PATVIRTINTA
Lietuvos Respublikos Vyriausybės
nutarimu Nr.

ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ KIBERNETINIO SAUGUMO SUBJEKTAMS, APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas (toliau – Aprašas) nustato organizacinius ir techninius kibernetinio saugumo reikalavimus (toliau kartu – Reikalavimai) kibernetinio saugumo subjektams.

2. Reikalavimai gali būti taikomi kaip rekomendaciniai įslaptintą informaciją apdorojančioms, perduodančioms ir saugančioms įslaptintos informacijos ryšių ir informacinėms sistemoms, kiek tai neprieštarauja Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme ir kituose atitinkamuose teisės aktuose tokioms ryšių ir informacinėms sistemoms nustatytiems reikalavimams.

3. Šiame Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme ir Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“.

II SKYRIUS
KIBERNETINIO SAUGUMO SUBJEKTŲ RYŠIŲ IR INFORMACINIŲ SISTEMŲ RIZIKOS VERTINIMAS

4. Kibernetinio saugumo subjektų ryšių ir informacinių sistemų kibernetinio saugumo organizacinių ir techninių priemonių užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus. Kibernetinio saugumo subjektai, organizuodami ryšių ir informacinių sistemų rizikos vertinimą:

4.1. paskiria už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą atsakingą asmenį arba asmenis ir nustato jiems taikomus kvalifikacinius reikalavimus;

4.2. nustato reikalavimus rizikos vertinimo procesui, rizikos išdėstymo pagal prioritetus kriterijus ir priimtiną rizikos lygį;

4.3. nustato grėsmes ir pažeidžiamumus, galinčius turėti įtakos ryšių ir informacinių sistemų kibernetiniam saugumui, ir nustato galimo grėsmių ir pažeidžiamumų poveikio vykdomai veiklai sritis;

4.4. įvertina ryšių ir informacinių sistemų pažeidimo grėsmių tikimybę ir pasekmes, nustato rizikos lygį, įvertina identifikuotas grėsmių tikimybes ir jas išdėsto prioriteto tvarka;

4.5. Aprašo nustatyta tvarka, atsižvelgdamas į atliktą rizikos vertinimą, rengia ir (ar) peržiūri patvirtintus teisės aktus, reglamentuojančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo politiką ir jos įgyvendinimą (toliau – kibernetinio saugumo dokumentai), viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles ar paslaugų kibernetinio saugumo valdymo taisykles ir nustato, kuriuos iš juose nustatytų kibernetinio saugumo reikalavimų būtina atnaujinti ir (ar) įgyvendinti pirmiausia, siekiant užtikrinti ryšių ir informacinių sistemų kibernetinį saugumą.

5. Organizuojant ryšių ir informacinių sistemų rizikos vertinimą, rekomenduojama vadovautis Lietuvos ir tarptautiniais standartais ar metodikomis, reglamentuojančiais rizikos valdymą, ir įtraukti ryšių ir informacinių sistemų rizikos vertinimą į veiklos rizikos vertinimo procesus.

III SKYRIUS
ORGANIZACINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS

6. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai:

6.1. ne rečiau kaip kartą per metus arba po esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ir ypatingos svarbos informacinės infrastruktūros valdytojai turi teisę atlikti kartu su valstybės informacinių išteklių rizikos ar ypatingos svarbos informacinės infrastruktūros rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu;

6.2. atsižvelgdami į atlikto rizikos vertinimo rezultatus ir jeigu nustatoma incidentų valdymo ir šalinimo, taip pat organizacijos nepertraukiamos veiklos užtikrinimo trūkumų, tobulina veiklos tęstinumo valdymo planus ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus. Veiklos tęstinumo valdymo planų ar kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų veikimo bandymų rezultatai išdėstomi šių planų bandymo ataskaitose, kurių kopijos ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo pateikiamos Nacionaliniam kibernetinio saugumo centrui;

6.3. suderinę su Nacionaliniu kibernetinio saugumo centru, tvirtina kibernetinio saugumo dokumentus, kuriuose turi būti nustatyta:

6.3.1. kibernetinio saugumo dokumentų taikymas ir naudojimas;

6.3.2. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų grupių sudarymas, teisių ir prieigos prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros paslaugų ir išteklių suteikimas ir valdymas;

6.3.3. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų pareigos ir funkcijos, susijusios su kibernetiniu saugumu;

6.3.4. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, mokymai kibernetinio saugumo klausimais;

6.3.5. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų vardų ir slaptažodžių sudarymas, apsauga ir keitimas;

6.3.6. audito įrašų administravimas ir saugojimas;

6.3.7. įsibrovimų aptikimas ir prevencija;

6.3.8. saugus naudojimasis belaidžiu tinklu;

6.3.9. mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugus naudojimas ir kontrolė;

6.3.10. duomenų, esančių mobiliuosiuose įrenginiuose, šifravimo nuostatos;

6.3.11. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros išteklių naudojimas už organizacijos ribų ir (arba) mobiliaisiais įrenginiais;

6.3.12. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamų svetainių saugos valdymas;

6.3.13. grėsmių ir pažeidžiamumų, galinčių turėti įtakos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetiniam saugumui, vertinimas;

6.3.14. pažeidžiamumų nustatymo dalyvių teisės ir pareigos;

6.3.15. pažeidžiamumų nustatymo plano rengimas;

6.3.16. pažeidžiamumų nustatymo programinės įrangos naudojimas;

6.3.17. pažeidžiamumų nustatymo rezultatų klasifikavimas;

6.3.18. pažeidžiamumų nustatymo ataskaitų rengimas ir nustatytų trūkumų šalinimas;

6.3.19. kibernetinio incidento valdymo organizavimas;

6.3.20. kibernetinio incidento nustatymas;

6.3.21. kibernetinio incidento vertinimas;

6.3.22. kibernetinio incidento stabdymas ir šalinimas;

6.3.23. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įprastinės veiklos atkūrimas ir maksimalus leistinas paslaugos neveikimo laikas;

6.3.24. įgytos kibernetinių incidentų valdymo patirties vertinimas;

6.3.25. kibernetiniam saugumui užtikrinti naudojamų priemonių diegimo ir šių priemonių parametrų keitimas;

6.3.26. Reikalavimų įgyvendinimo kontrolės ir atitikties vertinimas;

6.3.27. valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros kibernetinio saugumo būklės gerinimas;

6.3.28. elektroninio pašto naudojimas.

7. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, Aprašo 6.3 papunkčio nuostatas turi teisę išdėstyti Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, nustatyta tvarka rengiamuose ir tvirtinamuose saugos dokumentuose. Šiuo atveju minėti saugos dokumentai derinami Bendrųjų elektroninės informacijos saugos reikalavimų aprašo nustatyta tvarka.

8. Išvadas, pastabas ir pasiūlymus dėl kibernetinio saugumo dokumentų projektų Nacionalinis kibernetinio saugumo centras turi pateikti per 10 darbo dienų, jeigu šie projektai didelės apimties (daugiau kaip 10 puslapių) – per 15 darbo dienų, o dėl pakartotinai pateiktų derinti projektų – per 5 darbo dienas nuo jų gavimo. Prieš pateikdamas išvadas, pastabas ir pasiūlymus dėl kibernetinio saugumo dokumentų projektų, Nacionalinis kibernetinio saugumo centras turi teisę paprašyti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo pateikti kitus valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros saugumą nustatančius dokumentus.

9. Kibernetinio saugumo dokumentai turi būti peržiūrimi (persvarstomi) ne rečiau kaip kartą per metus. Keičiami kibernetinio saugumo dokumentai su Nacionaliniu kibernetinio saugumo centru gali būti nederinami tais atvejais, kai atliekami tik redakciniai pakeitimai. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui pateikiamos šių dokumentų kopijos.

10. Ne rečiau kaip kartą per metus turi būti organizuojamas ir atliekamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros atitikties Reikalavimams vertinimas.

11. Ne rečiau kaip kartą per mėnesį turi būti atliekama valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų veiksmų audito įrašų analizė.

12. Ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir šalinamos pastebėtos neatitiktys saugumo reikalavimams.

13. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

14. Subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, pirkdami paslaugas, darbus ar įrangą, susijusius su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi nustatyti, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas užtikrina atitiktį Reikalavimams.

IV SKYRIUS
TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS

15. Techniniai kibernetinio saugumo reikalavimai subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius ir ypatingos svarbos informacinės infrastruktūros valdytojams nustatomi pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbą. Ypatingos svarbos informacinės infrastruktūra, valstybės informaciniai ištekliai, atitinkantys valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų kategorijas pagal Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“ pagal svarbą išdėstomi taip:

15.1. Ypatingos svarbos informacinės infrastruktūra (YSII);

15.2. pirma kategorija (I);

15.3. antra kategorija (II);

15.4. trečia kategorija (III);

15.5. ketvirta kategorija (IV).

16. Išsamus techninių kibernetinio saugumo reikalavimų sąrašas pateiktas Aprašo priede.

17. Kibernetinio saugumo priemonės, pateiktos Aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerąja saugumo praktikos rekomendacija.

V SKYRIUS
VIEŠŲJŲ RYŠIŲ TINKLŲ IR (ARBA) VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ PASLAUGŲ TEIKĖJŲ ORGANIZACINIAI IR TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

18. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai:

18.1. ne rečiau kaip kartą per 2 metus arba po esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos savo teikiamų viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu;

18.2. įgyvendina organizacines ir technines priemones, kurios užtikrintų, kad suklastotų interneto protokolo (IP) adresų srautas būtų blokuojamas jų teikiamuose viešuosiuose ryšių tinkluose;

18.3. įgyvendina organizacines ir technines priemones, kurios užtikrintų, kad elektroninių paslaugų trikdymo atakos srautas būtų blokuojamas jų teikiamuose viešuosiuose ryšių tinkluose;

18.4. įgyvendina organizacines ir technines priemones, kurios užtikrintų jų viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;

18.5. tvirtina ir, kai įvyksta esminių organizacinių ar sisteminių pokyčių, atnaujina savo viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisykles, o Nacionaliniam kibernetinio saugumo centrui pareikalavus, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Viešųjų ryšių tinklų ir (arba) viešųjų elektroninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:

18.5.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;

18.5.2. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;

18.5.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;

18.5.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;

18.5.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;

18.6. neatlygintinai informuoja viešųjų elektroninių ryšių paslaugų gavėjus apie priemones, kuriomis viešųjų elektroninių ryšių paslaugų gavėjai gali pasinaudoti kibernetinių incidentų grėsmei, susijusiai su viešųjų elektroninių ryšių paslaugų gavėjų galiniais įrenginiais, pašalinti, ir nurodo tikėtinas tokių priemonių panaudojimo išlaidas;

18.7. ne vėliau kaip prieš 5 darbo dienas informuoja viešųjų elektroninių ryšių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų kibernetinį saugumą;

18.8. viešai skelbia rekomendacijas viešųjų elektroninių ryšių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų paslaugomis.

VI SKYRIUS
ELEKTRONINĖS INFORMACIJOS PRIEGLOBOS PASLAUGŲ TEIKĖJŲ IR SKAITMENINIŲ PASLAUGŲ TEIKĖJŲ ORGANIZACINIAI IR TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

19. Elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai:

19.1. ne rečiau kaip kartą per 2 metus arba po to esminių organizacinių ar sisteminių pokyčių šio Aprašo II skyriuje nustatyta tvarka organizuoja ir atlieka grėsmių ir pažeidžiamumų, galinčių turėti įtakos savo teikiamų elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetiniam saugumui, rizikos vertinimą. Šį rizikos vertinimą elektroninės informacijos prieglobos paslaugų teikėjai ir skaitmeninių paslaugų teikėjai turi teisę atlikti kartu su veiklos rizikos vertinimu ir (arba) informacinių technologijų saugos atitikties vertinimu;

19.2. kartu su viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjais imasi reikiamų priemonių kibernetiniam saugumui užtikrinti;

19.3. įgyvendina organizacines ir technines priemones, kurios užtikrintų jų elektroninės informacijos prieglobos ar skaitmeninėms paslaugoms teikti naudojamų sistemų ir įrangos kibernetinį saugumą;

19.4. tvirtina ir, kai įvyksta esminių organizacinių ar sisteminių pokyčių, atnaujina savo paslaugų kibernetinio saugumo valdymo taisykles, o Nacionaliniam kibernetinio saugumo centrui pareikalavus, jas pateikia Nacionaliniam kibernetinio saugumo centrui. Elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų kibernetinio saugumo valdymo taisyklėse nurodoma:

19.4.1. kibernetiniams incidentams valdyti reikalingų priemonių aprašymai;

19.4.2. elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų nepertraukiamo teikimo užtikrinimo planas ir jo taikymo sąlygos bei maksimalus leistinas paslaugos neveikimo laikas;

19.4.3. už kibernetinių incidentų valdymą atsakingų asmenų funkcijos ir atsakomybė;

19.4.4. viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugoms teikti naudojamų sistemų ir įrangos stebėsenos, patikrinimo, testavimo bei auditavimo tvarka ir sąlygos;

19.4.5. atitiktis Lietuvos ir tarptautiniams standartams, apibūdinantiems kibernetinį saugumą ar saugų elektroninės informacijos tvarkymą;

19.5. neatlygintinai informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus apie nustatytus kibernetinius incidentus, susijusius su elektroninės

informacijos prieglobos ar skaitmeninėmis paslaugomis, priskirtus prie turinčių didelį poveikį, nustatytą Nacionaliniame kibernetinių incidentų valdymo plane;

19.6. ne vėliau kaip prieš 5 darbo dienas informuoja elektroninės informacijos prieglobos paslaugų ar skaitmeninių paslaugų gavėjus ir Nacionalinį kibernetinio saugumo centrą apie numatomus planinius darbus, kuriuos atliekant yra tikimybė sutrikdyti elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinį saugumą;

19.7. informuoja elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjus, kuriose šalyse gali būti saugoma jų elektroninė informacija, kuri yra kuriama, tvarkoma ar pateikta saugoti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis, ir kokiais atvejais tokia informacija perkeliama į kitas šalis;

19.8. nustato elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjų įspėjimo apie elektroninės informacijos prieglobos ar skaitmeninių paslaugų kibernetinio saugumo pažeidimus tvarką ir kokių veiksmų tokiu atveju privalo imtis elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjai ir (ar) teikėjai;

19.9. viešai skelbia rekomendacijas elektroninės informacijos prieglobos ar skaitmeninių paslaugų gavėjams apie priemones kibernetiniam saugumui užtikrinti naudojantis elektroninės informacijos prieglobos ar skaitmeninėmis paslaugomis.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

20. Kibernetinio saugumo subjektai turi teisę nusistatyti ir taikyti papildomus Reikalavimus. Jeigu papildomais Reikalavimais nustatomos techninės ir organizacinės kibernetinio saugumo priemonės yra lygiavertės ir apima šiame Apraše nustatytus Reikalavimus, kibernetinio saugumo subjektai turi teisę taikyti tik papildomus Reikalavimus.

21. Kibernetinio saugumo subjektai, išskyrus skaitmeninių paslaugų teikėjus, teikia Nacionaliniam kibernetinio saugumo centrui techninę informaciją, reikalingą jų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti. Informacija teikiama:

21.1. Nacionaliniam kibernetinio saugumo centrui pareikalavus, jo nurodytais formatais ir terminais;

21.2. kibernetinių subjektų iniciatyva.

22. Nacionalinis kibernetinio saugumo centras kibernetinio saugumo subjektų pateiktą informaciją apie kibernetinio saugumo būklę, įskaitant ir konfidencialią informaciją, turi teisę tvarkyti tik tiek, kiek tai yra būtina kibernetinio saugumo subjektų valdomų ryšių ir informacinių sistemų kibernetiniam saugumui įvertinti.

23. Diegiant technines kibernetinio saugumo priemones viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams, elektroninės informacijos prieglobos paslaugų teikėjams ir skaitmeninių paslaugų teikėjams rekomenduojama vadovautis Aprašo priede pateiktu techninių kibernetinio saugumo reikalavimų sąrašu.

KAM Administracijos departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Lietuvos Respublikos
vidaus reikalų ministras
Eimutis Misiūnas
2018-11-06

Krašto apsaugos viceministras
Edvinas Kerza

Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo priedas

TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS, SĄRAŠAS

Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
1. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros priežiūrą vykdančio asmens (toliau – administratorius) funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo funkcijoms atlikti	x	x	x	x	x
2. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojams negali būti suteikiamos administratoriaus teisės	x	x	x	x	x
3. Kiekvienas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas turi būti unikaliai atpažįstamas (asmens kodas negali būti naudojamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui atpažinti)	x	x	x	x	x
4. Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *virtual private network*)	x	x	x	x	x
5. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone	x	x	x	x	x
6. Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x		
7. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo teisė dirbti su konkrečiu valstybės informaciniu ištekliu ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip 3 mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x
8. Administratoriaus teisė dirbti su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai administratorius nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip 2 mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x

9. Kai įstatymų nustatytais atvejais valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti panaikinta nedelsiant	x	x	x	x	x
10. Nereikalingos ar nenaudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų ir administratoriaus paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų nustatytam saugojimo terminui	x	x	x	x	x
11. Baigus darbą arba valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje, negalėtų susipažinti pašaliniai asmenys: turi būti atsijungiama nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, įjungiama ekrano užsklanda su slaptažodžiu (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x
12. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje neatliekant jokių veiksmų, darbo stotis turi užsirakinti, kad toliau naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra būtų galima tik pakartotinai patvirtinus savo tapatybę (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Laikas, per kurį valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui neatliekant jokių veiksmų darbo stotis užsirakina, nustatomas kibernetinio saugumo dokumentuose, tačiau negali būti ilgesnis kaip 15 minučių. Šis reikalavimas netaikomas jeigu, atlikus ryšių ir informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės	x	x	x	x	x
13. Prisijungimo prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros slaptažodžių reikalavimai:					
13.1. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių	x	x	x	x	x
13.2. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai)	x	x	x	x	x
13.3. Draudžiama slaptažodžius atskleisti kitiems asmenims	x	x	x	x	x
13.4. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys, patvirtinančios valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo tapatumą, turi drausti išsaugoti slaptažodžius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x
13.5. Turi būti nustatytas didžiausias leistinas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo			x	x	x

mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip 5 kartai) (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo paskyra turi užsirakinti ir neleisti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui patvirtinti tapatybės kibernetinio saugumo dokumentuose nustatytą laiką – ne trumpiau kaip 15 minučių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)					
13.6. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo mėginimų įvesti teisingą slaptažodį skaičius – ne daugiau kaip 3 kartai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo paskyra turi užsiblokuoti ir turi būti informuojamas administratorius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x			
13.7. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu	x	x	x	x	x
13.8. Papildomi valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo slaptažodžių reikalavimai:					
13.8.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius	x	x	x	x	
13.8.2. Slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	
13.8.3. Keičiant slaptažodį, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x		
13.8.4. Pirmąkart jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti reikalaujama, kad valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas pakeistų slaptažodį (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x
13.9. Papildomi administratorių slaptažodžių reikalavimai:					
13.9.1. Slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius	x	x	x	x	
13.9.2. Slaptažodį turi sudaryti ne mažiau kaip 12 simbolių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	

13.9.3. Keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	
14. Turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, sąrašai, periodiškai peržiūrimi kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais administratorius nušalinamas nuo darbo (pareigų)	x	x	x	x	
15. Turi būti vykdoma administratorių paskyrų kontrolė:					
15.1. Periodiškai tikrinama, ar nėra nepatvirtintų administratoriaus paskyrų				x	x
15.2. Naudojamos administratorių paskyrų kontrolės priemonės, kurios tikrina administratoriaus paskyras. Apie nepatvirtintas administratoriaus paskyras turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
16. Vykdoma valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolė:					
16.1. Tikrinama, ar nėra nepatvirtintų valstybės informacinių išteklių arba ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų, ir pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, apie nepatvirtintas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras	x	x	x	x	x
16.2. Naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras. Apie nepatvirtintas paskyras turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
17. Draudžiama valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus	x	x	x	x	x

Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
18. Auditui atlikti turi būti fiksuojama ši informacija:					
18.1. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros elementų įjungimas / išjungimas ar perkrovimas (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x	x	x	x
18.2. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas	x	x	x	x	x
18.3. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų / administratorių teisių naudotis sistemos /	x	x	x		

tinklo ištekliais pakeitimai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)					
18.4. Audito funkcijos įjungimas / išjungimas	x	x	x	x	x
18.5. Audito įrašų trynimas, kūrimas ar keitimas	x	x	x	x	x
18.6. Laiko ir (ar) datos pakeitimai	x	x	x		
19. Audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu	x	x	x		
20. Turi būti naudojami mažiausiai 2 laiko sinchronizavimo šaltiniai	x	x			
21. Kiekviename audito duomenų įraše turi būti fiksuojama:					
21.1. Įvykio data ir tikslus laikas	x	x	x	x	x
21.2. Įvykio rūšis / pobūdis	x	x	x		
21.3. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo / administratoriaus ir (arba) valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įrenginio, susijusio su įvykiu, duomenys	x	x	x	x	x
21.4. Įvykio rezultatas	x	x	x	x	x
22. Priemonės, naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais	x	x	x		
23. Valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti	x	x	x		
24. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant, bet ne vėliau kaip 1 darbo dieną turi būti informuojamas administratorius ir kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
25. Audito duomenys turi būti saugomi ne trumpiau kaip 60 dienų, užtikrinant visas prasmingas jų turinio reikšmes (pavyzdžiui, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo, su kuriuo nutraukti darbo santykiai ir kuris pašalintas iš sistemos, atpažinties duomenys turi būti išsaugoti visą būtiną audito duomenų saugojimo laiką)	x	x	x		
26. Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas	x	x	x	x	x
27. Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo	x	x	x		
28. Naudojimasis audito duomenimis turi būti kontroliuojamas ir fiksuojamas. Audito duomenys turi būti pasiekiami tik administratoriui ir kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis)	x	x	x		
29. Audito įrašų duomenys turi būti analizuojami administratoriaus ne rečiau kaip kartą per mėnesį ir apie analizės rezultatus informuojamas kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		

Įsibrovimų aptikimas ir prevencija

Reikalavimas	YSII	I	II	III	IV

30. Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų	x	x	x	x	x
31. Įvykus įtartinai veiklai, tai turi būti užfiksuojama audito įrašuose ir kuriamas pranešimas, kurį matytų administratorius	x	x	x		
32. Sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį	x	x	x		
33. Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)	x	x	x		
34. Pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros funkcionalumu ir administravimu susijusį, duomenų srautą	x	x	x	x	x
35. Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai)	x	x	x	x	x

Belaidžio tinklo saugumas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
36. Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus	x	x	x	x	x
37. Turi būti vykdoma belaidžių įrenginių kontrolė:					
37.1. Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje eksploatuojami belaidžiai įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius	x	x	x	x	x
37.2. Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
37.3. Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidės prieigos taškus	x	x	x	x	x
38. Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje	x	x	x	x	x

39. Prisijungiant prie belaidžio tinklo, turi būti taikomas RIS naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas	x	x	x	x	x
40. Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą	x	x	x	x	x
41. Turi būti uždrausti visi nebūtini valdymo protokolai	x	x	x	x	x
42. Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai	x	x	x	x	x
43. Turi būti uždraustas lygiarangis (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje	x	x	x	x	x
44. Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu	x	x	x	x	x
45. Prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai	x	x	x	x	
46. Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga	x	x	x		

Mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugumas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
47. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją	x	x	x	x	x
48. Leidžiama naudoti tik leistinus mobiliuosius įrenginius, atitinkančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo nustatytus saugumo reikalavimus	x	x	x	x	x
49. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą	x	x	x	x	
50. Turi būti vykdoma mobiliųjų įrenginių kontrolė:					
50.1. Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje naudojami mobilieji įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius	x	x	x	x	x
50.2. Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius ar kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą informuotų apie neleistinos mobiliosios įrangos prijungimą prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros	x	x	x		
51. Mobiliuosiuose įrenginiuose privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, užkardymo ir stebėjimo priemonės	x	x			
52. Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos	x	x	x	x	x

programinės įrangos gamintojų rekomenduojami atnaujinimai					
53. Mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, apribojančios neleistino vykdomojo kodo naudojimą ar informuojančios administratorių apie neleistino vykdomojo kodo naudojimą	x	x			
54. Turi būti parengti mobiliųjų įrenginių operacinių sistemų atvaizdai su saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų pažeidžiamumų ar atakų	x	x	x		
55. Pagal parengtus atvaizdus į mobiliuosius įrenginius turi būti įdiegiama operacinė sistema su saugumo nuostatomis	x	x	x		
56. Mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių	x	x	x		
57. Prie mobiliųjų įrenginių draudžiama prijungti toms sistemoms nepriklausančius įrenginius	x	x	x		
58. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu prie mobiliųjų įrenginių gali būti jungiami kiti įrenginiai. Administratoriaus parengtą, su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą suderintą leistinų jungti įrenginių sąrašą tvirtina valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas	x	x			
59. Duomenys, perduodami tarp mobiliojo įrenginio ir valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti šifruojami taikant VPN technologiją	x	x	x	x	
60. Jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį	x	x	x	x	
61. Nešiojamasis prietaisas, gaunantis energiją iš integruoto energijos šaltinio ir turintis galimybę perduoti ir (ar) priimti ir apdoroti elektroninius duomenis, siunčiamus fizine terpe, elektromagnetinėmis bangomis ir šviesa, kuriuo nesinaudojama nustatytą laiką (pavyzdžiui, 5 minutes), turi automatiškai užsirakinti	x	x	x		
62. Mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti duomenis	x	x			
63. Turi būti užtikrinta kompiuterinių laikmenų apsauga	x	x	x	x	x
64. Turi būti šifruojami duomenys tiek mobiliųjų įrenginių laikmenose, tiek išorinėse kompiuterinėse laikmenose	x	x	x		

Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamos svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
65. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar	x	x	x	x	x

ypatingos svarbos informacinės infrastruktūros svarbos kategoriją					
66. Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:					
66.1. Draudžiama slaptažodžius saugoti programiniame kode	x	x	x	x	x
66.2. Svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti išsaugoti slaptažodžius	x	x	x	x	
67. Turi būti įgyvendinti svetainės kriptografijos reikalavimai:					
67.1. Atliekant svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą	x	x	x	x	x
67.2. Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų	x	x	x	x	
67.3. Turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas	x	x	x		
67.4. Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*)	x	x	x	x	
67.5. Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*)	x	x	x		
67.6. Kriptografiniai raktai ir algoritmai turi būti valdomi pagal RIS valdytojo reikalavimus	x	x	x	x	x
68. Tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro rekomenduojamą testavimo priemonę	x	x	x		
69. Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai	x	x	x	x	x
70. Turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*). Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)	x	x	x		
71. Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. DOS), paskirstyto atsisakymo aptarnauti (angl. DDOS) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org	x	x	x		
72. Turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*)	x	x	x	x	
73. Tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį	x	x	x	x	
74. Svetainės saugumo priemonės turi gebėti uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai)	x	x	x		

75. Atliekamų veiksmų audito ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją	x	x	x	x	x
76. Tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus	x	x	x	x	x
77. Turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*)	x	x	x	x	x
78. Turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema	x	x	x		

Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamo interneto saugumas ir kontrolė

Reikalavimas	YSII	I	II	III	IV
79.Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas su interneto paslaugos teikėju (-ais) turi būti sudaręs šias sutartis:					
79.1. Reagavimo į kibernetinius incidentus įprastomis darbo valandomis	x	x	x	x	x
79.2. Reagavimo į kibernetinius incidentus po darbo valandų	x	x	x		
79.3. Nepertraukiamo interneto paslaugos teikimo:					
79.3.1. įprastomis darbo valandomis				x	x
79.3.2. 24 valandas per parą, 7 dienas per savaitę	x	x	x		
79.4. Interneto paslaugos sutrikimų registravimo:					
79.4.1. įprastomis darbo valandomis				x	x
79.4.2. 24 valandas per parą, 7 dienas per savaitę	x	x	x		
79.5. Apsaugos nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros trikdymo taikymo (angl. *Denial of Service, DoS*)	x	x	x	x	x

Lietuvos Respublikos
vidaus reikalų ministras
Eimutis Misiūnas
2018-4-06

KAM Administracinės departamento
Dokumentų administravimo skyriaus
vyr. specialistė
Vesta Adomaitienė

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Krašto apsaugos viceministras
Edvinas Kerza