Առաջին ընթերցում

Կ-1139-20.08.2025-ՊԻ-011/1

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՔԸ

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ

ԳԼՈՒԽ 1
ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

Սույն օրենքի նպատակը Հայաստանի Հանրապետությունում կենսական նշանակության ոլորտների տեղեկատվական համակարգերում (այսուհետ՝ տեղեկատվական համակարգ) և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգ միջավայրի ապահովումն է:

Հոդված 1. Օրենքի կարգավորման առարկան և գործողության ոլորտը

1. Սույն օրենքը կարգավորում է կենսական նշանակության ոլորտներում կրիտիկական տեղեկատվական ենթակառուցվածքների կամ տեղեկատվական համակարգերի կիբեռանվտանգության ապահովման հետ կապված հարաբերությունները, մասնավորապես՝ սույն օրենքի իմաստով ծառայություն մատուցող սուբյեկտների շրջանակը, կենսական նշանակության ոլորտները, կիբեռմիջադեպերի հայտնաբերման, դրանց մասին ծանուցման, կանխարգելման և լուծման, կիբեռանվտանգության ոլորտի պետական կառավարման համակարգի մարմինների և դրանց լիազորությունների շրջանակի, սույն օրենքի պահանջների պահպանման նկատմամբ մշտադիտարկման, վերահսկողության, պատասխանատվության, կիբեռանվտանգության աուդիտի, ինչպես նաև կիբեռանվտանգության հետ կապված այլ հարաբերությունները:

2. Ցանկացած այլ իրավաբանական անձ, որը սույն օրենքի իմաստով չի համարվում ծառայություն մատուցող, Հայաստանի Հանրապետության կառավարության կողմից սահմանված կարգով կարող է կամավոր ստանձնել սույն

օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամ հրաժարվել դրանցից:

3. Սույն օրենքի գործողությունը տարածվում է.

1) իրավաբանական անձանց և անհատ ձեռնարկատերերի վրա, որոնք գործունեություն են ծավալում սույն օրենքի 16-րդ հոդվածի 3-րդ մասում թվարկված կենսական նշանակության ոլորտներից մեկում կամ մի քանիսում միաժամանակ և շահագործում են տեղեկատվական համակարգ կամ կրիտիկական տեղեկատվական ենթակառուցվածք,

2) պետական կառավարման և տեղական ինքնակառավարման մարմինների վրա:

4. Սույն օրենքի գործողությունը չի տարածվում «Փոքր և միջին ձեռնարկատիրության աջակցության մասին» օրենքով նախատեսված գերփոքր և փոքր ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշներին բավարարող իրավաբանական անձանց և անհատ ձեռնարկատերերի վրա, բացառությամբ այն դեպքերի, երբ նշված անձինք շահագործում են կրիտիկական տեղեկատվական ենթակառուցվածք:

5. Սույն օրենքի գործողությունը չի տարածվում պաշտպանության, ազգային անվտանգության, արտաքին հարաբերությունների, արտաքին հետախուզական գործունեության իրականացման ոլորտներում պետական լիազոր մարմինների կողմից իրենց գործառույթներն իրականացնելիս օգտագործվող տեղեկատվական համակարգերի կիբեռանվտանգության պահանջների պահպանման նկատմամբ:

6. Սույն օրենքի գործողությունը չի տարածվում պետական գաղտնիք պարունակող տեղեկությունների մշակման նպատակով կիրառվող տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքների օգտագործմանն առնչվող կիբեռանվտանգության պահանջների պահպանման նկատմամբ:

7. Սույն օրենքի գործողությունը չի տարածվում այլ օրենքներով կիբեռհանցագործությունների ոլորտը կարգավորող հարաբերությունների վրա:

8. Սույն օրենքով սահմանված կիբեռանվտանգության ապահովմանն ուղղված միջոցառումներ իրականացնելիս ծառայություն մատուցողները անձնական

տվյալների հետ կապված ցանկացած գործողություն իրականացնելիս պետք է առաջնորդվեն անձնական տվյալներ մշակելու հետ կապված հարաբերությունները կարգավորող օրենսդրության պահանջներին համապատասխան:

9. Սույն օրենքով սահմանված կիբեռանվտանգության ապահովմանն ուղղված միջոցառումներ իրականացնելիս ծառայություն մատուցողները պետական գաղտնիք, ինչպես նաև օրենքով պահպանվող այլ գաղտնիք պարունակող տեղեկությունների հետ կապված ցանկացած գործողություն իրականացնելիս առաջնորդվում են օրենքով պահպանվող և տվյալ գաղտնիքի հետ կապված հարաբերությունները կարգավորող օրենսդրության պահանջներին համապատասխան:

Հոդված 2. Կիբեռանվտանգության մասին օրենսդրությունը

1.Կիբեռանվտանգության ապահովման ոլորտում ծագող հարաբերությունները կարգավորվում են Սահմանադրությամբ, սույն օրենքով, «Հանրային տեղեկությունների մասին» օրենքով, «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով, Հայաստանի Հանրապետության միջազգային պայմանագրերով, այլ իրավական ակտերով:

2. Եթե Հայաստանի Հանրապետության վավերացրած միջազգային պայմանագրերով սահմանվում են այլ նորմեր, քան նախատեսված են սույն օրենքով, ապա կիրառվում են միջազգային պայմանագրերի նորմերը:

Հոդված 3. Օրենքում օգտագործվող հիմնական հասկացությունները

1. Սույն օրենքում օգտագործվում են հետևյալ հիմնական հասկացությունները.

1) **կիբեռանվտանգություն**՝ կազմակերպչական, տեխնիկական, ծրագրային միջոցների ամբողջություն, որը պաշտպանում է համակարգչում, համակարգչային սարքավորումում, թվային հիշողության կրիչներում, տեղեկատվական համակարգում, կրիտիկական տեղեկատվական ենթակառուցվածքում, էլեկտրոնային հաղորդակցության ցանցում մշակվող, պահվող և փոխանցվող տեղեկությունը պատահական կորստից, չարտոնված մուտքից, օգտագործումից,

բացահայտումից, խափանումից, փոփոխումից, ոչնչացումից, հարձակումից, կրկնօրինակումից, ձայնագրումից, տարածումից և այլ անօրինական ներթափանցումից կամ միջամտությունից, ինչպես նաև ապահովում է այդ տեղեկության հասանելիությունը, ամբողջականությունը, իսկությունը (authenticity), գաղտնիությունը և անհերքելիությունը (non-repudiation).

2) **Լիազոր մարմին** - «Կառավարության կառուցվածքի և գործունեության մասին» օրենքի հավելվածի 16-րդ կետով թվարկված ոլորտներում քաղաքականություն մշակող և իրականացնող պետական կառավարման համակարգի մարմին (այսուհետ՝ Լիազոր մարմին).

3) **Ինքնավար մարմին** - «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով նախատեսված տեղեկատվական համակարգերի կարգավորման հանձնաժողով (այսուհետ՝ Ինքնավար մարմին).

4) **տեղեկատվական համակարգի անվտանգություն՝** տեղեկատվական համակարգի կարողություն՝ դիմակայելու ցանկացած իրադրության, որը վտանգում է այդ համակարգում պահպանված, մշակված, ձեռք բերված կամ փոխանցված տվյալների հասանելիությունը, իսկությունը (authenticity), ամբողջականությունը, գաղտնիությունը և անհերքելիությունը (non-repudiation) կամ այդ համակարգով առաջարկվող կամ այդ համակարգի միջոցով հասանելի դարձվող ծառայությունները.

5) **կրիտիկական տեղեկատվական ենթակառուցվածք՝** կենսական նշանակության ոլորտներում շահագործվող ավտոմատացված կառավարման համակարգեր, տեղեկատվական համակարգեր, սարքավորումներ կամ դրանց մի մասը, որոնց խափանումը կամ ոչնչացումը կարող է սպառնալիքներ ստեղծել ազգային անվտանգության, պաշտպանության, տնտեսության, սոցիալական բարեկեցության, բնակչության առողջության, շրջակա միջավայրի համար.

6) **կենսական նշանակության ոլորտ՝** ոլորտ, որն ունի առանցքային նշանակություն բնակչության բնականոն գործունեության, տնտեսական ակտիվության, պետական անվտանգության, հանրային առողջության և անվտանգության կամ շրջակա միջավայրի պահպանման, Հայաստանի

Հանրապետության կենսական նշանակության այլ շահերի պաշտպանության համար.

7) **ծառայություն մատուցող՝** սույն օրենքի 1-ին հոդվածի 3-րդ մասում նշված իրավաբանական անձ կամ անհատ ձեռնարկատեր, նույն հոդվածի 4-րդ մասում նշված գերփոքր և փոքր ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշներին բավարարող իրավաբանական անձինք կամ անհատ ձեռնարկատերեր, ովքեր շահագործում են կրիտիկական տեղեկատվական ենթակառուցվածք, ինչպես նաև պետական կառավարման կամ տեղական ինքնակառավարման մարմին.

8) **թվային ենթակառուցվածք՝** սույն օրենքի իմաստով էլեկտրոնային առևտրային հարթակ, առցանց որոնման համակարգ, ամպային հաշվողական ծառայություն, էլեկտրոնային թվային ստորագրության ստեղծման կամ ստուգման միջոցներ, էլեկտրոնային թվային ստորագրության հավաստագրերի տրամադրման և էլեկտրոնային թվային ստորագրությունների հետ կապված այլ ծառայություններ, էլեկտրոնային հաղորդակցության ծառայություն, հանրային էլեկտրոնային հաղորդակցության ծառայություն, ինտերնետային հասանելիության ծառայություն, Հայաստանի վերին մակարդակի ազգային դոմեյն հանդիսացող դոմենային տիրույթի ռեգիստր.

9) **էլեկտրոնային առևտրային հարթակ՝** սույն օրենքի իմաստով ծառայություն, որը թույլ է տալիս սպառողներին և արտադրողներին «Առևտրի և ծառայությունների մասին» և «Սպառողների իրավունքների պաշտպանության մասին» օրենքներով սահմանված պահանջների պահպանմամբ ինտերնետային կայքում, էլեկտրոնային հավելվածում կամ համանման այլ միջոցներով կնքել առցանց վաճառքի կամ սպասարկման էլեկտրոնային պայմանագրեր.

10) **առցանց որոնման համակարգ՝** թվային ծառայություն, որն օգտատերերին թույլ է տալիս հարցումներ մուտքագրել բոլոր վեբ-կայքերում կամ միայն որոշակի լեզվով վեբ-կայքերում որոնումներ կատարելու նպատակով՝ հիմնաբառի, ձայնային հարցման, արտահայտության կամ այլ ձևով մուտքագրման տեսքով և ներկայացնում է արդյունքները ցանկացած ձևաչափով, որում կարելի է գտնել հայցվող բովանդակության հետ կապված տեղեկությունը.

11) **ամպային հաշվողական ծառայություն՝** տվյալները և կիրառական ծրագրերը պահպանելու համար կիրառվող տեխնոլոգիա, որն աշխատում է ցանցի (առանձնացված կամ համացանցի) և վիրտուալ սերվերների միջավայրում և որն ամպային տեխնոլոգիայի կիրառմամբ հնարավորություն է տալիս մուտք գործել համօգտագործվող և մասշտաբային հաշվողական ռեսուրսների մի խումբ՝ առանց համակարգը փոփոխելու.

12) **կիբեռսպառնալիք՝** ցանկացած հանգամանք, իրադրություն կամ գործողություն կամ անգործություն, այդ թվում՝ տեղեկատվության չարտոնված մուտք, ոչնչացում, բացահայտում, փոփոխում կամ ծառայության մերժում, որը կարող է վնասել, խափանել, վտանգել կամ որևէ այլ կերպ բացասաբար ազդել կրիտիկական տեղեկատվական ենթակառուցվածքի կամ տեղեկատվական համակարգի անխափան աշխատանքի կամ դրանք օգտագործողների կամ այլ անձանց վրա.

13) **կիբեռհարձակում՝** կրիտիկական տեղեկատվական ենթակառուցվածքի կամ տեղեկատվական համակարգի աշխատանքը խափանելու, դրանցում մշակվող տվյալներին չարտոնված հասանելիություն ստանալու կամ ամբողջականության վրա բացասաբար ազդելու նպատակով դիտավորությամբ կամ արտաքին ուղղորդմամբ իրականացվող գործողությունների ամբողջություն.

14) **կիբեռմիջադեպ՝** կրիտիկական տեղեկատվական ենթակառուցվածքում, տեղեկատվական համակարգում տեղի ունեցող ցանկացած գործողություն կամ միջամտություն, որն անխուսափելիորեն վտանգում կամ բացասաբար է ազդում կրիտիկական տեղեկատվական ենթակառուցվածքի կամ տեղեկատվական համակարգի կիբեռանվտանգության, ինչպես նաև դրանց շարունակական, անխափան և անվտանգ օգտագործման վրա.

15) **ազգային համակարգչային արտակարգ իրավիճակների արձագանքման թիմ (CERT)՝** Ինքնավար մարմնի փորձագետների խումբ, որն իրականացնում է կիբեռմիջադեպերի կառավարումը՝ համակարգումը, վերլուծությունը, կանխումը, արձագանքումը, լուծումը, հետևանքների վերացումը.

16) **կիբեռանվտանգության գործառնությունների կենտրոն (Security Operations Center (SOC))՝** կիբեռանվտանգության կենտրոնացված մոնիտորինգի և

արձագանքման ստորաբաժանում, որը 24/7 ռեժիմով հսկում է տեղեկատվական համակարգերը, հայտնաբերում սպառնալիքները և իրականացնում անվտանգության միջոցառումներ.

17) **կարգավորող և վերահսկող այլ մարմին՝** օրենքով նախատեսված դեպքերում և կարգով ծառայություն մատուցողի գործունեության ոլորտը կարգավորող (նշանակող, որակավորում տվող կամ այլ կերպ գործունեության թույլտվություն տրամադրող, լիցենզավորող), վերահսկողություն, հսկողություն իրականացնող մարմին.

18) **կիբեռանվտանգության ապահովման ծառայություն մատուցող՝** իրավաբանական կամ ֆիզիկական անձ, ով մատուցում է կիբեռանվտանգության ապահովման ծառայություններ, ինչպես նաև սույն օրենքով նախատեսված դեպքերում պետական մարմիններ.

19) **համակարգիչ՝** սարք, որը պահպանում, փոխանցում և մշակում է թվային տվյալներ՝ ծրագրային ապահովման կամ հրահանգների հաջորդականության հիման վրա և թվային տվյալների պահպանման, փոխանցման կամ հաղորդակցության համար կիրառվող ցանկացած այլ սարքավորում, որն օգտագործվում է տվյալ սարքի հետ համակցված.

20) **ռիսկ՝** կիբեռմիջադեպի հետևանքով առաջացած կորստի կամ խափանման հավանականություն, որն արտահայտվում է այդպիսի կորստի կամ խափանման մեծության և կիբեռմիջադեպ տեղի ունենալու հավանականության համակցությամբ.

21) **խոցելիություն՝** տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի թույլ կողմ կամ թերություն, որն հնարավորություն է ստեղծում կիբեռսպառնալիքի համար.

22) **կիբեռանվտանգության մասնագետ՝** տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության պահանջների պահպանման համար ծառայություն մատուցողի կողմից նշանակված պատասխանատու անձ.

23) **կիբեռհիգիենա՝** կիբեռանվտանգության միջոցառումների ամբողջություն, որն ուղղված է կրիտիկական տեղեկատվական ենթակառուցվածքի,

տեղեկատվական համակարգերի տվյալների անվտանգության և ամբողջականության պահպանմանն ու բարելավմանը.

24) տեղեկատվական համակարգ - էլեկտրոնային հաղորդակցության ցանց կամ ցանկացած սարք կամ փոխկապակցված կամ հարակից (կապակցվող) սարքերի խումբ կամ տեխնիկական և ծրագրաապարատային միջոցների ամբողջություն, որոնցից մեկը կամ մի քանիսը միասին կատարում են թվային տվյալների ինքաշխատ մշակում, կամ թվային տվյալներ, որոնք պահվում, մշակվում, ձեռք են բերվում կամ փոխանցվում են սույն կետում նշված միջոցներով՝ նրանց օգտագործման, պաշտպանության և սպասարկման նպատակով:

Հոդված 4. Կիբեռանվտանգության ապահովման սկզբունքները

1. Կիբեռանվտանգության ապահովումն իրականացվում է հետևյալ սկզբունքներով.

1) անհատականության սկզբունք՝ տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգության ապահովումը կազմակերպում է ծառայություն մատուցողը.

2) համապարփակ պաշտպանության սկզբունք՝ ծառայություն մատուցողը պետք է գնահատի իր կողմից օգտագործվող տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի վրա հնարավոր ռիսկերը, կազմի ռիսկերի գնահատման սանդղակ, որոշի հավանական կիբեռմիջադեպի հետևանքների ծանրությունը, ազդեցության մաշտաբները, տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի անխափան շահագործման կամ հետևանքների վերացման համար անհրաժեշտ ֆինանսական միջոցների չափը և մշակի կիբեռմիջադեպերի կանխարգելման միջոցառումների ծրագիր.

3) բացասական ազդեցությունը նվազագույնի հասցնելու սկզբունք՝ կիբեռմիջադեպի դեպքում ծառայություն մատուցողը պետք է սույն օրենքով և կիբեռանվտանգության ապահովման ներքին կանոնակարգով սահմանված համապատասխան քայլեր և միջոցներ ձեռնարկի կիբեռմիջադեպի արագ սրացումը

(ազդեցության մասշտաբների ընդլայնումը), այլ համակարգերում դրա հնարավոր տարածումը կանխելու համար.

4) նվազագույն հասանելիության սկզբունք (least privilege)՝ ծառայություն մատուցողը պետք է ապահովի, որ յուրաքանչյուր ոք կամ որևէ ավտոմատացված գործընթաց տեղեկատվական համակարգին կամ կրիտիկական տեղեկատվական ենթակառուցվածքին կամ դրանում պահպանվող տվյալների ունենա ոչ ավելի հասանելիություն, որքան անհրաժեշտ է իր աշխատանքային պարտականությունների կամ գործառույթների պատշաճ իրականացման համար.

5) Տվյալների գաղտնիության սկզբունք՝ տվյալները պետք է հասանելի լինեն միայն այն անձանց համար, ովքեր ունեն համապատասխան մուտքի թույլտվություն.

6) համագործակցության սկզբունքը՝ կիբեռանվտանգության ապահովման, կիբեռհարձակումների, կիբեռսպառնալիքների կանխման և խափանման, ինչպես նաև կիբեռմիջադեպերի լուծման, հետևանքների վերացման կամ մեղման ընթացքում ծառայություն մատուցողները պետք է ապահովեն բավարար համագործակցություն պետական իրավասու մարմինների և հասարակության հետ, ինչպես նաև միմյանց միջև՝ հաշվի առնելով նաև տեղեկատվական համակարգերի կամ կրիտիկական տեղեկատվական ենթակառուցվածքների միջև փոխադարձ կապն ու փոխգործելիությունը.

7) Ամբողջականության (non-repudiation) սկզբունք՝ ծառայություն մատուցողները պետք է պաշտպանեն տեղեկությունը չարտոնված փոփոխումից կամ ոչնչացումից՝ ապահովելով դրա անխաթարությունը, իսկությունը, հուսալիությունը, ամբողջականությունը և անհերքելիությունը.

8) հասանելիության սկզբունք՝ ծառայություն մատուցողները պետք է ապահովեն տեղեկության ժամանակին պատշաճ հասանելիությունը և օգտագործումը իրավասու անձանց կողմից:

ԳԼՈՒԽ 2
ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՈԼՈՐՏԻ ՊԵՏԱԿԱՆ ԿԱՌԱՎԱՐՈՒՄԸ ԵՎ ԿԱՐԳԱՎՈՐՈՒՄԸ

Հոդված 5. Կիբեռանվտանգության ոլորտում օրենքով նախատեսված լիազորություններ իրականացնող մարմինները

Կիբեռանվտանգության ոլորտում օրենքով նախատեսված լիազորություններ իրականացնում են Լիազոր մարմինը, Ինքնավար մարմինը և տեղեկատվական անվտանգության ապահովման աշխատանքների իրականացումը համակարգող լիազոր մարմինը:

Հոդված 6. Լիազոր մարմնի գործառույթները

1. Լիազոր մարմնի գործառույթներն են՝

1) կիբեռանվտանգության միասնական քաղաքականության և դրան առնչվող ոլորտային կարգավորող իրավական դաշտի, ներառյալ կիբեռանվտանգության ապահովման ոլորտի ռազմավարության և դրանից բխող միջոցառումների ծրագրի մշակում.

2) հասարակության կիբեռհասունությանն ուղղված իրազեկման և կրթական միջոցառումների մշակում և իրականացում.

3) Հայաստանի Հանրապետության միջազգային համաձայնագրերով ստանձնած կիբեռանվտանգության ոլորտի միջազգային հանձնառությունների իրականացում.

4) միջազգային վարկանիշային զեկույցներում կիբեռանվտանգության ցուցանիշների մասնագիտական վերլուծություն, առաջընթացի ապահովում.

5) համագործակցելով Ինքնավար մարմնի հետ՝ միջազգային ստանդարտների հիման վրա կիբեռանվտանգության ապահովման ազգային ստանդարտների մշակում և ներկայացում ստանդարտացման և չափագիտության ազգային մարմնի հաստատմանը.

6) կիրառելի միջազգային ստանդարտների ցանկի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.

7) արտակարգ իրավիճակներում, արտակարգ կամ ռազմական դրության ժամանակ դրա տևողության ամբողջ ընթացքում տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման միջոցառումների ձեռնարկում և դրանց իրականացման նկատմամբ հսկողության ապահովում.

8) կենսական նշանակության ոլորտներում կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկը ըստ կիբեռանվտանգության ապահովման համար պատասխանատու պետական մարմինների սահմանելու մասին Հայաստանի Հանրապետության կառավարության որոշման նախագծի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.

9) կենսական նշանակության ոլորտներում ծառայությունների տեսակները ըստ տնտեսական գործունեության տեսակների դասակարգիչների սահմանելու մասին Հայաստանի Հանրապետության կառավարության որոշման նախագծի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.

10) ծառայություն մատուցող չհամարվող իրավաբանական անձի կողմից սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամավոր ստանձնելու և դրանցից հրաժարվելու դեպքերի սահմանման մասին կարգի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.

11) կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշները սահմանելու մասին Հայաստանի Հանրապետության կառավարության որոշման նախագծի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.

12) իրականացնում է օրենքով նախատեսված այլ լիազորություններ:

Հոդված 7. Կիբեռանվտանգության ոլորտում Ինքնավար մարմնի գործառույթները

1. Ինքնավար մարմինը՝ որպես միասնական կոնտակտային կետ, կարգավորում, կառավարում և հսկում է կիբեռմիջադեպերի գրանցման, կանխարգելման և լուծման, հետևանքների վերացմանն ուղղված գործողությունները, իրականացնում սույն օրենքի ու դրա հիման վրա ընդունված իրավական ակտերի պահանջների պահպանման նկատմամբ մշտադիտարկում և վերահսկողություն:

2. Ինքնավար մարմինն իրականացնում է հետևյալ գործառույթները.

1) սույն օրենքով սահմանված գործառույթների շրջանակում արձագանքում է կիբեռմիջադեպերին.

2) սահմանում և դասակարգում է կիբեռմիջադեպերի արձագանքման առաջնահերթությունները.

3) գրանցում է կիբեռմիջադեպերը, վարում է կիբեռմիջադեպերի գրանցամատյանը.

4) վերլուծում է կիբեռմիջադեպեր.

5) կազմակերպում է կիբեռմիջադեպերի կանխարգելման միջոցառումները.

6) ծառայություն մատուցողներին ցուցաբերում է ռիսկերի գնահատման մեթոդական աջակցություն.

7) կիբեռանվտանգության ոլորտում վարում է վիճակագրական հաշվետվություններ.

8) բարձրացնում է կիբեռանվտանգության խնդիրների վերաբերյալ հասարակության տարբեր խմբերի շրջանում իրազեկվածությունը՝ այդ թվում կիբեռհիգիենայի պահպանման մասով, մշակում և իրականացնում է իրազեկման և կրթական ծրագրեր՝ համագործակցելով Լիազոր մարմնի և կրթության ոլորտում պատասխանատու պետական մարմինների հետ, ինչպես նաև տրամադրում է խորհրդատվություն կիբեռանվտանգության խնդիրների վերաբերյալ իրազեկվածության բարձրացում իրականացնող պետական մարմիններին.

9) մշակում և հաստատում է ծառայություն մատուցողների կողմից շահագործվող տեղեկատվական համակարգերի (այդ թվում՝ կիրառվող տեղեկատվական տեխնոլոգիաների, ծառայությունների, գործընթացների և

արտադրանքների մասով՝ հաշվի առնելով սույն օրենքի 16-րդ հոդվածի 3-րդ մասով թվարկված ոլորտների, ենթաոլորտների կամ ծառայության տեսակների առանձնահատկությունները) և կրիտիկական տեղեկատվական ենթակառուցվածքների կիբեռանվտանգության ապահովման նվազագույն պահանջները.

10) մշակում և հաստատում է ծառայություն մատուցողների կողմից կիբեռմիջադեպերի ծանուցման և հաշվետությունների ներկայացման կարգը.

11) մշակում և հաստատում է կիբեռանվտանգության աուդիտի հաշվետվության չափորոշիչները, կիբեռանվտանգության աուդիտորների որակավորման կարգը և կիբեռնավտանգության աուդիտ իրականացնող անձանց ներկայացվող պահանջները.

12) մշակում, հաստատում և իրականացնում է կիբեռվարժանքների տարեկան ծրագրերը.

13) տեղեկատվական համակարգեր կամ կրիտիկական տեղեկատվական ենթակառուցվածքներ օգտագործող պետական մարմիններում կազմակերպում է կիբեռվարժանքների իրականացման տարեկան ծրագրով նախատեսված միջոցառումներ.

14) հնարավոր կիբեռմիջադեպերը կանխելու կամ ազդեցությունը նվազեցնելու նպատակով ապահովում է իրազեկում.

15) մշակում և հաստատում է սույն օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական նորմատիվ իրավական ակտերով սահմանված պահանջների պահպանմանն առնչվող ուղեցույցներ.

16) իրականացնում է ծառայություն մատուցողների կողմից սույն օրենքով սահմանված պահանջների պահպանման նկատմամբ մշտադիտարկում օրենքով սահմանված կարգով, մշակում և հաստատում է կիբեռանվտանգության ոլորտում մշտադիտարկման ընթացակարգ.

17) սույն օրենքով սահմանված իր իրավասությունների շրջանակում փոխգործակցության երկկողմ համաձայնագրերի կնքմամբ կամ առանց դրա համագործակցում է պետական այլ մարմինների, այդ թվում՝ ազգային անվտանգության հարցերով լիազորված պետական մարմնի, անձնական տվյալների

պաշտպանության բնագավառում և կիբեռհանցագործությունների դեմ պայքարի ոլորտում լիազոր մարմինների, ինչպես նաև օտարերկրյա պետություններում կիբեռանվտանգության ապահովման ոլորտում պատասխանատու մարմինների կամ համապատասխան համակարգչային արտակարգ իրավիճակների արձագանքման թիմերի հետ: Օտարերկրյա պետություններում կիբեռանվտանգության ապահովման ոլորտում պատասխանատու մարմինների, միջազգային կազմակերպությունների հետ կնքվող երկկողմ համաձայնագրերը, հուշագրերը, իրավաբանական պարտադիր ուժ չունեցող միջազգային բնույթի այլ փաստաթղթերը նախապես համաձայնեցնում է սույն օրենքով նախատեսված լիազոր մարմնի և օրենքով նախատեսված դեպքերում այլ լիազոր մարմինների հետ.

18) իր գործունեության ընթացքում կիբեռմիջադեպի քրեաիրավական բնույթի վերաբերյալ կասկածներ ունենալու կամ բավարար հիմքեր ի հայտ գալու դեպքում իրավապահ մարմիններին ներկայացնում է հաղորդում.

19) օրենքով սահմանված կարգով և դեպքերում ծառայություն մատուցողների նկատմամբ իրականացնում է վերահսկողություն, օժանդակում է օրենքով կարգավորող և վերահսկող այլ մարմինների կողմից իրականացվող վերահսկողությանը, այդ թվում՝ պատասխանատվություն կիրառելու միջնորդություն ներկայացնելով, որի քննությունը և դրա հիման վրա որոշման ընդունումը պարտադիր է.

20) ստեղծում և կառավարում է կիբեռանվտանգության մշտադիտարկման ազգային օպերատիվ կենտրոնը.

21) ներկայացնում է առաջարկություններ Հայաստանի Հանրապետության կառավարության որոշմամբ հաստատված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկում փոփոխություններ կամ լրացումներ կատարելու վերաբերյալ.

22) կիբեռանվտանգության վերաբերյալ հարցերով փորձագիտական աջակցության ցուցաբերում Հայաստանի Հանրապետության կառավարությանը.

23) մշակում և հաստատում է կիբեռմիջադեպերը կանխելու կամ ազդեցությունը նվազեցնելու նպատակով Ինքնավար մարմնի կողմից հասցեատերերին իրազեկման կարգ.

24) մշակում և հաստատում է Ինքնավար մարմնի կողմից կիբեռմիջադեպերի գրանցամատյանի վարման կարգ.

25) մշակում և հաստատում է Ինքնավար մարմնի կողմից ծառայություն մատուցողների գրանցամատյանի վարման կարգ.

26) մշակում և հաստատում է կիբեռմիջադեպերի վերաբերյալ տեղեկության հավաքագրման և պահպանման կարգ.

27) մշակում և հաստատում է ծառայություններ մատուցողների կողմից կիբեռանվտանգության ապահովման ներքին կանոնակարգերին ներկայացվող պահանջները, ինչպես նաև ռիսկերի և կիբեռմիջադեպերի գնահատման չափանիշները. .

28) պետական մարմիններում և տեղական ինքնակառավարման մարմիններում իրականացնում է կիբեռանվտանգության գործառնությունների կենտրոնի (SOC) ծառայություններ.

29) իրականացնում է օրենքով նախատեսված այլ լիազորություններ:

3. Ինքնավար մարմինը իրավունք ունի օտարերկրյա պետության կիբեռանվտանգության ապահովման ոլորտում պատասխանատու մարմիններին կամ համապատասխան համակարգչային արտակարգ իրավիճակների արձագանքման թիմերին կամ միջազգային կազմակերպություններին փոխանցել կիբեռմիջադեպի կանխմանն ու լուծմանը վերաբերող տեղեկությունը սույն օրենքով նախատեսված գործառույթների կատարման համար, եթե նման տեղեկության փոխանցումը չի վնասում ազգային անվտանգությանը, Հայաստանի Հանրապետության օրինական շահերին կամ քրեական վարույթին: Այն դեպքում, երբ սույն կետի համաձայն փոխանցվող տեղեկությունը որևէ ձևով առնչվում է պաշտպանության, ազգային անվտանգության, կամ արտաքին հարաբերությունների ոլորտին, ապա տեղեկության փոխանցումը նախապես գրավոր համաձայնեցվում է, համապատասխանաբար, պաշտպանության, արտաքին հարաբերությունների լիազոր մարմինների, ինչպես նաև ազգային անվտանգության հարցերով լիազորված պետական մարմնի հետ, իսկ քրեական վարույթին առնչվող տեղեկատվության փոխանցումը համաձայնեցվում է քրեական վարույթն իրականացնող մարմնի հետ: Այն դեպքում, երբ սույն մասի համաձայն փոխանցվող տեղեկությունը հանդիսանում

է անձնական տվյալ, ապա տեղեկության փոխանցումն իրականացվում է բացառապես միջազգային պայմանագրերին համապատասխան:

4. Ինքնավար մարմինը վարում է ծառայություն մատուցողների գրանցամատյան: Ըստ անհրաժեշտության, բայց ոչ պակաս քան երկու տարին մեկ անգամ Ինքնավար մարմինը վերանայում և թարմացնում է իր կողմից հաստատված ծառայություն մատուցողների գրանցամատյանի տվյալները:

5. Սույն օրենքի 16-րդ հոդվածի 3-րդ մասում թվարկված ոլորտներում պետական քաղաքականություն մշակող և իրականացնող մարմինները իրենց իրավասությունների շրջանակում Ինքնավար մարմնին ցուցաբերում են տեղեկատվական և խորհրդատվական աջակցություն՝ սույն հոդվածի 4-րդ մասում նշված ծառայություն մատուցողների գրանցամատյանի վարման համար:

6. Ինքնավար մարմինը Հայաստանի Հանրապետության կառավարության որոշմամբ սահմանված կարգով և դեպքերում իրականացնում է պետական և տեղական ինքնակառավարման մարմին հանդիսացող ծառայություն մատուցողների կիբեռանվտանգության ապահովումը:

7. Պետական մարմիններում և տեղական ինքնակառավարման մարմիններում իրականացվող կիբեռանվտանգության գործառնությունների կենտրոնի ծառայությունների շրջանակը սահմանվում է Ինքնավար մարմնի կողմից:

Հոդված 8. Արտակարգ իրավիճակներում, արտակարգ դրության կամ ռազմական դրության ժամանակ տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքների կիբեռանվտանգության ապահովման միջոցառումները

1. Արտակարգ իրավիճակներում, արտակարգ կամ ռազմական դրության ժամանակ դրա տևողության ամբողջ ընթացքում տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման միջոցառումներ ձեռնարկում և դրանց կատարման նկատմամբ հսկողություն իրականացնող պատասխանատու պետական մարմին հանդիսանում է Լիազոր մարմինը՝ համագործակցելով Ինքնավար մարմնի և ազգային անվտանգության հարցերով լիազորված պետական մարմնի հետ:

2. Արտակարգ իրավիճակներում, արտակարգ կամ ռազմական դրության ժամանակ տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման միջոցառումների ձեռնարկման և դրանց հսկման, ինչպես նաև Ինքնավար մարմնի ու ազգային անվտանգության հարցերով լիազորված պետական մարմնի հետ համագործակցության կարգը հաստատում է Հայաստանի Հանրապետության կառավարությունը:

ԳԼՈՒԽ 3
ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԿԱՆՈՆՆԵՐ

Հոդված 9. Ծառայություն մատուցողի պարտականությունները

1. Ծառայություն մատուցողը պարտավոր է անընդհատ ռեժիմով (շաբաթը յոթ օր, քսանչորս ժամ) ձեռնարկել կազմակերպչական, տեխնիկական միջոցներ՝

1) կիբեռսպառնալիքները հայտնաբերելու և կառավարելու.

2) կիբեռմիջադեպը կանխելու, հայտնաբերելու, արգելափակելու, լուծելու.

3) տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքների անխափան գործունեության ապահովման համար ռիսկերը կառավարելու, կիբեռմիջադեպի հետևանքները նվազագույնի հասցնելու կամ այլ ածանցյալ կամ հնարավոր ազդեցությունները կանխելու և մեղմելու համար:

2. Ծառայություն մատուցողը կիբեռանվտանգության ապահովման համար պարտավոր է ունենալ կիբեռանվտանգության ապահովման ներքին կանոնակարգ, որով սահմանվում է ծառայություն մատուցողի կողմից կիբեռանվտանգության ոլորտում որդեգրած քաղաքականությունը, ինչպես նաև տրվում է ծառայություն մատուցողի կողմից սույն օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական նորմատիվ իրավական ակտերով սահմանված պահանջների պահպանման մանրամասն նկարագրությունը:

3. Ծառայություն մատուցողը՝

1) իրականացնում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի ռիսկերի գնահատում, կազմում ռիսկերի

գնահատման սանդղակ, որոշում հավանական կիբեռմիջադեպի հետևանքների ծանրությունն ու ազդեցության մասշտաբները, հաստատում կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագիր՝ հիմնվելով Ինքնավար մարմնի կողմից հաստատված ռիսկերի և կիբեռմիջադեպերի գնահատման չափանիշների, կիբեռանվտանգության ապահովման ներքին կանոնակարգերին ներկայացվող պահանջների վրա.

2) ռիսկերի կառավարման համար ձեռնարկում է կազմակերպչական և տեխնիկական միջոցներ, այդ թվում՝ տեղեկատվական համակարգերի ֆիզիկական անվտանգության ապահովման, համակարգիչներին կամ տեղեկատվություն մշակող, պահպանող կամ փոխանցող այլ սարքավորումներին չթույլատրված ֆիզիկական մուտքը, վնասումը կամ միջամտությունը կանխելու համար.

3) ապահովում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի վրա գնահատված հնարավոր կիբեռսպառնալիքների փաստաթղթավորումը, անվտանգության կանոնների և միջոցների կիրառման նկարագրությունը.

4) ապահովում է կիբեռանվտանգության ապահովման ներքին կանոնակարգով սահմանված պահանջներին համապատասխան ամենօրյա մշտադիտարկում՝ տեղեկատվական համակարգին կամ կրիտիկական տեղեկատվական ենթակառուցվածքին ուղղված կիբեռհարձակումների, կիբեռսպառնալիքների, խոցելիություններ հայտնաբերելու նպատակով (այդ թվում՝ կիրառվող տեղեկատվական տեխնոլոգիաները, ծառայությունները, գործընթացները և արտադրանքները, որոնց վնասումը կամ խափանումը սպառնում է տեղեկատվական համակարգի և կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգությանը).

5) կիբեռմիջադեպերի մասին սույն օրենքի 11-րդ հոդվածով սահմանված կարգով և դեպքերում ծանուցում է Ինքնավար մարմնին, ինչպես նաև կիբեռմիջադեպի հետևանքով հնարավոր ազդեցության ենթարկված անձանց.

6) միջոցներ է ձեռնարկում կիբեռմիջադեպի հետևանքները մեղմելու, դրա արագ սրացումը (ազդեցության մասշտաբների ընդլայնումը) կանխելու համար՝ անհրաժեշտության դեպքում իրականացնելով տեղեկատվական համակարգի կամ

կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործման, հասանելիության, մուտքի ամբողջական կամ մասնակի սահմանափակում.

7) վերահսկում է կիբեռմիջադեպին արձագանքելու, լուծելու, հետևանքները մեղմելու ուղղությամբ ձեռնարկված գործընթացները, գնահատում է դրանց կիրառման բավարար ու համարժեք լինելը կիբեռմիջադեպի հետևանքների ծանրությանն ու ազդեցության մաշտաբներին, փաստաթղթավորում է արդյունքները և կազմում է հաշվետվություններ, որոնք ենթակա են պահպանման ոչ պակաս, քան երեք տարի ժամկետով.

8) հավաքագրում է կիբեռմիջադեպերի վերաբերյալ տեղեկությունը և պահպանում այն դրա ստեղծման պահից ոչ պակաս, քան երեք տարի ժամկետով.

9) իր անձնակազմի համար կազմակերպում է կիբեռանվտանգության վերաբերյալ ընդհանուր և հատուկ դասընթացներ, իրականացնում է կիբեռվարժանքներ՝ համագործակցելով Լիազոր և Ինքնավար մարմինների հետ, ապահովում է իր մասնակցությունն Ինքնավար մարմնի կողմից կազմակերպվող վերապատրաստումներին և կիբեռանվտանգության ոլորտում կարողությունների զարգացման այլ միջոցառումներին.

10) կիբեռմիջադեպի արդյունքում կամ դրա ընթացքում հանցագործության հատկանիշներ ի հայտ գալու դեպքում օրենքով սահմանված կարգով հաղորդում է ներկայացնում իրավապահ մարմիններին.

11) ապահովում է կիբեռհիգիենայի հիմնական պահանջների կատարումը զրոյական վստահության սկզբունքի (չվստահել ոչ մեկին, ստուգել ամեն ինչ) հիման վրա, ինչպիսիք են՝ ծրագրային ապահովման թարմացումները, տեղեկատվական համակարգ մուտքի կառավարումը, անձնակազմի ուսուցումը և կիբեռսպառնալիքների, ֆիշինգի (phishing) մասին տեղեկացվածության բարձրացումը.

12) կատարում է սույն օրենքով, դրա հիման վրա ընդունված ենթաօրենսդրական նորմատիվ իրավական ակտերով, ծառայություն մատուցողի ներքին կանոնակարգով սահմանված այլ պարտականություններ.

13) ապահովում է կիբեռանվտանգության ապահովման նվազագույն պահանջների կատարումը:

Հոդված 10. Կիբեռանվտանգության մասնագետը

1. Ծառայություն մատուցողը պարտավոր է նշանակել կիբեռանվտանգության մասնագետ կամ մասնագետներ, բացառությամբ սույն օրենքի 19-րդ հոդվածով նախատեսված դեպքի:

2. Կիբեռանվտանգության մասնագետի որակավորման կարգը սահմանում է Ինքնավար մարմնի կողմից հաստատվող կիբեռանվտանգության ապահովման նվազագույն պահանջներով: Ինքնավար մարմինը կարող է սահմանել կիբեռանվտանգության մասնագետին օտարերկրյա որակավորման մարմինների կողմից տրված որակավորման ճանաչման կարգ:

3. Ինքնավար մարմինը որակավորում է կիբեռանվտանգության մասնագետին՝ որակավորման կարգին համապատասխան կամ սահմանված կարգով ճանաչում է որակավորումը:

Հոդված 11. Կիբեռմիջադեպի մասին ծանուցումը

1. Ծառայություն մատուցողը, անկախ այն հանգամանքից, թե տեղեկատվական համակարգը կամ կրիտիկական տեղեկատվական ենթակառուցվածքը շահագործվում է իր, թե այլ անձի կողմից կամ տեղակայված է իր, թե այլ անձի մոտ, պարտավոր է կիբեռմիջադեպի մասին իրեն հայտնի դառնալուց հետո անհապաղ, բայց ոչ ուշ, քան 24 ժամվա ընթացքում Ինքնավար մարմնին ծանուցել այն կիբեռմիջադեպի մասին՝

1) որն էական ազդեցություն ունի տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի շարունակական և անխափան գործունեության կամ դրանց անվտանգ օգտագործման վրա, կամ

2) որի էական ազդեցությունը տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի շարունակական և անխափան գործունեության կամ դրանց անվտանգ օգտագործման վրա թեև տվյալ պահին հնարավոր չէ գնահատել կամ ակնհայտ չէ, բայց ողջամտորեն կարող է ենթադրվել,

2. Կիբեռմիջադեպը էական ազդեցություն ունի, եթե բավարարում է հետևյալ պայմաններից առնվազն մեկին.

1) կիբեռմիջադեպը սպառնում է մարդու կյանքին և առողջությանը, պաշտպանությանը, ազգային անվտանգությանը, միջազգային հարաբերություններին, տնտեսությանը, շրջակա միջավայրին, հասարակական կարգին.

2) կիբեռմիջադեպի հետևանքների ծանրության աստիճանը սույն օրենքի 9-րդ հոդվածի 3-րդ մասի 1-ին կետի համաձայն ռիսկերի գնահատման սանդղակով համարվում է բարձր.

3) սույն օրենքի 9-րդ հոդվածի 2-րդ մասով սահմանված կիբեռանվտանգության ապահովման ներքին կանոնակարգով կամ կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագրով կամ ծառայության շարունակականությունը կամ անվտանգությունը նկարագրող մեկ այլ փաստաթղթով կամ իրավական ակտով (եթե այդպիսին առկա է) նախատեսված է նման կիբեռմիջադեպին արձագանքելու արտակարգ միջոցառումների անհապաղ ձեռնարկում.

4) կիբեռմիջադեպի հետևանքով հնարավոր չէ վերականգնել տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի միջոցով մատուցվող ծառայության շարունակական, անխափան, անվտանգ աշխատանքը՝ օրենսդրությամբ կամ կնքված պայմանագրով նախատեսված առավելագույն թույլատրելի ժամանակահատվածում.

5) կիբեռմիջադեպի պատճառով խաթարվել է այլ ծառայություն մատուցողի ծառայության շարունակականությունը, անխափանությունը կամ անվտանգ օգտագործումը.

6) կիբեռմիջադեպի պատճառով ծառայություն մատուցողը, փոխկապակցված այլ ծառայություն մատուցողը կամ համապատասխան ծառայությունից օգտվողները կրել կամ կարող են կրել զգալի նյութական կամ ոչ նյութական վնաս.

7) ցանկացած այլ անօրինական ներթափանցում կամ միջամտություն, որը ելնելով իր բնույթից, նպատակից, ծագման աղբյուրից, մասշտաբից կամ քանակից կամ դրա կանխարգելման համար պահանջվող ռեսուրսներից և միջոցներից կամ դրանց բավարար համակցությամբ սպառնում է տեղեկատվական համակարգի կամ

կրիտիկական տեղեկատվական ենթակառուցվածքի շարունակական և անխափան գործունեությանը կամ անվտանգ օգտագործմանը:

3. Կիբեռմիջադեպի մասին ծանուցման հետ միասին ծառայություն մատուցողը հնարավորության դեպքում Ինքնավար մարմնին տեղեկություն է տրամադրում կիբեռմիջադեպի առաջացման հավանական պատճառների և հնարավոր հետևանքների մասին:

4. Կիբեռմիջադեպի մասին իրեն հայտնի դառնալուց հետո, 72 ժամվա ընթացքում ծառայություն մատուցողը Ինքնավար մարմին է ներկայացնում կիբեռմիջադեպի վերաբերյալ թարմացված տեղեկատվություն՝ ներառյալ կիբեռմիջադեպի ծանրության և ունեցած հետևանքների մասով:

5. Ինքնավար մարմինը կարող է սեփական հայեցողությամբ ծառայություն մատուցողից պահանջել ներկայացնել թարմացված տեղեկատվություն կիբեռմիջադեպի ծանրության, ձեռնարկված միջոցառումների և ունեցած հետևանքների մասին:

6. Սույն հոդվածի 1-ին մասի 1-ին կետով նախատեսված պարտավորությունը չի սահմանափակում ծառայություններ մատուցողի իրավունքը՝ ծանուցելու այն կիբեռմիջադեպերի մասին, որոնք տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի վրա չունեն էական ազդեցություն:

7. Ծառայություն մատուցողը պարտավոր է կիբեռմիջադեպի մասին իրեն հայտնի դառնալուց հետո անհապաղ կամ նման հնարավորության բացակայության դեպքում երկու օրվա ընթացքում ծանուցել կիբեռմիջադեպի հնարավոր ազդեցության ենթարկված անձանց:

8. Եթե ծառայություն մատուցողը չի կատարում սույն հոդվածի 7-րդ մասում նշված ժամկետներում ծանուցման պարտավորությունը, Ինքնավար մարմինը կարող է ծանուցել կիբեռմիջադեպի հետևանքով հնարավոր ազդեցության ենթարկված անձանց կամ անմիջապես հանրությանը՝ այդ մասին տեղեկացնելով նաև ծառայություն մատուցողին:

9. Սույն հոդվածի 4-րդ մասում նշված տեղեկատվության ներկայացման պահից հետո մեկ ամսվա ընթացքում ծառայություն մատուցողը Ինքնավար մարմին

է ներկայացնում վերջնական հաշվետվություն, որը ներառում է տեղեկություն կիբեռմիջադեպի առաջացման հնարավոր պատճառների, դրա լուծման համար կիրառված միջոցների, կիբեռմիջադեպի ծանրության, ունեցած հետևանքների, դրանց ազդեցության մասշտաբների, ծախսված ժամանակի, ֆինանսական միջոցների, դրա հետագա կանխարգելման ուղղությամբ ձեռնարկված քայլերի և միջոցառումների մասին:

Հոդված 12. Կամավոր ծանուցում

1. Սույն օրենքի իմաստով ծառայություն մատուցող չհանդիսացող անձինք (այդ թվում ֆիզիկական անձինք) Ինքնավար մարմին կարող են ծանուցել կիբեռմիջադեպի, կիբեռհարձակման, կիբեռսպառնալիքի, կամ տեղեկատվական համակարգի և կրիտիկական տեղեկատվական ենթակառուցվածքի խոցելիության մասին:

2. Սույն հոդվածի 1-ին մասով նախատեսված ծանուցումը Ինքնավար մարմինը դիտարկում է սույն օրենքի 7-րդ հոդվածի 2-րդ մասի 10-րդ կետի համաձայն հաստատված կարգով, ընդ որում Ինքնավար մարմինը պարտավոր է ապահովել ծանուցող անձի գաղտնիությունը՝ բացառությամբ հանցագործությունների բացահայտման, նախաքննության և կանխարգելման հետ կապված միջոցառումների իրականացմամբ պայմանավորված համապատասխան իրավասու մարմիններին տեղեկատվության բացահայտման դեպքերի: Միևնույն ժամանակ կիբեռմիջադեպերի վերաբերյալ մեկից ավելի ծանուցումներ ներկայացվելու դեպքում Ինքնավար մարմինը առաջնահերթության կարգով դիտարկում է սույն օրենքով պարտադիր ներկայացման ենթակա ծանուցումները:

3. Կամավոր ծանուցումը սույն հոդվածի 1-ին մասում նշված անձանց համար չի առաջացնում որևէ լրացուցիչ պարտավորություն, որը նրանց համար չէր առաջանա, եթե նրանք Ինքնավար մարմին կամավոր ծանուցում չներկայացնեին, բացառությամբ այն պարտավորությունների, որոնք կապված են հանցագործությունների բացահայտման, նախաքննության և կանխարգելման հետ կապված միջոցառումների իրականացման հետ:

4. Սույն հոդվածի 1-ին մասում նշված տեղեկատվությունը ստանալուց հետո Ինքնավար մարմինն այդ մասին անհապաղ, բայց ոչ ուշ քան 24 ժամվա ընթացքում տեղեկացնում է ծառայություն մատուցողին:

ԳԼՈՒԽ 4
ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄԸ

Հոդված 13. Կիբեռմիջադեպերի հայտնաբերումը, կանխարգելումը և լուծումը, ազգային համակարգչային արտակարգ իրավիճակների արձագանքման թիմը

1. Հայաստանի Հանրապետությունում (ազգային մակարդակում) կիբեռմիջադեպերի հայտնաբերումը, կանխարգելումն ու լուծումը, ինչպես նաև կիբեռմիջադեպերի լուծման ուղղությամբ ծառայություն մատուցողների գործողությունների համակարգումը սույն օրենքով սահմանված կարգով ապահովում է Ինքնավար մարմինը, որի կազմում ձևավորվում է ազգային համակարգչային արտակարգ իրավիճակների արձագանքման թիմը (այսուհետ՝ CERT):

2. Կիբեռանվտանգության ապահովման համար առաջնահերթ են դիտարկվում սույն օրենքի 11-րդ հոդվածի 1-ին և 2-րդ մասերով նկարագրված կիբեռմիջադեպերի լուծումը և դրանց հետևանքների վերացումը:

3. Կիբեռմիջադեպերի հայտնաբերման, կանխարգելման ու լուծման խնդիրները լուծելիս Ինքնավար մարմինը կարող է համագործակցել նաև օտարերկրյա պետությունների համապատասխան համակարգչային արտակարգ իրավիճակների արձագանքման թիմերի կամ միջազգային կազմակերպությունների հետ (այդ թվում կիբեռանվտանգության ապահովմանը աջակցելու նպատակով)՝ Հայաստանի Հանրապետության միջազգային պայմանագրերով և սույն օրենքով սահմանված կարգով:

4. Ինքնավար մարմինը կրիտիկական տեղեկատվական ենթակառուցվածք տիրապետող ծառայություն մատուցողների մոտ, Ինքնավար մարմնի կողմից սահմանած կարգով, նախապես տեղեկացնելով այդ մասին, կարող է իրականացնել խոցելիության գնահատում և ներթափանցման թեստավորում, որն ուղղված է գնահատելու ծառայություն մատուցողների տեղեկատվական համակարգի կամ

կրիտիկական տեղեկատվական ենթակառուցվածքի պաշտպանվածությունը արտաքին ռիսկերից և հնարավոր խոցելիության մասին տեղեկացնել համապատասխան ծառայություն մատուցողին:

5. Կիբեռանվտանգության ապահովման նպատակով Ինքնավար մարմինը մշտադիտարկում է էլեկտրոնային կայքի տիրույթները (դոմեյները)՝ հայկական համացանցային հաղորդակարգի հասցեների (Internet Protocol Addresses) տարածքում և կապված Հայաստան երկրի կոդի հետ, վերլուծում է տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում տեղի ունեցած կիբեռմիջադեպերը և դրանց հնարավոր ազդեցությունը երկրի տնտեսության, շրջակա միջավայրի և մարդու կյանքի և առողջության վրա:

6. Կիբեռմիջադեպը կանխելու և լուծելու նպատակով Ինքնավար մարմինը իրազեկում է հասցեատերերին՝ նշելով այն միջոցները, որոնք անհրաժեշտ է ձեռնարկել՝ կիբեռմիջադեպի հետագա սրացումը կանխելու կամ ազդեցությունը նվազեցնելու համար:

7. Կիբեռսպառնալիքի դեպքում, որը Ինքնավար մարմնի դիտարկմամբ կարող է վերածվել էական ազդեցություն ունեցող կիբեռմիջադեպի, Ինքնավար մարմինը կարող է ծառություն մատուցողի մոտ իրականացնել կիբեռմիջադեպի համատեղ ուսումնասիրություն՝ համագործակցելով համապատասխան ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնի հետ, ծառայություն մատուցողի համաձայնությամբ ունենալ դեպի տեղեկատվական համակարգեր կամ կրիտիկական տեղեկատվական ենթակառուցվածքներ մուտք գործելու հնարավորություն՝ ապահովելու համար կիբեռմիջադեպի պատշաճ հայտնաբերումը և արձագանքումը:

8. Ինքնավար մարմինը ծառայություն մատուցողների կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողների վերաբերյալ տեղեկություն փոխանցելիս պարտավոր է պահպանել տվյալ ծառայություն մատուցողների կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողների վերաբերյալ առևտրային, ինչպես նաև օրենքով պահպանվող այլ գաղտնիքը (այդպիսիք առկա լինելու դեպքում):

9. Սույն օրենքով սահմանված՝ մշակվող, պահպանվող և փոխանցվող տվյալների համար պետք է ապահովվի անվտանգ պահպանության օրենսդրությամբ նախատեսված տեխնիկական և ծրագրային պայմաններ: Այդ տվյալները կարող են հասանելի լինել միայն օրենքով սահմանված կարգով իրավասու մարմինների կամ անձանց համար:

10. Ինքնավար մարմնի CERT թիմի անդամ չեն կարող լինել այն անձինք, ովքեր չեն համապատասխանում «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով սահմանված տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողներին ներկայացվող հիմնական պահանջներին և սահմանափակումներին, ինչպես նաև ճանաչվել են սնանկ և ունեն չմարված (չներված) պարտավորություններ:

Հոդված 14. Ինքնավար մարմնի կողմից տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործումը կամ դրանց հասանելիությունը սահմանափակելը

1. Էական ազդեցություն ունեցող կիբեռմիջադեպի դեպքում Ինքնավար մարմինը իրավասու է ձեռնարկել համապատասխան միջոցներ և ամբողջությամբ կամ մասնակիորեն սահմանափակել ծառայություն մատուցողի կողմից կիրառվող տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործումը կամ դրանց հասանելիությունը՝ հետևյալ պայմանների համաժամանակյա առկայության դեպքում.

1) կիբեռմիջադեպը վտանգի է ենթարկում կամ վնասում է այլ տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգությանը,

2) ծառայություն մատուցողի կիբեռանվտանգության մասնագետը չի կարողանում կամ ժամանակին ի վիճակի չէ դիմակայել էական ազդեցություն ունեցող կիբեռմիջադեպին կամ վերացնել կիբեռմիջադեպի հետևանքով առաջացած այլ կիբեռսպառնալիքները,

3) Ինքնավար մարմնի պատճառաբանված և հիմնավորված եզրակացությամբ, այլ ճանապարհով հնարավոր չէ հակազդել կիբեռմիջադեպին

կամ կանխել դրա հետագա սրացումը կամ առավել նվազ միջամտությամբ չեզոքացնել բացասական ազդեցությունը,

4) կիբեռմիջադեպից բխող այլ կիբեռսպառնալիքներին հակազդելու կամ կիբեռմիջադեպի հետևանքները վերացնելու արդյունքում ծառայություն մատուցողին անհամաչափ վնաս չի պատճառվում:

2. Սույն հոդվածի 1-ին մասով նախատեսված միջոցի կիրառության մասին ծառայություն մատուցողն անհապաղ, բայց ոչ ուշ, քան 24 ժամվա ընթացքում տեղեկացվում է Ինքնավար մարմնի կողմից:

3. Սույն հոդվածի 1-ին մասով նախատեսված միջոցի կիրառումը համաձայնեցնվում է համապատասխան ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնի հետ: Այն դեպքում, երբ էական ազդեցություն ունեցող կիբեռմիջադեպի հետևանքները մեղմացնելու, դրա արագ սրացումը (ազդեցության մասշտաբների ընդլայնումը) կանխելու համար պահանջվում է հրատապ միջոցառումների ձեռնարկում և Ինքնավար մարմնի կողմից գնահատվում է, որ հապաղելու արդյունքում Հայաստանի Հանրապետության քաղաքացիներին կամ պետությանը պատճառվող վնասի չափերը կմեծանան, Ինքնավար մարմինը սույն հոդվածի 1-ին մասում նշված միջոցը կիրառում է՝ նախապես այն չհամաձայնեցնելով համապատասխան ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնի հետ: Սույն մասում նշված դեպքում կիրառված միջոցի մասին Ինքնավար մարմինը, առաջին իսկ հնարավորության դեպքում, սակայն ոչ ուշ քան էական ազդեցություն ունեցող կիբեռմիջադեպից հետո 1 (մեկ) օրվա ընթացքում տեղեկացնում է համապատասխան ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնին՝ ներկայացնելով մանրամասն տեղեկատվություն կիբեռմիջադեպի բնույթի, ձեռնարկված քայլերի, դրանց անհրաժեշտության և անհետաձգելիության մասին:

4. Սույն հոդվածի 1-ին մասով նախատեսված միջոցի կիրառության դեպքում կազմվում է արձանագրություն:

Հոդված 15. Կիբեռմիջադեպերի գրանցամատյան

1. Կիբեռմիջադեպերի գրանցամատյանը Ինքնավար մարմնի կողմից վարվող տվյալների շտեմարան է, որտեղ մուտքագրվում են կիբեռմիջադեպերը նկարագրող տվյալներ՝ կիբեռմիջադեպերի վերաբերյալ տվյալները գրանցելու, դրանք կանխարգելելու, լուծելու, ծանուցումներ ուղարկելու, վերահսկողական և մշտադիտարկման, ինչպես նաև սույն օրենքից բխող այլ գործառույթների իրականացման նպատակով վերլուծելու համար:

2. Կիբեռմիջադեպերի գրանցամատյանում ստացվող, վերլուծվող և տրամադրվող տվյալները դասակարգվում են և դրանց գաղտնիության աստիճանը որոշվում է օրենքով սահմանված կարգով: Գրանցամատյանի մուտքը սահմանափակված է, և դրանում պահվող տվյալները նախատեսված են ներքին օգտագործման համար, եթե այլ բան նախատեսված չէ օրենքով: Կիբեռմիջադեպերի գրանցամատյանի տեղեկությունները կարող են օգտագործվել միայն սույն օրենքով սահմանված նպատակներով:

3. Ինքնավար մարմնի աշխատակիցները, որոնց հասանելի են կիբեռմիջադեպերի գրանցամատյանում ստացվող, վերլուծվող և տրամադրվող տվյալները, պահպանում են այդ տվյալների գաղտնիությունը իրենց պարտականությունների կատարման ընթացքում և դրանց դադարումից հետո, ինչպես նաև օրենքով սահմանված կարգով պատասխանատվություն են կրում դրա անօրինական հրապարակման կամ երրորդ անձի փոխանցելու համար:

ԳԼՈՒԽ 5
ԿԵՆՍԱԿԱՆ ՆՇԱՆԱԿՈՒԹՅԱՆ ՈԼՈՐՏՆԵՐԻ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԱՌԱՆՁՆԱՀԱՏԿՈՒԹՅՈՒՆՆԵՐԸ

Հոդված 16. Կենսական նշանակության ոլորտները և դրանցում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքները

1. Կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշները հաստատում է Հայաստանի Հանրապետության կառավարությունը, որոնց մշակման համար Լիազոր մարմինը հիմք է ընդունում հետևյալ հանգամանքները՝

1) կիբեռմիջադեպի հնարավոր ազդեցությունը մեկ կամ մի քանի կենսական նշանակության ծառայությունների մատուցման վրա (համակարգային էֆեկտ).

2) կիբեռմիջադեպի տևողությունը և վտանգավորության աստիճանը տնտեսական ակտիվության, շրջակա միջավայրի, բնակչության բնականոն կենսագործունեության ապահովման համար, ազգային անվտանգության կամ բնակչության առողջության վրա.

3) օգտվողների թիվը.

4) կրիտիկական տեղեկատվական ենթակառուցվածքի վերականգման կամ նորի ստեղծման համար անհրաժեշտ ֆինանսական ծախսերի գնահատականը և տվյալ պահի հաշվեկշռային արժեքը:

2. Կենսական նշանակության ոլորտներում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկը հաստատում է Հայաստանի Հանրապետության կառավարությունը, ըստ կիբեռանվտանգության ապահովման համար պատասխանատու պետական մարմինների:

3. Սույն օրենքի իմաստով կենսական նշանակության ոլորտներ են՝

1) Էներգետիկայի ոլորտ.

2) Արտադրության ոլորտ (քիմիական, սննդամթերքի, զենքի և զինամթերքի, բժշկական, էլեկտրական, համակարգչային, էլեկտրոնային և օպտիկական սարքերի արտադրության).

3) Տրանսպորտային ոլորտ.

4) Ջրի մատակարարման և կեղտաջրերի հեռացման ոլորտ.

5) Կապի, այդ թվում՝ հեռահաղորդակցության ոլորտ.

6) Փոստային կապի գործունեության ոլորտ.

7) Ֆինանսական ծառայությունների ոլորտ.

8) Առողջապահության ոլորտ.

9) Տեղեկատվական տեխնոլոգիաների ոլորտ, այդ թվում՝ թվային ենթակառուցվածքներ.

10) Ռադիոակտիվ, ընդերքօգտագործման և վտանգավոր թափոնների կառավարման ոլորտ.

11) Տիեզերական գործունեության ոլորտ.

12) Տվյալների շտեմարանների կառավարման և շահագործման ոլորտ.

13) Արտակարգ իրավիճակներում անվտանգության ապահովման ոլորտ.

14) Պետական կառավարման ոլորտ, այդ թվում՝ պետական մարմինների կողմից շահագործվող թվային ենթակառուցվածքներ:

4. Կենսական նշանակության ոլորտներում ծառայությունների տեսակները, ըստ տնտեսական գործունեության տեսակների դասակարգիչների, սահմանում է Հայաստանի Հանրապետության կառավարությունը՝ ծառայություններ մատուցողներին նույնականացնելու համար:

5. Ինքնավար մարմինը, սույն հոդվածի 1-ին մասում նշված նույնականացման չափանիշների հիման վրա, կարող է առանձին տեղեկատվական համակարգեր ժամանակավորապես ճանաչել որպես կենսական նշանակության ոլորտում կրիտիկական տեղեկատվական ենթակառուցվածք, այդ մասին ծանուցել ծառայություն մատուցողին և սահմանել միջոցառումներ, որոնք պետք է իրականացվեն: Ծանուցման մեջ սահմանվում է ողջամիտ ժամկետ, դրանց իրականացման համար: Ժամանակավորապես կրիտիկական տեղեկատվական ենթակառուցվածք ճանաչված տեղեկատվական համակարգի համար սահմանվող միջոցառումները պետք է համապատասխանեն խոցելիության գնահատման արդյունքում բացահայտված ռիսկերը նվազեցնելու նպատակին:

6. Սույն հոդվածի 5-րդ մասում նշված ծանուցումից հետո չորս ամսվա ընթացքում Ինքնավար մարմինը միջոցներ է ձեռնարկում ժամանակավորապես կրիտիկական տեղեկատվական ենթակառուցվածք ճանաչված տեղեկատվական համակարգը սույն հոդվածի 2-րդ մասում նշված ցանկում ներառելու համար: Սույն մասում նշված ժամկետի ավարտից հետո տեղեկատվական համակարգը սույն հոդվածի 2-րդ մասում նշված ցանկում չներառելու պարագայում այն այլևս չի հանդիսանա կրիտիկական տեղեկատվական ենթակառուցվածք:

Հոդված 17. Տեղեկատվական համակարգում և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման հիմնական պայմանները

1. Տեղեկատվական համակարգերում կիբեռանվտանգության ապահովման համար սույն օրենքով, այլ օրենքներով դրա հիման վրա ընդունված իրավական ակտերով և «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով նախատեսված կարգավորման գործառույթներից բխող պահանջների, այդ թվում՝ կիբեռանվտանգության ապահովման նվազագույն պահանջների, կատարումը պարտադիր է: Ծառայություն մատուցողի կարգավորող և վերահսկող այլ մարմինը կարող է սահմանել կիբեռանվտանգության ապահովման նվազագույն պահանջներից ավելի խիստ պահանջներ, հաշվի առնելով կարգավորվող ոլորտի առանձնահատկությունները: Այդպիսի պահանջներ սահմանված լինելու դեպքում օրենքով նախատեսված աուդիտ, վերահսկողություն և մշտադիտարկում իրականացվում է՝ հիմք ընդունելով նաև այդ պահանջները:

2. Կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովման համար, բացի սույն հոդվածի 1-ին մասով սահմանված պահանջների կատարումից, ծառայություն մատուցողները պարտավոր են սույն օրենքով սահմանված կարգով և ժամկետներում անցնել կիբեռանվտանգության աուդիտ՝ կիրառելի միջազգային ստանդարտի (ինչպիսին է օրինակ՝ ստանդարտացման միջազգային կազմակերպության (ISO) ստանդարտը) կամ ազգային ստանդարտի հիման վրա: Կիրառելի միջազգային ստանդարտների ցանկը սահմանում է Հայաստանի Հանրապետության կառավարությունը:

3. Տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կառավարումը կամ շահագործումը (host of the system) կամ փոխգործելիությունը այլ անձի պատվիրակելու դեպքում, կիրառված կիբեռանվտանգության ապահովման միջոցների համար պատասխանատվություն կրում և Ինքնավար մարմնի հետ կոնտակտային կետ հանդիսանում է ծառայություն մատուցողը:

4. Տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովումը կիբեռանվտանգության

ապահովման ծառայություն մատուցողի պատվիրակելու դեպքում, կիրառված կիբեռանվտանգության ապահովման միջոցների համար պատասխանատվություն կրում և Ինքնավար մարմնի հետ կոնտակտային կետ հանդիսանում է ծառայություն մատուցողը:

5. Ծառայություն մատուցողը մինչև պատվիրակման համապատասխան պայմանագրի կնքումը և դրանից հետո.

1) պարտավոր է գնահատել և կառավարել այն ռիսկերը, որոնք կարող են ազդել տեղեկատվական համակարգում կամ կրիտիկական տեղեկատվական ենթակառուցվածքում պահվող տվյալների գաղտնիության, հասանելիության կամ ամբողջականության վրա,

2) պարտավոր է գնահատել և հավաստիանալ, որ կիբեռանվտանգության ապահովման ծառայություն մատուցողն ունի կիբեռանվտանգության ոլորտի օրենսդրությամբ սահմանված պահանջների վերաբերյալ բավարար գիտելիքներ և կիրառման փորձ, գործնական գիտելիքներ և փորձ, աշխատողների համար ստեղծված են բավարար պայմաններ՝ սույն օրենքի 4-րդ հոդվածով սահմանված սկզբունքների պահպանմամբ ծառայություններ մատուցելու համար:

6. Ծառայություն մատուցողը տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովման պատվիրակումը նախապես համաձայնեցնում է Ինքնավար մարմնի հետ: Սույն մասով նախատեսված պատվիրակման համաձայնեցման կարգը և ներկայացվող տեղեկությունների ցանկը հաստատում է Ինքնավար մարմինը:

Հոդված 18. Կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման առանձնահատկությունները

1. Կրիտիկական տեղեկատվական ենթակառուցվածքում կիբեռանվտանգության պետական կառավարումը և կարգավորումն իրականացվում է հաշվի առնելով Հայաստանի Հանրապետության կառավարության կողմից հաստատված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկը:

2. Ծառայություն մատուցողը պարտավոր է սույն օրենքից բխող կազմակերպչական, տեխնիկական, ծրագրային միջոցներ ձեռնարկել կրիտիկական

տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության պատշաճ ապահովման համար, համագործակցել իրավասու պետական մարմինների հետ, ստանալ տեղեկատվություն և խորհրդատվություն կիբեռմիջադեպերից պաշտպանության միջոցների, ինչպես նաև դրանց հայտնաբերման, կանխարգելման, հետևանքների վերացման մեթոդների վերաբերյալ:

ԳԼՈՒԽ 6
ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԾԱՌԱՅՈՒԹՅՈՒՆ ՄԱՏՈՒՑՈՂՆԵՐԻՆ ՆԵՐԿԱՅԱՑՎՈՂ ՊԱՀԱՆՋՆԵՐԸ

Հոդված 19. Կիբեռանվտանգության ապահովման ծառայություն մատուցողներին ներկայացվող պահանջները

1. Կիբեռանվտանգության ապահովումը կարող է պատվիրակվել կիբեռանվտանգության ապահովման ծառայություն մատուցողի, որը ունի կիբեռանվտանգության ոլորտում կիրառելի միջազգային ստանդարտով կամ ազգային ստանդարտով սահմանված չափանիշներին և պահանջներին համապատասխանությունը հավաստող փաստաթուղթ:

2. Կիբեռանվտանգության ապահովումն այլ պետություններում գրանցված կամ գործունեություն իրականացնող կիբեռանվտանգության ապահովման ծառայություն մատուցողի պատվիրակելու դեպքում, միջազգային ստանդարտով կամ ազգային ստանդարտով սահմանված չափանիշներին և պահանջներին համապատասխանությունը հավաստող փաստաթուղթ ճանաչում է Ինքնավար մարմինը, Հայաստանի Հանրապետությունում կիրառելի՝ միջազգային համագործակցության մասին համաձայնագրերի (պայմանագրերի) հիման վրա:

3. Կիբեռանվտանգության ապահովման ծառայություն մատուցողը պարտավոր է սույն օրենքի 20-րդ հոդվածի 2-րդ մասով սահմանված կարգով անցնել կիբեռանվտանգության աուդիտ: Աուդիտի արդյունքներով կազմված հաշվետվությունն այն ստանալուց հետո տասնհինգ օրվա ընթացքում ներկայացվում է Ինքնավար մարմին և ծառայություն մատուցողին:

4. Կիրառելի միջազգային ստանդարտների ցանկը սահմանում է Հայաստանի Հանրապետության կառավարությունը:

ԳԼՈՒԽ 7
ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՈՒԴԻՏ

Հոդված 20. Կիբեռանվտանգության աուդիտ

1. Կիբեռանվտանգության աուդիտի արդյունքում գնահատվում է ծառայության մատուցողի կիբեռանվտանգության ապահովման ներքին կանոնակարգի և դրա կիրարկման համապատասխանությունը սույն օրենքի պահանջներին:

2. Ծառայություն մատուցողը պարտավոր է երեք տարին մեկ անցնել կիբեռանվտանգության աուդիտ, եթե կիրառելի միջազգային ստանդարտով կամ ազգային ստանդարտով այլ ժամկետ սահմանված չէ: Աուդիտի արդյունքներով կազմված հաշվետվությունը այն ստանալուց հետո մեկ ամսվա ընթացքում ներկայացվում է Ինքնավար մարմին: Կիրառելի միջազգային ստանդարտների ցանկը սահմանում է Հայաստանի Հանրապետության կառավարությունը:

3. Ինքնավար մարմինը կիբեռանվտանգության աուդիտորների որակավորմանը ներկայացվող պահանջներին համապատասխան որակավորում է ֆիզիկական անձանց և կազմակերպությունների, ինչպես նաև իրականացնում Հայաստանի Հանրապետությունում ընդունելի՝ միջազգայնորեն ճանաչված աուդիտորի որակավորում ունեցող անձանց հաշվառում և վերջիններիս ցանկի հրապարակումը Ինքնավար մարմնի պաշտոնական կայքէջում:

4. Շահագործվող տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի առանձնահատկություններով պայմանավորված ծառայություն մատուցողը կարող է իր ինքնուրույն որոշմամբ սույն հոդվածի 2-րդ մասում նշված ժամկետից շուտ անցնել կիբեռանվտանգության աուդիտ:

5. Այն դեպքում, երբ Ինքնավար մարմինն ուսումնասիրության արդյունքում պարզում է, որ ծառայություն մատուցողի մոտ կիբեռանվտանգության աուդիտը չի իրականացվել սույն օրենքի կամ կիբեռանվտանգության աուդիտի պահանջներին համապատասխան, կարող է ծառայություն մատուցողից պահանջել անցնել կիբեռանվտանգության նոր աուդիտ:

6. Կիբեռանվտանգության աուդիտ իրականացնող անձը վճարվում է ծառայություն մատուցողի կողմից:

ԳԼՈՒԽ 8
ՕՐԵՆՔԻ ԵՎ ԴՐԱ ՀԻՄԱՆ ՎՐԱ ԸՆԴՈՒՆՎԱԾ ԻՐԱՎԱԿԱՆ ԱԿՏԵՐԻ ՊԱՀԱՆՋՆԵՐԻ ԿԱՏԱՐՄԱՆ ՆԿԱՏՄԱՄԲ ՎԵՐԱՀՍԿՈՂՈՒԹՅՈՒՆԸ, ՄՇՏԱԴԻՏԱՐԿՈՒՄԸ, ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ

Հոդված 21. Օրենքի և դրա հիման վրա ընդունված իրավական ակտերի պահանջների պահպանման նկատմամբ վերահսկողությունը

1. Ինքնավար մարմինը սույն օրենքի և դրա հիման վրա ընդունված իրավական ակտերի պահանջների պահպանման նկատմամբ վերահսկողություն իրականացնում է «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով սահմանված կարգով:

2. Ինքնավար մարմինը կարգավորող և վերահսկող այլ մարմինների կողմից շահագործվող կենսական նշանակության տեղեկատվական համակարգերի կամ կրիտիկական տեղեկատվական ենթակառուցվածքների նկատմամբ վերահսկողություն իրականացնում է մշտադիտարկման միջոցով՝ նշված մարմիններից ստացված, սույն օրենքով սահմանված աուդիտի արդյունքների հիման վրա:

Հոդված 22. Ինքնավար մարմնի կողմից իրականացվող մշտադիտարկումը

1. Ինքնավար մարմինը սույն օրենքով սահմանված դեպքերում և կարգով իրականացնում է ծառայություն մատուցողների գործունեության մշտադիտարկում՝ (այսուհետ՝ մշտադիտարկում) ծառայություն մատուցողների տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում կիրառվող կիբեռանվտանգության ապահովման միջոցների համապատասխանությունը սույն օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական իրավական ակտերով սահմանված պահանջներին գնահատելու նպատակով:

2. Մշտադիտարկումը կարող է իրականացվել ինչպես Ինքնավար մարմնում, այնպես էլ ծառայություն մատուցողի համաձայնությամբ իր տարածքում՝ ծառայություն մատուցողի գտնվելու կամ գործունեության իրականացման վայրում:

3. Մշտադիտարկում իրականացնելիս կարող են կիրառվել համակարգչային տեխնոլոգիաներ և այլ տեխնիկական կամ ծրագրային միջոցներ, էլեկտրոնային և այլ սարքավորումներ, կրիչներ, կատարվել այլ գործողություններ՝ ուղղված մշտադիտարկման իրականացմանն ու արդյունքների ամփոփմանը:

4. Ինքնավար մարմնի կողմից ծառայություն մատուցողի մոտ մշտադիտարկումն իրականացվում է հետևյալ եղանակներով.

1) կիբեռանվտանգության ապահովման նվազագույն պահանջներին համապատասխանության գնահատում.

2) ռիսկերի գնահատման հիման վրա կազմված կիբեռմիջադեպերի կանխարգելման միջոցառումների ծրագրով նախատեսված առանձին միջոցառումների կատարման համապատասխանության գնահատում.

3) որակավորված աուդիտորի կողմից կիբեռանվտանգության աուդիտի արդյունքներով կազմված հաշվետվության պահանջների կատարման գնահատում.

օրենքով նախատեսված այլ դեպքերում:

4. Նախքան ծառայություն մատուցողի տարածքում մշտադիտարկման իրականացումը Ինքնավար մարմինն այդ մասին տեղեկացնում է ծառայություն մատուցողին, ինչպես նաև համապատասխան ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնին՝ նշելով մշտադիտարկման առարկան, նպատակը, ժամանակահատվածը, իրականացման վայրը:

5. Մշտադիտարկման արդյունքներով կազմվում է արձանագրություն, որի վերաբերյալ ծառայություն մատուցողը այն ստանալու օրվանից հետո՝ յոթնօրյա ժամկետում, իրավունք ունի Ինքնավար մարմնին ներկայացնելու առարկություններ կամ առաջարկություններ:

6. Ինքնավար մարմինը կարող է ծառայություն մատուցողին տալ պարտադիր կատարման ենթակա ցուցումներ, սահմանել ժամանակացույց՝ ծառայություն մատուցողի կողմից տրված ցուցումների կատարման կամ թերությունների վերացման նպատակով՝ համաձայնեցնելով համապատասխան

ծառայություն մատուցողին կարգավորող և վերահսկող այլ մարմնի հետ: Ծառայություն մատուցողը պարտավոր է սահմանված ժամանակացույցի համաձայն կատարել Ինքնավար մարմնի տրված ցուցումները կամ վերացնել արձանագրված թերությունները և այդ մասին տեղեկացնել Ինքնավար մարմին՝ ներկայացնելով ապացույցներ:

7. Մշտադիտարկման արդյունքների հիման վրա պատասխանատվության միջոցներ չեն կարող կիրառվել:

Հոդված 23. Ինքնավար մարմնի օրինական պահանջները չկատարելու հետևանքները

1. Եթե ծառայություն մատուցողը կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողը չի կատարում Ինքնավար մարմնի օրինական պահանջները, ապա Ինքնավար մարմինը.

1) դիմում է ծառայություն մատուծողի կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողի վերադաս մարմնին կամ համապատասխան պաշտոնատար անձին՝ պարտականությունների կատարման մեջ թերացած անձի նկատմամբ կարգապահական պատասխանատվության միջոց կիրառելու գործընթաց սկսելու համար.

2) դիմում է ծառայություն մատուծողի կարգավորող և վերահսկող այլ մարմնին՝ համապատասխան վարույթ հարուցելու և պատասխանատվության միջոց կիրառելու պահանջով.

3) օրենքով սահմանված կարգով նախաձեռնում է համապատասխանության գնահատում անցկացնելու գործընթաց.

4) ամբողջությամբ կամ մասնակիորեն սահմանափակում է պետական տեղեկատվական համակարգի կամ տվյալների փոխանակման շերտի օգտագործման հնարավորությունը՝ մինչև Ինքնավար մարմնի օրինական պահանջների կատարումը, եթե ունի հիմնավոր կասկածներ, որ նշված սահմանափակումը չկիրառելը կարող է խափանել պետական տեղեկատվական համակարգի անվտանգ և անխափան աշխատանքը:

2. Սույն հոդվածի 1-ին մասի 4-րդ կետով նախատեսված հետևանքը կարող է կիրառվել ինչպես առանձին, այնպես էլ 1-ին կամ 2-րդ կամ 3-րդ կետերի հետ միաժամանակ:

3. Կարգապահական պատասխանատվության միջոց կիրառելու իրավունք ունեցող պաշտոնատար անձը պարտավոր է դիմումը ստանալու պահից մեկամսյա ժամկետում ձեռնարկել միջոցներ և արդյունքների մասին տեղեկացնել Ինքնավար մարմնին:

4. Ծառայություն մատուցողի կարգավորող և վերահսկող այլ մարմինը համապատասխան վարույթ հարուցելու և պատասխանատվության միջոց կիրառելու դիմումի ընթացքի մասին Ինքնավար մարմնին տեղեկացնում է դիմումը ստանալու պահից տասնհինգ օրվա ընթացքում:

Հոդված 24. Պատասխանատվությունը սույն օրենքի պահանջների խախտման համար

1. Սույն օրենքի պահանջների խախտումն առաջացնում է օրենքով սահմանված վարչական կամ քրեական պատասխանատվություն:

2. Ծառայություն մատուցողը կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողը կամ նրանց աշխատողները (ղեկավարները) չեն կարող ենթարկվել գույքային, վարչական պատասխանատվության՝ սույն օրենքից բխող իրենց պարտականությունների պատշաճ կատարման համար:

3. Ինքնավար մարմնի հանրային ծառայողները կամ աշխատակիցները չեն կարող ենթարկվել գույքային, վարչական պատասխանատվության սույն օրենքով նախատեսված իրենց պարտականությունների պատշաճ կատարման համար:

ԳԼՈՒԽ 9
ԵԶՐԱՓԱԿԻՉ ՄԱՍ ԵՎ ԱՆՑՈՒՄԱՅԻՆ ԴՐՈՒՅԹՆԵՐ

Հոդված 25. Եզրափակիչ մաս և անցումային դրույթներ

1. Սույն օրենքն ուժի մեջ է մտնում պաշտոնական հրապարակմանը հաջորդող տասներորդ օրը, բացառությամբ.

1) սույն օրենքի 8-րդ հոդվածի, որն ուժի մեջ է մտնում նշված հոդվածի 2-րդ մասով սահմանված ենթաօրենսդրական նորմատիվ իրավական ակտի ուժի մեջ մտնելուց հետո,

2) սույն օրենքի 9-րդ հոդվածի 2-րդ մասի, 3-րդ մասի 1-2-րդ, 4-6-րդ և 13-րդ կետերի, որոնք ուժի մեջ են մտնում համապատասխան ենթաօրենսդրական նորմատիվ իրավական ակտերի ուժի մեջ մտնելուց հետո:

2. Ծառայություն մատուցողները, ովքեր շահագործում են կրիտիկական տեղեկատվական ենթակառուցվածքներ և կիբեռանվտանգության ապահովման ծառայություն մատուցողները օրենքի ուժի մեջ մտնելուց հետո քսանչորսամսյա ժամկետում Ինքնավար մարմին են ներկայացնում կիբեռանվտանգության ոլորտում միջազգային ստանդարտով կամ ազգային ստանդարտով սահմանված չափանիշներին և պահանջներին համապատասխանությունը հավաստող փաստաթուղթ:

3.Կիբեռանվտանգության ապահովման ծառայություն մատուցողները կիբեռանվտանգության աուդիտ անցնում են կիբեռանվտանգության ոլորտում միջազգային կամ ազգային ստանդարտներով սահմանված համապատասխանություն հավաստող փաստաթուղթ ստանալուց հետո մեկ տարի անց:

4. Սույն օրենքից բխող ենթաօրենսդրական նորմատիվ իրավական ակտերն, այդ թվում ազգային ստանդարտն ընդունվում են սույն օրենքն ուժի մեջ մտնելուց հետո՝ տասներկուամսյա ժամկետում:

5.Ծառայություն մատուցողներն իրենց կիբեռանվտանգության ապահովման ներքին կանոնակարգերը ընդունում, իրենց կողմից կիրառվող տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում ռիսկերի գնահատումը, կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագրի մշակումն իրականացնում են սույն օրենքի ուժի մեջ մտնելուց հետո՝ տասութամսյա ժամկետում: