EELNÕU
26.09.2017

Küberturvalisuse seadus[1]

1. peatükk
Üldsätted

§ 1. Seaduse reguleerimisala

(1) Käesolev seadus sätestab nõuded riigi ja ühiskonna toimimise seisukohast oluliste võrgu- ja infosüsteemide pidamisele, küberintsidentide ennetamise ja lahendamise alused ning järelevalve seaduses sätestatud kohustuste täitmise üle.

(2) Käesolevat seadust ei kohaldata riigisaladuse või salastatud välisteabe töötlemisele riigisaladuse ja salastatud välisteabe seaduse tähenduses.

(3) Kui nõuded võrgu- ja infosüsteemi pidamisele on reguleeritud välislepingus, muus seaduses või selle alusel kehtestatud õigusaktis, kohaldatakse asjaomases välislepingus, seaduses või muus õigusaktis sätestatud nõudeid.

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

§ 2. Mõisted

Käesolevas seaduses kasutatakse mõisteid 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 automatiseeritud töötlemine, või digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse eelnimetatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks;
2) süsteemi turvalisus – süsteemi vastupanuvõime mis tahes tegevusele, mis ohustab süsteemis töödeldavate andmete või süsteemi kaudu osutatavate või juurdepääsetavate teenuste käideldavust, autentsust, terviklust ja konfidentsiaalust;
3) infovara – informatsioon, andmed ja nende töötlemiseks vajalik tarkvara, vajalikud tehnilised rakendused ning muud vahendid;
4) küberintsident –süsteemis toimuv sündmus, mis kahjustab süsteemi turvalisust;
5) 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 CSIRT (*Computer security incident response team*) pöörduda digitaalse teenuse osutaja asemel seoses digitaalse teenuse osutaja käesolevast seadusest tulenevate kohustustega;
6) internetipõhine kauplemiskoht – infoühiskonna teenus, mis võimaldab tarbijakaitseseaduse tähenduses tarbijal ja kauplejal sõlmida internetipõhine müügi- või teenuse osutamise leping kas internetipõhise kauplemiskoha veebisaidil või kaupleja veebisaidil, mis kasutab internetipõhise kauplemiskoha pakutavat andmetöötlusteenust;
7) internetipõhine otsingumootoriteenus – infoühiskonna teenus, mis võimaldab kasutajal teha otsingut üldjuhul kõikidel veebisaitidel või konkreetses keeles veebisaitidel mis tahes teemal

[1] 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).

võtmesõna, fraasi või muu sisendi vormis päringu alusel, ning saadab vastuseks lingid, kust võib leida teavet taotletud sisu kohta;
8) pilvandmetöötlusteenus – infoühiskonna teenus, mis võimaldab juurdepääsu skaleeritavale ja paindlikule jagatavale andmetöötlusressursside kogumile;
9) CSIRT – ekspertide grupp, kelle ülesandeks on küberintsidendi tuvastamist, analüüsimist ja ohjeldamist ning küberintsidendile reageerimist toetavad toimingud, sealjuures Eestis täidab riikliku CSIRT-i ülesandeid Riigi Infosüsteemi Amet.

§ 3. Teenuse osutaja

(1) Teenuse osutaja käesoleva seaduse tähenduses on:
1) hädaolukorra seaduses sätestatud elutähtsa teenuse osutaja elutähtsa teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
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 majandamise toimimise ja raudteeveo ning avaliku reisijateveo toimimise teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
3) lennundusseaduses sätestatud lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja lennuvälja toimimise ja aeronavigatsiooniteenuse toimimise teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
4) sadamaseaduses sätestatud sadam, mis teenindab rahvusvahelises meresõidus sõitvaid reisilaevu või 500 ja enama kogumahutavusega laevu, ja sadam, mis teenindab meresõiduohutuse seaduse kohaselt määratletud kohalikus rannasõidus sõitvaid I kategooria laevu või A-klassi reisilaevu sadamate toimimise ja laevaliikluse korraldamise süsteemi toimimise teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
5) elektroonilise side seaduses sätestatud sideettevõtja, kes osutab kaabelleviteenust, mida tarbib vähemalt 10 000 lõppkasutajat, ja ringhäälinguvõrgu teenuse osutaja kaabelleviteenuse või ringhäälinguvõrgu teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
6) tervishoiuteenuste korraldamise seaduses sätestatud piirkondlik haigla ja keskhaigla pidaja statsionaarse eriarstiabi osutamiseks ning perearst üldarstiabi teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara osas;
7) Eesti maatunnusega seotud tipptaseme domeeninimede registri haldaja registri pidamiseks kasutatava süsteemi ja sellega seotud infovara osas.
8) Eesti Rahvusringhääling Eesti rahvusringhäälingu seaduse § 5 lõige 1 punktis 10 sätestatud ülesannete täitmiseks kasutatavate infosüsteemide ja nendega seotud infovarade osas;
9) kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja elektroonilise side seaduse tähenduses nende teenuste osutamiseks kasutatavate infosüsteemide ja nendega seotud infovarade osas.

(2) Teenuse osutajat, kes tegutseb Euroopa parlamendi ja nõukogu direktiivi (EL) nr 2016/1148 II lisas esitatud sektorites loetakse olulise teenuse operaatoriks vastava direktiivi tähenduses.

(3) Riigi Infosüsteemi Amet identifitseerib hiljemalt 9. novembriks 2018. a seaduse kohaldamisalas olevad teenuse osutajad, kes tegutsevad Euroopa parlamendi ja nõukogu direktiivi (EL) nr 2016/1148 II lisas esitatud sektorites.

§ 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) osutab internetipõhist otsingumootoriteenust või
3) osutab pilvandmetöötlusteenust.

(2) Käesolevat seadust ei kohaldata digitaalse teenuse osutajale, kes on mikro- või väikeettevõtja raamatupidamise seaduse § 3 punktide 14 ja 15 tähenduses.

§ 5. Ühtne kontaktpunkt ja pädev asutus

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) artikli 8 lõikes 1 nimetatud pädeva asutuse ja lõikes 3 nimetatud ühtse kontaktpunkti ülesandeid täidab Riigi Infosüsteemi Amet.

§ 6. Küberturvalisuse tagamise põhimõtted

Küberturvalisuse tagamisel arvestatakse järgmisi põhimõtteid:
1) isiklikkuse põhimõte – süsteemi ja sellega seotud infovara turvalisuse tagamist korraldab selle haldaja;
2) tervikliku kaitse põhimõte – süsteemi haldaja teeb kindlaks võimalikud ohud süsteemile ja sellega seotud infovarale ning rakendab süsteemi kaitseks kohaseid korralduslikke ja tehnilisi abinõusid;
3) kahjuliku mõju vähendamise põhimõte – süsteemi haldaja rakendab küberintsidendi korral vajalikku hoolsust ja abinõusid, et vältida küberintsidendi mõju laienemist ja võimalikku levimist teisele süsteemile, ning teavitab küberintsidendist käesolevas seaduses sätestatud järelevalveasutust;
4) koostööpõhimõte – küberturvalisuse tagamisel ja küberintsidentide lahendamisel teevad osalised koostööd ja võtavad vajadusel arvesse süsteemide ja teenuste omavahelist seotust ning sõltuvust;
5) põhiõiguste kaitse põhimõte – küberturvalisuse tagamisel kindlustatakse põhiõiguste ja -vabaduste ning isikuandmete ja identiteedi kaitse.

2. peatükk
Kohustused küberturvalisuse tagamisel

§ 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 süsteemile ja sellega seotud infovarale avalduva mõju leevendamiseks või teise sõltuva teenuse toimepidevusele või süsteemile ja sellega seotud infovarale avalduva mõju ennetamiseks.

(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:
1) viima läbi süsteemi ja sellega seotud infovara riskide hindamise;
2) tagama dokumenteeritud turvaeeskirjade ja turvameetmete rakendamise kirjelduse olemasolu ja ajakohasuse;

3) tagama süsteemi turvalisust ohustava tegevuse või tarkvara tuvastamiseks süsteemi seire, mis võimaldab küberintsidendi ennetamist ja toimunud küberintsidendi tekkepõhjuste väljaselgitamist, ning edastama teabe süsteemi ohustava tegevuse või tarkvara kohta Riigi Infosüsteemi Ametile;
4) piirama süsteemi kasutamist või juurdepääsu juhul, kui see on vajalik küberintsidendi leviku vältimiseks ühelt süsteemilt teisele süsteemile või süsteemi turvalisuse taastamiseks;
5) kontrollima turvameetmete rakendamise piisavust ja vastavust ning dokumenteerima kontrolli tulemused;
6) säilitama punktis 5 sätestatud dokumentatsiooni vähemalt kolm aastat alates dokumendi loomisest.

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

(4) Teenuse osutamiseks kasutatava süsteemi ja sellega seotud infovara turvameetmete kirjelduse kehtestab Vabariigi Valitsus määrusega.

§ 8. Teenuse osutaja küberintsidendist teavitamine

(1) Teenuse osutaja teavitab Riigi Infosüsteemi Ametit olulise mõjuga küberintsidendist viivitamata, kuid mitte hiljem kui 24 tunni jooksul küberintsidendist teada saamisest arvates.

(2) Teenuse osutaja on kohustatud teavitama isikut, keda küberintsident võib mõjutada.

(3) Kui teenuse osutaja ei täida käesoleva paragrahvi lõikes 2 sätestatud teavitamiskohustust mõistliku aja jooksul, võib Riigi Infosüsteemi Amet mõjutatud isikut või isikuid ise teavitada.

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

(5) Kui küberintsident põhjustab isikuandmetega seotud rikkumise, teavitab Riigi Infosüsteemi Amet küberintsidendist Andmekaitse Inspektsiooni.

(6) Küberintsidendist teavitamise ja raporti esitamise korra ning olulise mõjuga küberintsidendi kriteeriumid kehtestab Vabariigi Valitsus määrusega.

(7) Teenuse osutaja on kohustatud teavitama Riigi Infosüsteemi Ametit digitaalse teenuse osutajat puudutavast küberintsidendist, kui tema teenus sõltub käesoleva seaduse §-s 4 määratletud digitaalse teenuse osutaja teenusest ning küberintsident mõjutab teenuse toimepidevust.

§ 9. Riigi ja kohaliku omavalitsuse üksuse süsteemi turvanõuded

(1) Käesoleva seaduse § 7 lõigetes 1–3 sätestatud kohustusi ning käesoleva seaduse §-s 8 sätestatud küberintsidendist teavitamise nõudeid kohaldatakse riigi- ja kohaliku omavalitsuse üksusele avalike ülesannete täitmiseks kasutatava süsteemi haldamisel.

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

§ 10. Digitaalse teenuse osutaja süsteemi turvameetmed

(1) Digitaalse teenuse osutaja on kohustatud tegema kindlaks ja analüüsima riske, mis ohustavad süsteemi turvalisust, 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) vastavust rahvusvahelistele standarditele.

(3) Käesoleva paragrahvi lõike 2 rakendamisel on digitaalse teenuse osutaja kohustatud juhinduma Euroopa Komisjoni rakendusmäärusest xxx/2017.

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

§ 11. Digitaalse teenuse osutaja küberintsidendist teavitamine

(1) Digitaalse teenuse osutaja teavitab pädevat asutust või CSIRT-i küberintsidendist, millel on oluline mõju osutatavale digitaalsele teenusele, viivitamata pärast küberintsidendist teada saamist.

(2) Teade tuleb esitada selle liikmesriigi pädevale asutusele või CSIRT-ile, kus on:
1) digitaalse teenuse osutaja asutatud;
2) kontserni puhul asutatud kontserni emaettevõtja või;
3) kolmandast riigist pärit ettevõtja määranud esindaja.

(3) Küberintsidendist teavitamisel lähtutakse Euroopa Komisjoni rakendusmääruses xxx/2017 sätestatud kriteeriumitest.

(4) Teade peab sisaldama teavet, mis võimaldab pädeval asutusel või CSIRT-il kindlaks teha küberintsidendi piiriülene mõju.

(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, käimasoleva küberintsidendi lahendamiseks või muul viisil avalikes huvides on vajalik avalikkuse teavitamine, võib Riigi Infosüsteemi Amet pärast digitaalse teenuse osutaja informeerimist teavitada küberintsidendist avalikkust või kohustada selleks digitaalse teenuse osutajat.

(7) Käesoleva paragrahvi lõiget 1 ei kohaldata, kui digitaalse teenuse osutajal puudub teave, et tuvastada küberintsidendi mõju olulisust.

§ 12. Kolmandas riigis asutatud digitaalse teenuse osutaja

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 esindaja kontaktandmed vahetult ja püsivalt kättesaadavaks.

3. peatükk
Riiklik küberturvalisuse tagamine

§ 13. Küberintsidendi ennetus ja lahendamine

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

(2) Riigi Infosüsteemi Amet teostab küberintsidendi ennetamiseks seiret, analüüsib süsteemide turvalisust ohustavaid riske ning nende mõju riigi ja ühiskonna toimepidevusele.

(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, Euroopa Võrgu- ja Infoturbe Agentuurile või muule organisatsioonile edastada küberintsidendi ennetamise ja lahendamisega seotud teavet käesolevas seaduses sätestatud ülesannete või Euroopa Liidu õigusest tuleneva kohustuse täitmiseks või välislepinguga ettenähtud juhtudel ja korras.

(5) Riigi Infosüsteemi Amet kaitseb teabe edastamisel teabe konfidentsiaalsust ning arvestab teenuse osutaja või digitaalse teenuse osutaja turvalisuse ja ärihuvidega.

§ 14. 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 läbiviimise toetamiseks.

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

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

4. peatükk
Riiklik ja haldusjärelevalve

§ 15. Riikliku ja haldusjärelevalve teostamine

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

(2) Riiklikku järelevalvet digitaalse teenuse osutaja käesoleva seaduse §-des 10 ja 11 sätestatud nõuete täitmise üle teostatakse juhul, kui Riigi Infosüsteemi Ametit teavitatakse, et digitaalse teenuse osutaja ei täida käesoleva seaduse §-des 10 ja 11 kehtestatud nõudeid:
1) teenuse osutaja suhtes, kes on asutatud Eestis;

2) kontserni kuuluva teenuse osutaja suhtes vaid juhul, kui tema emaettevõtja on asutatud Eestis;
3) kolmanda riigi digitaalse teenuse osutaja suhtes, kellel on Eestis esindaja.

§ 16. Riikliku järelevalve erimeetmed

(1) Korrakaitseorgan võib käesolevas seaduses sätestatud riikliku järelevalve teostamiseks 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 täitmise üle riikliku järelevalve teostamisel võib korrakaitseorgan kohaldada lisaks käesoleva paragrahvi lõikes 1 nimetatud erimeetmetele korrakaitseseaduse §-s 52 sätestatud riikliku järelevalve erimeedet korrakaitseseaduses sätestatud alusel ja korras.

§ 17. Küberintsidendi tõkestamine

(1) Riikliku järelevalve teostamisel võib Riigi Infosüsteemi Amet süsteemi juhtimise vahetult või kaughalduse teel üle võtta ning küberintsidendist põhjustatud kõrgendatud ohu väljaselgitamiseks või tõrjumiseks süsteemi kasutamist või süsteemile juurdepääsu piirata.

(2) Käesoleva paragrahvi lõikes 1 sätestatud meedet võib kohaldada üksnes juhul, kui:
1) küberintsident ohustab teise süsteemi turvalisust või avalikku korda;
2) süsteemi haldaja ei saa õigel ajal küberintsidenti lahendada;
3) küberintsidenti ei saa tõkestada või ohtu tõrjuda muu, vähem riivava meetmega;
4) küberintsidendi tõkestamisega ei tekitata ebaproportsionaalselt suurt kahju süsteemi haldaja varale või süsteemi kasutajatele.

(3) Käesolevas paragrahvis sätestatud meetme kohaldamisest tuleb süsteemi haldajat esimesel võimalusel teavitada.

(4) Käesolevas paragrahvis sätestatud meetme protokollimine on kohustuslik.

(5) Käesoleva paragrahvi lõikes 1 sätestatud meetme kohaldamise otsustab Riigi Infosüsteemi Ameti peadirektor.

§ 18. Haldusjärelevalve teostamine

(1) Haldusjärelevalve teostamiseks on Riigi Infosüsteemi Ameti pädeval ametiisikul õigus saada juurdepääs süsteemile, andmetöötluseks kasutatavale tarkvarale ning kontrollida infovara kasutamist.

(2) Riigi Infosüsteemi Ameti pädev ametiisik võib süsteemi juhtimise vahetult või kaughalduse teel üle võtta ning küberintsidendi asjaolude väljaselgitamiseks või küberintsidendi tõrjumiseks süsteemi kasutamist või juurdepääsu süsteemile piirata, kui:
1) küberintsident ohustab teise isiku süsteemi turvalisust või avaliku ülesande täitmist;
2) küberintsidenti ei ole võimalik muu meetmega tõkestada;
3) küberintsidendi tõkestamisega ei tekitata ebaproportsionaalselt suurt kahju süsteemi haldaja ülesannete täitmisele või süsteemi kasutajatele.

(4) Käesoleva paragrahvi lõikes 2 sätestatud meetme kohaldamisest tuleb süsteemi haldajat esimesel võimalusel teavitada.

(5) Käesolevas paragrahvi lõikes 2 sätestatud meetme protokollimine on kohustuslik.

(6) Käesoleva paragrahvi lõikes 2 sätestatud meetme kohaldamise otsustab Riigi Infosüsteemi Ameti peadirektor.

5. peatükk
Vastutus

§ 19. 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.

§ 20. Menetlus

Käesoleva seaduse §-s 19 sätestatud väärteo kohtuväline menetleja on Riigi Infosüsteemi Amet.

6. peatükk
Rakendussätted

§ 21. 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 küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

2) paragrahvi 41 lõiked 3 ja 4 tunnistatakse kehtetuks;

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

„4) riiklikku järelevalvet käesoleva seaduse § 41 lõike 1 nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seadusega sätestatud pädevuse piires.“;

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

§ 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, ja ringhäälinguvõrgu teenust, kohaldatakse käesoleva paragrahvi

lõigetes 1–5 sätestatud nõuete asemel küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud õigusaktis sätestatud nõudeid.“;

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

„(3) Kriitilise tähtsusega sideteenuse osutaja peab teenuse osutamiseks kasutatava küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 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 küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 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 küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 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) internetiseansi alguse ja lõpu kuupäeva ning kellaaja konkreetse ajavööndi järgi koos internetiprotokolli aadressiga, mille andmeside teenuse osutaja on seadmele eraldanud;
2) seadme internetiprotokolli aadressi protokolli ja pordi numbriga, mis sisaldab seadmesse liikuvate pakettide sihtporti ja vastuspakettide lähteporti.“;

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. Lennundusseaduse muutmine

Lennundusseaduses tehakse järgmised muudatused:

1) paragrahv 59^1 muudetakse ja sõnastatakse järgmiselt:

„**§ 59[1]. Süsteemi ja sellega seotud infovara turvalisuse tagamine**

Lennuvälja käitaja, kelle käitatav lennuväli on avatud rahvusvaheliseks regulaarseks lennuliikluseks, samuti Tallinna lennuinfopiirkonnas lennuliikluse teenindamist tagav aeronavigatsiooniteenuse osutaja, peab teenuse osutamiseks kasutatava küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

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

„(5) Riiklikku järelevalvet käesoleva seaduse § 59[1] nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seadusega sätestatud pädevuse piires.“;

3) paragrahvi 60[2] lõige 1[2] tunnistatakse kehtetuks;

4) paragrahvi 60[3] lõige 7 tunnistatakse kehtetuks;

5) paragrahv 60[44] ja paragrahvi 60[45] lõige 3 tunnistatakse kehtetuks.

§ 24. Raudteeseaduse muutmine

Raudteeseaduses tehakse järgmised muudatused:

1) paragrahvi 4 lõige 1[1] muudetakse 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 küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

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

„(7[1]) Riiklikku järelevalvet käesoleva seaduse § 4 lõike 1[1] nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seadusega sätestatud pädevuse piires.“;

3) paragrahvi 72 lõige 2 tunnistatakse kehtetuks;

4) paragrahvi 73 lõige 3 tunnistatakse kehtetuks;

5) paragrahv 79[1] ja paragrahvi 111 lõige 4[1] tunnistatakse kehtetuks.

§ 25. Sadamaseaduse muutmine

Sadamaseaduses tehakse järgmised muudatused:

1) paragrahvi 13 lõige 4 muudetakse ja sõnastatakse järgmiselt:

„(4) Sadam, mis teenindab käesoleva paragrahvi lõigetes 1 ja 2 nimetatud laevu, peab teenuse osutamiseks kasutatava küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara

turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 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 seadusega sätestatud pädevuse piires.“;

3) paragrahvi 43 lõige 2 tunnistatakse kehtetuks;

4) paragrahvi 44 lõige 2 tunnistatakse kehtetuks;

5) paragrahvi § 48^1 tunnistatakse kehtetuks;

6) paragrahv 57 lõige 1^1 tunnistatakse kehtetuks.

§ 26. Tervishoiuteenuste korraldamise seaduse muutmine

Tervishoiuteenuste korraldamise seaduses tehakse järgmised muudatused:

1) paragrahv 10 muudetakse ja sõnastatakse järgmiselt:

„**§ 10. Nõuded perearsti tegevuskoha ruumidele, sisseseadele ja elektroonilisele turvalisusele**

(1**)** Perearsti tegevuskoha ruumidele, sisseseadele ja aparatuurile esitatavad nõuded kehtestab valdkonna eest vastutav minister.

(2) Perearst peab üldarstiabi osutamisel teenuse osutamiseks kasutatava küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

2) 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 teenuse osutamiseks kasutatava küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

3) paragrahvi 60 täiendatakse lõikega 2 järgmises sõnastuses:

„(2) Riiklikku järelevalvet käesoleva seaduse § 22 lõike 4^2 ja § 10 lõike 2 nõuete täitmise üle teostab Riigi Infosüsteemi Amet küberturvalisuse seadusega sätestatud pädevuse piires.“;

4) paragrahvi 73 täiendatakse lõikega 4 järgmises sõnastuses:

„(4) Käesoleva seaduse § 10 lg 2 jõustub 2020. a 1. jaanuaril.“.

§ 27. Eesti Rahvusringhäälingu seaduse muutmine

Eesti Rahvusringhäälingu seaduses tehakse järgmised muudatused:

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

„(2^1) Rahvusringhääling on kohustatud lõike 1 punktis 10 sätestatud ülesande täitmiseks kasutatava ning küberturvalisuse seaduse mõistes süsteemi ja sellega seotud infovara turvalisuse tagamiseks täitma küberturvalisuse seaduse §-des 7 ja 8 ning nende alusel kehtestatud nõudeid.“;

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

(4^1) Käesoleva seaduse § 8 lõikes 5 sätestatud nõuete täitmise üle teostab järelevalvet Riigi Infosüsteemi Amet küberturvalisuse seadusega sätestatud pädevuse piires.“.

§ 28. Krediidiasutuste seaduse muutmine

Krediidiasutuste seaduses tehakse järgmised muudatused:

1) paragrahvi 88 täiendatakse lõikega 4^3 järgmises sõnastuses:
„(4^3) Krediidiasutusel on õigus avaldada pangasaladust Riigi Infosüsteemi Ametile küberturvalisuse seaduses sätestatud riikliku järelevalve teotamisel.“.

§ 29. Seaduse jõustumine

(1) Käesolev seadus jõustub 2018. a 10. mail.

(2) Käesoleva seaduse § 9 jõustub 2020. a 1. jaanuaril.

Eiki Nestor
Riigikogu esimees

Tallinn 2017

Algatab Vabariigi Valitsus