nadpis sa nahrádza takto:

„**ATCO.AR.B.005. Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením ATCO.OR.C.001A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením ATCO.AR.B.001 písm. e) zahŕňal všetky úlohy osvedčovania a zachovania dohľadu vykonávané v jeho mene.“

e) V ustanovení ATCO.AR.C.001 sa dopĺňa toto písmeno f):

„f) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením ATCO.OR.C.001A, príslušný orgán okrem súladu s písmenami a) až e) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

f) Za ustanovenie ATCO.AR.E.010 sa vkladá toto ustanovenie ATCO.AR.E.010A:

„**ATCO.AR.E.010A. Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení ATCO.AR.C.001. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením ATCO.AR.C.010.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

2. Príloha III (časť ATCO.OR) sa mení takto:

Za ustanovenie ATCO.OR.C.001 sa vkladá toto ustanovenie ATCO.OR.C.001A:

„**ATCO.OR.C.001A. Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení ATCO.OR.C.001 musí výcviková organizácia zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

PRÍLOHA IX

Prílohy II (časť ATM/ANS.AR) a III (časť ATM/ANS.OR) k vykonávaciemu nariadeniu (EÚ) 2017/373 sa menia takto:

1. Príloha II (časť ATM/ANS.AR) sa mení takto:

a) V ustanovení ATM/ANS.AR.A.020 sa dopĺňa toto písmeno c):

„c) Príslušný orgán členského štátu poskytne agentúre čo najskôr informácie dôležité z hľadiska bezpečnosti vyplývajúce zo správ o informačnej bezpečnosti, ktoré dostal podľa ustanovenia IS.I.OR.230 prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203.“

b) Za ustanovenie ATM/ANS.AR.A.025 sa vkladá toto ustanovenie ATM/ANS.AR.A.025A:

„**ATM/ANS.AR.A.025A Okamžitá reakcia na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s vplyvom na bezpečnosť letectva**

a) Príslušný orgán zavedie systém na primerané zhromažďovanie, analýzu a šírenie informácií týkajúcich sa incidentov a zraniteľností v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva, ktoré nahlásia organizácie. Uskutočňuje sa to v koordinácii s akýmikoľvek inými relevantnými orgánmi zodpovednými za informačnú bezpečnosť alebo kybernetickú bezpečnosť v rámci členského štátu s cieľom zvýšiť koordináciu a kompatibilitu systémov nahlasovania.

b) Agentúra zavedie systém na primeranú analýzu všetkých relevantných informácií dôležitých z hľadiska bezpečnosti prijatých v súlade s ustanovením ATM/ANS.AR.A.020 písm. c), a bez zbytočného odkladu poskytne členským štátom a Komisii všetky informácie vrátane odporúčaní alebo nápravných opatrení, ktoré sa majú prijať, potrebné na to, aby mohli včas reagovať na incident alebo zraniteľnosť v oblasti informačnej bezpečnosti s možným vplyvom na bezpečnosť letectva vrátane výrobkov, súčastí, nenainštalovaného vybavenia, osôb alebo organizácií, na ktoré sa vzťahuje nariadenie (EÚ) 2018/1139 a jeho delegované a vykonávacie akty.

c) Po prijatí informácií uvedených v písmenách a) a b) príslušný orgán prijme primerané opatrenia na riešenie potenciálneho vplyvu incidentu alebo zraniteľnosti v oblasti informačnej bezpečnosti na bezpečnosť letectva.

d) O opatreniach prijatých v súlade s písmenom c) okamžite informuje všetky osoby alebo organizácie, ktoré sa nimi musia riadiť podľa nariadenia (EÚ) 2018/1139 a jeho delegovaných a vykonávacích aktov. Príslušný orgán členského štátu o týchto opatreniach informuje aj agentúru, a ak sú potrebné spojené opatrenia, príslušné orgány ostatných dotknutých členských štátov.“

c) V ustanovení ATM/ANS.AR.B.001 sa dopĺňa toto písmeno e):

„e) Okrem požiadaviek uvedených v písmene a) musí byť systém riadenia, ktorý zriadil a udržiava príslušný orgán, v súlade s prílohou I (časť IS.AR) k vykonávaciemu nariadeniu (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

d) Ustanovenie ATM/ANS.AR.B.005 sa mení takto:

i) Nadpis sa nahrádza takto:

„**ATM/ANS.AR.B.005 Prideľovanie úloh**“.

ii) Dopĺňa sa toto písmeno c):

„c) Pokiaľ ide o osvedčovanie súladu organizácie s ustanovením ATM/ANS.OR.B.005A a dohľad nad ním, príslušný orgán môže prideliť úlohy oprávneným subjektom v súlade s písmenom a) alebo akémukoľvek relevantnému orgánu zodpovednému za informačnú bezpečnosť alebo kybernetickú bezpečnosť v členskom štáte. Pri prideľovaní úloh musí príslušný orgán zabezpečiť, aby:

1. všetky aspekty súvisiace s bezpečnosťou letectva koordinoval a zohľadňoval oprávnený subjekt alebo relevantný orgán;

2. výsledky činností osvedčovania a dohľadu, ktoré vykonáva oprávnený subjekt alebo relevantný orgán, boli začlenené do celkovej dokumentácie organizácie týkajúcej sa osvedčovania a dohľadu;

3. jeho vlastný systém riadenia informačnej bezpečnosti zriadený v súlade s ustanovením ATM/ANS.AR.B.001 písm. e) zahŕňal všetky úlohy osvedčovania a trvalého dohľadu vykonávané v jeho mene.“

e) V ustanovení ATM/ANS.AR.C.010 sa dopĺňa toto písmeno d):

„d) Pokiaľ ide o osvedčovanie a dohľad nad súladom organizácie s ustanovením ATM/ANS.OR.B.005A, príslušný orgán okrem súladu s písmenami a) až c) preskúma každé schválenie udelené podľa ustanovenia IS.I.OR.200 písm. e) tohto nariadenia alebo ustanovenia IS.D.OR.200 písm. e) delegovaného nariadenia (EÚ) 2022/1645 v nadväznosti na príslušný cyklus auditu dohľadu a vždy, keď sa vykonajú zmeny v rozsahu práce organizácie.“

f) Za ustanovenie ATM/ANS.AR.C.025 sa vkladá toto ustanovenie ATM/ANS.AR.C.025A:

„**ATM/ANS.AR.C.025A Zmeny systému riadenia informačnej bezpečnosti**

a) Pokiaľ ide o zmeny riadené a oznamované príslušnému orgánu v súlade s postupom stanoveným v ustanovení IS.I.OR.255 písm. a) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203, príslušný orgán začlení preskúmanie takýchto zmien do svojho trvalého dohľadu v súlade so zásadami stanovenými v ustanovení ATM/ANS.AR.C.010. Ak sa zistí akýkoľvek nesúlad, príslušný orgán ho oznámi organizácii, požiada o ďalšie zmeny a koná v súlade s ustanovením ATM/ANS.AR.C.050.

b) Pokiaľ ide o iné zmeny, ktoré si vyžadujú žiadosť o schválenie v súlade s ustanovením IS.I.OR.255 písm. b) prílohy II (časť IS.I.OR) k vykonávaciemu nariadeniu (EÚ) 2023/203:

1. po prijatí žiadosti o zmenu príslušný orgán pred vydaním schválenia skontroluje, či organizácia spĺňa príslušné požiadavky;

2. príslušný orgán stanoví podmienky, za ktorých môže organizácia pôsobiť počas zavádzania zmeny;

3. ak sa príslušný orgán presvedčí, že organizácia spĺňa príslušné požiadavky, zmenu schváli.“

2. Príloha III (časť ATM/ANS.OR) sa mení takto:

a) Za ustanovenie ATM/ANS.OR.B.005 sa vkladá toto ustanovenie ATM/ANS.OR.B.005A:

„**ATM/ANS.OR.B.005A Systém riadenia informačnej bezpečnosti**

Okrem systému riadenia uvedeného v ustanovení ATM/ANS.OR.B.005 musí poskytovateľ služieb zriadiť, zaviesť a udržiavať systém riadenia informačnej bezpečnosti v súlade s vykonávacím nariadením (EÚ) 2023/203 s cieľom zabezpečiť riadne riadenie rizík v oblasti informačnej bezpečnosti, ktoré môžu mať vplyv na bezpečnosť letectva.“

b) Ustanovenie ATM/ANS.OR.D.010 sa nahrádza takto:

„**ATM/ANS.OR.D.010 Riadenie bezpečnostnej ochrany**

a) Poskytovatelia leteckých navigačných služieb, poskytovatelia, ktorí zabezpečujú manažment toku letovej prevádzky, a manažér siete musia ako neoddeliteľnú súčasť svojho systému riadenia podľa ustanovenia ATM/ANS.OR.B.005 zriadiť systém riadenia bezpečnostnej ochrany, aby zabezpečili:

1. takú bezpečnostnú ochranu svojich zariadení a pracovníkov, aby sa zabránilo akémukoľvek protiprávnemu zasahovaniu do poskytovania služieb;

2. takú bezpečnostnú ochranu prevádzkových údajov, ktoré prijímajú, vytvárajú alebo inak používajú, aby prístup k nim mali vyhradený len oprávnené osoby.

b) V systéme riadenia bezpečnostnej ochrany sa vymedzujú:

1. proces a postupy súvisiace s posudzovaním bezpečnostného rizika a jeho zmierňovaním, monitorovaním bezpečnostnej ochrany a jej zlepšovaním, preskúmaním bezpečnostnej ochrany a so šírením poznatkov;

2. prostriedky určené na identifikáciu, monitorovanie a odhaľovanie narušenia bezpečnostnej ochrany a na upozornenie pracovníkov vhodnými bezpečnostnými upozorneniami;

3. prostriedky na zvládanie následkov narušenia bezpečnostnej ochrany a na identifikovanie opatrení na zotavenie a postupov na zmiernenie účinkov s cieľom zabrániť ich opätovnému výskytu.

c) Poskytovatelia leteckých navigačných služieb, poskytovatelia, ktorí zabezpečujú manažment toku letovej prevádzky, a manažér siete v prípade potreby zabezpečia bezpečnostnú previerku svojich pracovníkov a spolupracujú s príslušnými civilnými a vojenskými orgánmi s cieľom zaistiť bezpečnostnú ochranu svojich zariadení, personálu a údajov.

d) Aspekty súvisiace s informačnou bezpečnosťou sa riadia v súlade s ustanovením ATM/ANS.OR.B.005A.“