Väljaandja:	Riigikogu
Akti liik:	seadus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	23.05.2018
Redaktsiooni kehtivuse lõpp:	Hetkel kehtiv
Avaldamismärge:	RT I, 22.05.2018, 1

Välja kuulutanud
Vabariigi President
14.05.2018 otsus nr 252

Küberturvalisuse seadus[1]

Vastu võetud 09.05.2018

1. peatükk
Üldsätted

§ 1. Seaduse reguleerimis- ja kohaldamisala

(1) Käesolev seadus sätestab ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused.

(2) Käesolevat seadust ei kohaldata riigisaladuse ja salastatud välisteabe töötlemisele ning sellise teabe töötlussüsteemide pidamisele.

(3) Käesolevat seadust ei kohaldata digitaalse teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades mikro- ja väikeste ettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41).

(4) Kui võrgu- ja infosüsteemi pidamise nõuded on reguleeritud välislepinguga või muu seadusega, kohaldatakse käesolevat seadust välislepingust või muust seadusest tulenevate erisustega.

(5) Käesolevas seaduses sätestatud haldusmenetlusele kohaldatakse haldusmenetluse seaduse sätteid, arvestades käesoleva seaduse erisusi.

§ 2. Terminid

Käesolevas seaduses kasutatakse termineid järgmises tähenduses:
1) võrgu- ja infosüsteem (edaspidi *süsteem*) – elektroonilise side võrk elektroonilise side seaduse § 2 punkti 8 tähenduses, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringuga või edastatakse eelnimetatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks;
2) süsteemi turvalisus – süsteemi võime osutada vastupanu mis tahes tegevusele, mis ohustab süsteemis töödeldavate andmete või süsteemi kaudu osutatavate või juurdepääsetavate teenuste käideldavust, autentsust, terviklust ja konfidentsiaalsust;
3) küberintsident – süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust;
4) digitaalse teenuse osutaja esindaja (edaspidi *esindaja*) – Euroopa Liidus asuv füüsiline või juriidiline isik, kes on määratud tegutsema väljaspool Euroopa Liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib liikmesriigi pädev asutus või küberturbe intsidentide lahendamise üksus pöörduda digitaalse teenuse osutaja asemel seoses digitaalse teenuse osutaja kohustusega, mis tuleneb käesolevast seadusest;
5) internetipõhine kauplemiskoht – infoühiskonna teenus, mis võimaldab tarbijakaitseseaduse tähenduses tarbijal ja kauplejal sõlmida internetipõhise müügi- või teenuse osutamise lepingu kas internetipõhise kauplemiskoha veebisaidil või kaupleja veebisaidil, mis kasutab internetipõhise kauplemiskoha pakutavat andmetöötlusteenust;
6) internetipõhine otsimootor – infoühiskonna teenus, mis võimaldab kasutajal teha otsingut kõikidel veebisaitidel või konkreetses keeles veebisaitidel mis tahes teemal võtmesõna, fraasi või muu sisendi vormis päringu alusel ning saadab vastuseks lingid, kust võib leida teavet taotletud sisu kohta;

7) pilvandmetöötlusteenus – infoühiskonna teenus, mis võimaldab juurdepääsu andmetöötlusressursside kogumile, mis on paindlikult jagatav ning laiendatav süsteemi ennast muutmata;
8) küberturbe intsidentide lahendamise üksus – ekspertide grupp, kelle ülesandeks on küberintsidendi tuvastamist, analüüsimist ja ohjeldamist ning küberintsidendile reageerimist toetavad toimingud.

§ 3. Teenuse osutaja

(1) Teenuse osutaja käesoleva seaduse tähenduses on isik, kes kasutab süsteemi järgmiselt:
1) hädaolukorra seaduses sätestatud elutähtsa teenuse osutaja elutähtsa teenuse osutamisel;
2) raudteeseaduses sätestatud raudtee-ettevõtja, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20 protsenti kaubaveo või reisijateveo turuosast avaliku raudtee toimimise ning raudteeveo ja avaliku reisijateveo toimimise teenuse osutamisel;
3) lennundusseaduses sätestatud lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja lennuvälja toimimise ja aeronavigatsiooni toimimise teenuse osutamisel;
4) sadamateenuse osutaja, kellele kuulub sadamaseaduses sätestatud sadam, mis teenindab rahvusvahelises meresõidus sõitvaid reisilaevu või 500-se ja enama kogumahutavusega laevu, ning sadam, mis teenindab meresõiduohutuse seaduse kohaselt määratletud kohalikus rannasõidus sõitvaid I kategooria laevu või A-klassi reisilaevu sadama toimimise teenuse osutamisel;
5) elektroonilise side seaduses sätestatud sideettevõtja, kes osutab kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, ja ringhäälinguvõrgu teenuse osutaja kaabelleviteenuse või ringhäälinguvõrgu teenuse osutamisel;
6) tervishoiuteenuste korraldamise seaduses sätestatud haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja statsionaarse eriarstiabi osutamisel ja kiirabibrigaadi pidaja kiirabi osutamisel;
7) tervishoiuteenuste korraldamise seaduses sätestatud perearst üldarstiabi osutamisel;
8) Eesti maatunnusega seotud tipptaseme domeeninimede registri haldaja registri pidamiseks kasutatava süsteemi ja tipptaseme nimeserveri teenuse osutamisel;
9) kriitilise tähtsusega side-, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja elektroonilise side seaduse tähenduses nende teenuste osutamisel;
10) Eesti Rahvusringhääling Eesti Rahvusringhäälingu seaduse § 5 lõike 1 punktis 10 sätestatud ülesande täitmisel.

(2) Käesoleva paragrahvi lõikes 1 nimetatud teenuse osutajat, kes tegutseb Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.07.2016, lk 1–30), II lisas esitatud sektorites, loetakse olulise teenuse operaatoriks nimetatud direktiivi tähenduses.

(3) Riigi Infosüsteemi Amet tuvastab iga kahe aasta tagant käesoleva seaduse kohaldamisalas olevad teenuse osutajad, kes tegutsevad Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 II lisas esitatud sektorites.

(4) Käesolevas seaduses teenuse osutaja kohta sätestatut kohaldatakse ka riigi ja kohaliku omavalitsuse üksusele käesoleva seaduse §-s 9 sätestatud erisusega.

§ 4. Digitaalse teenuse osutaja

(1) Digitaalse teenuse osutaja käesoleva seaduse tähenduses on infoühiskonna teenuse seaduses sätestatud infoühiskonna teenuse osutaja, kes:
1) pakub internetipõhist kauplemiskohta;
2) pakub internetipõhist otsimootorit või
3) osutab pilvandmetöötlusteenust.

(2) Eestis teenust osutav, kuid väljaspool Euroopa Liitu asutatud digitaalse teenuse osutaja peab määrama esindaja Eestis või mõnes teises Euroopa Liidu liikmesriigis, kus ta teenust osutab, ning tegema püsivalt avalikult kättesaadavaks esindaja kontaktandmed.

§ 5. Ühtne kontaktpunkt ja pädev asutus

Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 artikli 8 lõikes 1 nimetatud pädeva asutuse ja lõikes 3 nimetatud ühtse kontaktpunkti ning artikli 9 lõikes 1 nimetatud küberturbe intsidentide lahendamise üksuse ülesandeid täidab Riigi Infosüsteemi Amet.

§ 6. Küberturvalisuse tagamise põhimõtted

Küberturvalisuse tagamisel arvestatakse järgmisi põhimõtteid:
1) isiklikkuse põhimõte – süsteemi turvalisuse tagamist korraldab teenuse osutaja;
2) tervikliku kaitse põhimõte – teenuse osutaja teeb kindlaks võimalikud ohud süsteemile ning rakendab süsteemi kaitseks kohaseid korralduslikke ja tehnilisi abinõusid;
3) kahjuliku mõju vähendamise põhimõte – teenuse osutaja rakendab küberintsidendi korral vajalikku hoolsust ja abinõusid, et vältida küberintsidendi mõju laienemist ja võimalikku levikut teisele süsteemile, ning teavitab küberintsidendist käesolevas seaduses sätestatud järelevalveasutust;
4) koostööpõhimõte – küberturvalisuse tagamisel ja küberintsidentide lahendamisel teevad osalised koostööd ja võtavad vajaduse korral arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust.

2. peatükk
Kohustused küberturvalisuse tagamiseks

§ 7. Teenuse osutaja süsteemi turvameetmed

(1) Teenuse osutaja peab rakendama alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid:
1) küberintsidendi ennetamiseks;
2) küberintsidendi lahendamiseks;
3) küberintsidendi tõttu teenuse toimepidevusele või süsteemi turvalisusele avalduva mõju ennetamiseks ja leevendamiseks või teise sõltuva teenuse toimepidevusele või süsteemi turvalisusele avalduda võiva mõju ennetamiseks ja leevendamiseks.

(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:
1) koostama süsteemi riskianalüüsi, milles tuleb esitada süsteemi turvalisust ja teenuse toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu, määrata riskide realiseerumisel tekkiva küberintsidendi tagajärgede raskusaste ning kirjeldada küberintsidendi lahendamise abinõusid;
2) tagama dokumenteeritud süsteemi riskianalüüsi, turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasuse;
3) tagama süsteemi turvalisust ohustava tegevuse või tarkvara tuvastamiseks süsteemi seire ja edastama teavet süsteemi turvalisust ohustava tegevuse või tarkvara kohta Riigi Infosüsteemi Ametile;
4) võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile;
5) kontrollima turvameetmete rakendamise piisavust ja vastavust ning dokumenteerima kontrolli tulemused;
6) säilitama käesoleva lõike punktis 5 sätestatud dokumente vähemalt kolm aastat dokumendi loomisest arvates.

(3) Kui teenuse osutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuse osutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise.

(4) Teenuse osutamiseks kasutatava süsteemi turvameetmete kirjelduse ning riskianalüüsi koostamise nõuded kehtestab valdkonna eest vastutav ministermäärusega.

§ 8. Teenuse osutaja kohustus teavitada küberintsidendist

(1) Teenuse osutaja teavitab Riigi Infosüsteemi Ametit viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist:
1) millel on süsteemi turvalisusele või teenuse toimepidevusele oluline mõju;
2) mille oluline mõju süsteemi turvalisusele või teenuse toimepidevusele ei ole ilmne, kuid seda võib mõistlikult eeldada.

(2) Küberintsidendil on oluline mõju, kui on täidetud vähemalt üks järgmistest tingimustest:
1) küberintsidendi mõju on käesoleva seaduse § 7 lõike 2 punkti 1 alusel koostatud süsteemi riskianalüüsis määratud tagajärgede raskusastme kohaselt vähemalt raske;
2) küberintsidendi tõttu ei ole teenuse osutamist võimalik jätkata teenustaseme kokkuleppes või teenuse toimepidevuse nõuetes sätestatud teenuse maksimaalse lubatud katkestuse aja möödumisel;
3) küberintsidendi tõttu on häiritud teise teenuse osutaja teenuse toimepidevus;
4) küberintsidendi lahendamiseks tuleb rakendada käesoleva seaduse § 7 lõike 2 punkti 1 alusel koostatud süsteemi riskianalüüsis või selle olemasolul muus teenuse toimepidevuse või süsteemi turvalisuse taastamist kirjeldavas dokumendis toodud erakorralisi abinõusid;
5) teenuse osutajale, teise teenuse osutajale või teenuse kasutajatele on küberintsidendi tõttu tekkinud või võib tekkida märkimisväärne kahju.

(3) Kui küberintsidendi tagajärjel on teenuse või teise teenuse osutamine häiritud veel vähemalt ühes Euroopa Liidu liikmesriigis, loetakse küberintsident alati olulise mõjuga küberintsidendiks.

(4) Käesoleva paragrahvi lõikes 1 sätestatud kohustus ei piira teenuse osutaja õigust teavitada Riigi Infosüsteemi Ametit küberintsidendist, millel ei ole käesoleva paragrahvi lõikes 2 sätestatud olulist mõju.

(5) Teenuse osutaja on kohustatud teavitama mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada.

(6) Kui teenuse osutaja ei täida käesoleva paragrahvi lõikes 5 sätestatud teavitamiskohustust mõistliku aja jooksul, võib Riigi Infosüsteemi Amet mõjutatud isikut või avalikkust ise teavitada, informeerides teavitamisest ka teenuse osutajat.

(7) Teenuse osutaja on olulise mõjuga küberintsidendi lahendamisel kohustatud edastama Riigi Infosüsteemi Ametile raporti, mis sisaldab informatsiooni küberintsidendi tekkepõhjuste, selle lahendamiseks kulunud aja ja rakendatud abinõude ning küberintsidendi mõju kohta.

(8) Küberintsidendist teavitamise korra ja raporti vormi võib kehtestada valdkonna eest vastutav ministermäärusega.

(9) Teenuse osutaja on kohustatud teavitama Riigi Infosüsteemi Ametit digitaalse teenuse osutajat puudutava küberintsidendi olulisest mõjust oma teenuse toimepidevusele, kui tema teenus sõltub käesoleva seaduse §-s 4 määratletud digitaalse teenuse osutaja teenusest.

§ 9. Riigi ja kohaliku omavalitsuse üksuse süsteemi turvameetmed

(1) Riigi ja kohaliku omavalitsuse üksuse süsteemi haldamisel kohaldatakse käesoleva seaduse § 7 lõigetes 1–3 sätestatud kohustusi ning §-s 8 sätestatud küberintsidendist teavitamise nõudeid.

(2) Käesoleva paragrahvi lõikes 1 nimetatud süsteemi turvalisuse tagamisele kohaldatakse avaliku teabe seaduse § 43^9 lõike 1 punkti 4 alusel kehtestatud määruses sätestatud nõudeid.

(3) Kaitseministeeriumi valitsemisalas rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvanõuded kehtestab valdkonna eest vastutav ministermäärusega.

§ 10. Digitaalse teenuse osutaja süsteemi turvameetmed

(1) Digitaalse teenuse osutaja on kohustatud tegema kindlaks riskid, mis ohustavad süsteemi turvalisust, ja neid analüüsima ning rakendama riskide juhtimiseks kohaseid korralduslikke ja tehnilisi meetmeid.

(2) Süsteemi turvalisuse tagamise meetmete valikul tuleb arvestada:
1) tehnilise taristu turvalisust;
2) küberintsidendi ennetamist, tuvastamist ja lahendamist;
3) toimepidevuse haldamist;
4) seiret, auditeerimist ja testimist;
5) rahvusvahelistele standarditele vastavust.

(3) Käesoleva paragrahvi lõike 2 rakendamisel on digitaalse teenuse osutaja kohustatud juhinduma Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 artikli 16 lõike 8 alusel antud Euroopa Komisjoni rakendusmäärusest.

(4) Digitaalse teenuse osutaja rakendab asjakohaseid meetmeid, et võimalikult vähendada küberintsidendi mõju osutatava teenuse toimepidevusele.

§ 11. Digitaalse teenuse osutaja kohustus teavitada küberintsidendist

(1) Digitaalse teenuse osutaja teavitab pädevat asutust või küberturbe intsidentide lahendamise üksust küberintsidendist, millel on oluline mõju osutatavale digitaalsele teenusele, viivitamata pärast küberintsidendist teada saamist.

(2) Teade tuleb esitada selle liikmesriigi pädevale asutusele või küberturbe intsidentide lahendamise üksusele, kus on:
1) digitaalse teenuse osutaja asutatud;
2) kontserni puhul asutatud kontserni emaettevõtja või
3) kolmandast riigist pärit ettevõtja määratud esindaja.

(3) Küberintsidendist teavitamisel lähtutakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 artikli 16 lõike 8 alusel antud Euroopa Komisjoni rakendusmääruses sätestatud kriteeriumidest.

(4) Teade peab sisaldama teavet, mis võimaldab pädeval asutusel või küberturbe intsidentide lahendamise üksusel küberintsidendi piiriülest mõju kindlaks teha.

(5) Kui küberintsidendil on oluline mõju digitaalse teenuse toimepidevusele teises liikmesriigis, teavitab Riigi Infosüsteemi Amet digitaalse teenuse osutaja esitatud teabe põhjal mõjutatud liikmesriiki.

(6) Kui küberintsidendi ennetamiseks või käimasoleva küberintsidendi lahendamiseks ja avalikes huvides on vajalik avalikkuse teavitamine, võib Riigi Infosüsteemi Amet pärast digitaalse teenuse osutaja informeerimist teavitada küberintsidendist avalikkust või kohustada seda tegema digitaalse teenuse osutajat.

(7) Käesoleva paragrahvi lõiget 1 ei kohaldata, kui digitaalse teenuse osutajal puudub küberintsidendi mõju olulisuse tuvastamiseks teave.

3. peatükk

Küberturvalisuse tagamine

§ 12. Küberintsidendi ennetus ja lahendamine

(1) Küberturvalisuse tagamist ning küberintsidendi ennetamist ja lahendamist käesolevas seaduses sätestatud ulatuses koordineerib Riigi Infosüsteemi Amet.

(2) Riigi Infosüsteemi Amet teostab küberturvalisuse tagamiseks Eesti internetiprotokolli aadressiruumis olevate ning Eesti maatunnusega seotud domeenide vaatlust, analüüsib süsteemide turvalisust ohustavaid riske ning nende mõju riigile, ühiskonnale ja süsteemide turvalisusele.

(3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

(4) Riigi Infosüsteemi Ametil on õigus välisriigile või Euroopa Liidu Võrgu- ja Infoturbeametile või muule organisatsioonile edastada küberintsidendi ennetamise ja lahendamisega seotud teavet käesoleva seaduse §-s 5 sätestatud ülesannete või Euroopa Liidu õigusest tuleneva kohustuse täitmiseks või välislepinguga ettenähtud juhtudel ja korras, kui edastatav teave ei kahjusta riigi julgeolekut või kriminaalmenetlust.

(5) Teabe edastamisel arvestab Riigi Infosüsteemi Amet teenuse osutaja või digitaalse teenuse osutaja ärihuve ja juhindub ärisaladuse hoidmise kohustusest.

§ 13. Küberintsidentide register

(1) Küberintsidentide register (edaspidi *register*) on Riigi Infosüsteemi Ameti peetav andmekogu, kuhu kantakse küberintsidendi toimumist kirjeldavad andmed eesmärgiga pidada küberintsidentide üle arvestust ning analüüsida küberintsidente nende lahendamiseks, ohuteadete edastamiseks ja järelevalvetoimingute tegemiseks.

(2) Register on piiratud juurdepääsuga ja registriandmed on mõeldud asutusesiseseks kasutamiseks, kui õigusaktis ei ole sätestatud teisiti.

(3) Registri asutab ja selle põhimääruse kehtestab valdkonna eest vastutav ministermäärusega.

4. peatükk
Riiklik ja haldusjärelevalve

§ 14. Riikliku ja haldusjärelevalve tegemine

(1) Käesolevas seaduses ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle teeb riiklikku ja haldusjärelevalvet Riigi Infosüsteemi Amet.

(2) Riiklikku järelevalvet digitaalse teenuse osutajale käesoleva seaduse §-dega 10 ja 11 kehtestatud nõuete täitmise üle tehakse juhul, kui Riigi Infosüsteemi Ametit teavitatakse, et nimetatud nõudeid ei täida:
1) digitaalse teenuse osutaja, kes on asutatud Eestis;
2) kontserni kuuluv digitaalse teenuse osutaja, kelle emaettevõtja on asutatud Eestis;
3) kolmanda riigi digitaalse teenuse osutaja, kellel on Eestis esindaja.

(3) Käesoleva seaduse § 9 lõike 3 alusel kehtestatud määruses sätestatud süsteemide nõuete täitmise üle teevad haldusjärelevalvet Kaitseministeerium ja Kaitsevägi.

§ 15. Riikliku järelevalve erimeetmed

(1) Korrakaitseorgan võib käesolevas seaduses sätestatud riikliku järelevalve tegemiseks kohaldada korrakaitseseaduse §-des 30, 31, 32, 49, 50 ja 51 sätestatud riikliku järelevalve erimeetmeid korrakaitseseaduses sätestatud alusel ja korras.

(2) Käesoleva seaduse §-de 7 ja 8 ning nende alusel kehtestatud õigusaktide nõuete täitmise üle riikliku järelevalve tegemisel võib korrakaitseorgan kohaldada lisaks käesoleva paragrahvi lõikes 1 nimetatud erimeetmetele ka korrakaitseseaduse §-s 52 sätestatud riikliku järelevalve erimeedet korrakaitseseaduses sätestatud alusel ja korras.

§ 16. Riikliku järelevalve erisused

(1) Riigi Infosüsteemi Amet võib küberintsidendi korral vahetu kõrgendatud ohu tõrjumiseks või korrarikkumise kõrvaldamiseks süsteemi kasutamist või süsteemile juurdepääsu piirata, kui esinevad kõik järgmised tingimused:
1) küberintsident ohustab või kahjustab teise süsteemi turvalisust;
2) süsteemi haldaja ei saa või ei saa õigel ajal ise küberintsidendist lähtuvat kõrgendatud ohtu tõrjuda või korrarikkumist kõrvaldada;
3) küberintsidendist lähtuvat kõrgendatud ohtu ei saa tõrjuda ega korrarikkumist kõrvaldada vähem riivava meetmega;
4) küberintsidendist lähtuva kõrgendatud ohu tõrjumisega või korrarikkumise kõrvaldamisega ei tekitata isikule ebaproportsionaalset kahju.

(2) Käesolevas paragrahvis sätestatud meetme kohaldamisest tuleb adressaati ja käesoleva seaduse § 3 lõike 1 punktis 1 sätestatud teenuse osutaja puhul ka elutähtsa teenuse toimepidevust korraldavat asutust esimesel võimalusel teavitada.

(3) Käesolevas paragrahvis sätestatud meetme protokollimine on kohustuslik.

§ 17. Haldusjärelevalve meetmed

(1) Riigi Infosüsteemi Amet on haldusjärelevalve tegemisel volitatud pääsema ligi süsteemile ning piirama süsteemi kasutamist või süsteemile juurdepääsu, kui esinevad kõik järgmised tingimused:
1) küberintsident ohustab või kahjustab teise süsteemi turvalisust;
2) süsteemi haldaja ei saa või ei saa õigel ajal ise küberintsidendist lähtuvat ohtu tõrjuda või küberintsidenti kõrvaldada;
3) küberintsidendist lähtuvat ohtu ei saa tõrjuda ega küberintsidenti kõrvaldada isiku suhtes vähem riivava meetmega;
4) küberintsidendist lähtuva ohu tõrjumisega või küberintsidendi kõrvaldamisega ei tekitata isikule ebaproportsionaalset kahju.

(2) Käesolevas paragrahvis sätestatud meetme kohaldamisest tuleb adressaati esimesel võimalusel teavitada.

(3) Käesolevas paragrahvis sätestatud meetme protokollimine on kohustuslik.

5. peatükk
Vastutus

§ 18. Seaduse nõuete rikkumine

(1) Käesoleva seaduse § 7 lõigetes 1–3 sätestatud nõuete rikkumise eest –
karistatakse rahatrahviga kuni 200 trahviühikut.

(2) Sama teo eest, kui selle on toime pannud juriidiline isik, –
karistatakse rahatrahviga kuni 20 000 eurot.

§ 19. Menetlus

(1) Käesoleva seaduse §-s 18 sätestatud väärteo kohtuväline menetleja on Riigi Infosüsteemi Amet.

(2) Kui käesoleva seaduse §-s 18 sätestatud väärtegu on seotud isikuandmete töötlemise nõuete rikkumisega, kohaldatakse väärteomenetluse puhul isikuandmete kaitse seadust.

6. peatükk
Rakendussätted

§ 20. Teenuse osutajate tuvastamine

Riigi Infosüsteemi Amet tuvastab käesoleva seaduse § 3 lõikes 3 nimetatud teenuse osutajad 2018. aasta 9. novembriks.

§ 21. Eesti Rahvusringhäälingu seaduse muutmine

Eesti Rahvusringhäälingu seaduses tehakse järgmised muudatused:

1)paragrahvi 5 täiendatakse lõikega 2^1 järgmises sõnastuses:

„(2^1) Rahvusringhääling on kohustatud käesoleva paragrahvi lõike 1 punktis 10 sätestatud ülesande täitmiseks kasutatavate võrgu- ja infosüsteemide turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.";

2)paragrahvi 34 täiendatakse lõikega 4^1 järgmises sõnastuses:

„(4^1) Haldusjärelevalvet käesoleva seaduse § 5 lõike 2^1 nõuete täitmise üle teeb Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.".

§ 22. Elektroonilise side seaduse muutmine

Elektroonilise side seaduses tehakse järgmised muudatused:

1)paragrahvi 87^2 lõige 6 muudetakse ja sõnastatakse järgmiselt:

„(6) Sideettevõtjale, kes osutab elutähtsat teenust, kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, või ringhäälinguvõrgu teenust, kohaldatakse käesoleva paragrahvi lõigetes 1–5 sätestatud nõuete asemel küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.";

2)paragrahvi 100^3 lõige 3 muudetakse ja sõnastatakse järgmiselt:

„(3) Kriitilise tähtsusega sideteenuse osutaja peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.";

3)paragrahvi 100^4 lõige 2 muudetakse ja sõnastatakse järgmiselt:

„(2) Mereraadioside teenuse osutaja peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.";

4)paragrahvi 100^5 lõige 2 muudetakse ja sõnastatakse järgmiselt:

„(2) ESTER-i teenuse osutaja peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.";

5)seadust täiendatakse §-ga 114^3 järgmises sõnastuses:

„**§ 114^3. Riigi Infosüsteemi Ametile teabe andmise kohustus**

Sideettevõtja on kohustatud Riigi Infosüsteemi Ameti järelepärimisel esitama küberintsidendi põhjustanud seadme või küberintsidendist ohustatud seadme väljaselgitamiseks järgmised andmed:
1) Interneti-seansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille andmeside teenuse osutaja on seadmele eraldanud;
2) seadme Interneti-protokolli aadressi protokoll ning seadmesse liikuvate pakettide sihtport ja vastuspakettide lähteport.";

6)paragrahvi 133 lõige 5 muudetakse ja sõnastatakse järgmiselt:

„(5) Riiklikku ja haldusjärelevalvet käesoleva seaduse §-s 87^2 sätestatud sidevõrkude ja -teenuste turvalisuse ning terviklikkuse tagamise üle ning käesoleva seaduse § 87^2 lõike 6, § 100^3 lõike 3, § 100^4 lõike 2 ja § 100^5 lõike 2 nõuete täitmise üle teostab Riigi Infosüsteemi Amet käesolevas seaduses ja küberturvalisuse seaduses sätestatud pädevuse piires.";

7)paragrahv 170^2 tunnistatakse kehtetuks;

8)paragrahvi 188 lõige 8 muudetakse ja sõnastatakse järgmiselt:

„(8) Käesoleva seaduse §-s 170^1 sätestatud väärteo kohtuväline menetleja on Riigi Infosüsteemi Amet.".

§ 23. Hädaolukorra seaduse muutmine

Hädaolukorra seaduses tehakse järgmised muudatused:

1)paragrahvi 41 lõige 1 muudetakse ja sõnastatakse järgmiselt:

„(1) Elutähtsa teenuse osutaja peab elutähtsa teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

2)paragrahvi 41 lõige 3 tunnistatakse kehtetuks;

3)paragrahvi 41 lõige 4 tunnistatakse kehtetuks;

4)paragrahvi 45 lõike 1 punkt 4 muudetakse ja sõnastatakse järgmiselt:

„4) riiklikku ja haldusjärelevalvet käesoleva seaduse § 41 nõuete täitmise üle teeb Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”;

5)paragrahv 50 ja § 52 lõige 2 tunnistatakse kehtetuks.

§ 24. Krediidiasutuste seaduse muutmine

Krediidiasutuste seaduse § 88 täiendatakse lõikega 4^3järgmises sõnastuses:

„(4^3) Krediidiasutusel on õigus avaldada pangasaladust Riigi Infosüsteemi Ametile küberturvalisuse seaduses sätestatud riikliku järelevalve tegemisel.”.

§ 25. Lennundusseaduse muutmine

Lennundusseaduses tehakse järgmised muudatused:

1)paragrahv 59^1muudetakse ja sõnastatakse järgmiselt:

„**§ 59^1. Süsteemi turvalisuse tagamine**

Lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

2)paragrahvi 60^1lõige 5 muudetakse ja sõnastatakse järgmiselt:

„(5) Riiklikku järelevalvet käesoleva seaduse § 59^1nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”;

3)paragrahvi 60^2lõige 1^2, § 60^3lõige 7 ja § 60^{44}tunnistatakse kehtetuks.

§ 26. Raudteeseaduse muutmine

Raudteeseaduses tehakse järgmised muudatused:

1)paragrahvi 4 lõige 1^1muudetakse ja sõnastatakse järgmiselt:

„(1^1) Raudtee-ettevõtja, kes majandab avalikku raudteeinfrastruktuuri või kelle kaubaveo või reisijateveo turuosa on vähemalt 20 protsenti kaubaveo või reisijateveo turuosast, peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

2)paragrahvi 71 lõige 7^1muudetakse ja sõnastatakse järgmiselt:

„(7^1) Riiklikku järelevalvet käesoleva seaduse § 4 lõike 1^1nõuete täitmise üle teeb Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”;

3)paragrahvi 72 lõige 2, § 73 lõige 3, § 79^1ja § 111 lõige 4^1tunnistatakse kehtetuks.

§ 27. Sadamaseaduse muutmine

Sadamaseaduses tehakse järgmised muudatused:

1)paragrahvi 13 lõige 4 muudetakse ja sõnastatakse järgmiselt:

„(4) Sadamateenuse osutaja, kes teenindab käesoleva paragrahvi lõigetes 1 ja 2 nimetatud laevu, peab teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

2)paragrahvi 42 lõige 5 muudetakse ja sõnastatakse järgmiselt:

„(5) Riiklikku järelevalvet käesoleva seaduse § 13 lõike 4 nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”;

3)paragrahvi 43 lõige 2, § 44 lõige 2, § 48[1]ja § 57 lõige 1[1]tunnistatakse kehtetuks.

§ 28. Tervishoiuteenuste korraldamise seaduse muutmine

Tervishoiuteenuste korraldamise seaduses tehakse järgmised muudatused:

1)paragrahvi 10 senine tekst loetakse lõikeks 1 ja paragrahvi täiendatakse lõikega 2 järgmises sõnastuses:

„(2) Perearst peab üldarstiabi osutamisel kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

2)paragrahvi 17 täiendatakse lõikega 1[2]järgmises sõnastuses:

„(1[2]) Kiirabibrigaadi pidaja peab kiirabi osutamisel kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

3)paragrahvi 22 täiendatakse lõikega 4[2]järgmises sõnastuses:

„(4[2]) Käesoleva seaduse § 55 lõike 1 alusel kehtestatud haiglavõrgu piirkondliku haigla ja keskhaigla pidaja peab statsionaarse eriarstiabi osutamisel võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid.”;

4)paragrahvi 60 täiendatakse lõikega 2 järgmises sõnastuses:

„(2) Riiklikku järelevalvet käesoleva seaduse § 17 lõike 1[2]ja § 22 lõike 4[2]nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”;

5)paragrahvi 60 lõige 2 muudetakse ja sõnastatakse järgmiselt:

„(2) Riiklikku järelevalvet käesoleva seaduse § 10 lõike 2, § 17 lõike 1[2]ja § 22 lõike 4[2]nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seaduses sätestatud pädevuse piires.”.

§ 29. Seaduse jõustumine

(1) Käesolev seadus jõustub Riigi Teatajas avaldamisele järgneval päeval.

(2) Käesoleva seaduse § 3 lõike 1 punkt 8, § 3 lõige 3, § 9 ning § 23 punkt 3 jõustuvad 2020. aasta 1. jaanuaril.

(3) Käesoleva seaduse § 3 lõike 1 punktid 7 ja 10, § 21 ning § 28 punktid 1 ja 5 jõustuvad 2022. aasta 1. jaanuaril.

[1]Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.07.2016, lk 1–30).

Eiki Nestor
Riigikogu esimees