Լրամշակված նախագիծ

Կ-1139-20.08.2025-ՊԻ-011 *Երկրորդ ընթերցում*

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 կամ անհատ ձեռնարկատեր, որը սույն օրենքի իմաստով չի համարվում ծառայություն մատուցող, 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 4-րդ մասում թվարկված կենսական նշանակության ոլորտներից մեկում կամ մի քանիսում միաժամանակ և շահագործում են տեղեկատվական համակարգ կամ կրիտիկական տեղեկատվական ենթակառուցվածք,

2) պետական և տեղական ինքնակառավարման մարմինների վրա:

4. Սույն օրենքի գործողությունը չի տարածվում «Փոքր և միջին ձեռնարկատիրության պետական 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 շահագործվող 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 շահագործմանն 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 ճշգրտությունը .

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 ճշգրտությունը 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, հասարակական կարգի, միջազգային հարաբերությունների և կառավարման շարունակականության (governance continuity) 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 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 շահագործման 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 անձ, անհատ ձեռնարկատեր կամ աշխատանքային պայմանագրով ներգրավված ֆիզիկական անձ, ովքեր մատուցում են 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 կիբեռանվտանգության ապահովումը կազմակերպում է այն շահագործող ծառայություն մատուցողը.

2) **համապարփակ պաշտպանության սկզբունք՝** ծառայություն մատուցողը պետք է գնահատի իր կողմից շահագործվող 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 տվյալներին ունենա ոչ ավելի հասանելիություն, քան անհրաժեշտ է իր աշխատանքային պարտականությունների կամ գործառույթների պատշաճ իրականացման համար.

5) **տվյալների գաղտնիության սկզբունք (confidentiality)՝** տվյալները պետք է հասանելի լինեն միայն այն անձանց համար, ովքեր ունեն համապատասխան հասանելիության թույլտվություն.

6) **համագործակցության սկզբունք՝** 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 սկզբունք (integrity)** ՝ ծառայություն մատուցողները պետք է պաշտպանեն տեղեկությունը չարտոնված փոփոխումից կամ ոչնչացումից՝ ապահովելով դրա անխաթարությունը, իսկությունը, հուսալիությունը և ճշգրտությունը.

8) հասանելիության սկզբունք (availability)՝ 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

1. 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 կամ գործողությունների 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 Կառավարության հաստատմանը.

7) արտակարգ իրավիճակներում, արտակարգ կամ ռազմական դրության ժամանակ դրա տևողության ամբողջ ընթացքում տեղեկատվական համակարգերում և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության

ապահովման միջոցառումների ձեռնարկում և դրանց իրականացման նկատմամբ հսկողության ապահովում.

8) կենսական նշանակության ոլորտներում նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների, դրանք շահագործող ծառայություն մատուցողների և կիբեռանվտանգության պահանջների ապահովման, վերահսկման համար պատասխանատու պետական մարմինների ցանկը սահմանելու մասին Կառավարության որոշման նախագծի մշակում և ներկայացում Կառավարության հաստատմանը.

9) կենսական նշանակության ոլորտներում ծառայությունների տեսակներն ըստ տնտեսական գործունեության տեսակների դասակարգիչների սահմանելու մասին Կառավարության որոշման նախագծի մշակում և ներկայացում Կառավարության հաստատմանը.

10) ծառայություն մատուցող չհամարվող իրավաբանական անձի կամ անհատ ձեռնարկատիրոջ կողմից սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամավոր ստանձնելու և դրանցից հրաժարվելու դեպքերի սահմանման մասին կարգի մշակում և ներկայացում Կառավարության հաստատմանը.

11) կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշները սահմանելու մասին Կառավարության որոշման նախագծի մշակում և ներկայացում 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 գրանցամատյան.

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 պահպանմանն ուղղված, մշակում և իրականացնում է իրազեկման և կրթական ծրագրեր՝ համագործակցելով Լիազոր մարմնի և կրթության ոլորտում պատասխանատու պետական մարմինների, ինչպես նաև իրավաբանական անձանց հետ, 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 4-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 շահագործող 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) սույն օրենքով սահմանված կարգով իրականացնում է ծառայություն մատուցողների կողմից սույն օրենքով սահմանված պահանջների պահպանման նկատմամբ մշտադիտարկում, 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) Լիազոր մարմնին ներկայացնում է առաջարկություններ Կառավարության որոշմամբ հաստատված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկում փոփոխություններ կամ լրացումներ կատարելու վերաբերյալ.

22) կիբեռանվտանգության վերաբերյալ հարցերով փորձագիտական աջակցություն է ցուցաբերում 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 (Security Operations Center (SOC) ծառայություններ.

29) օրենքով նախատեսված լիազորությունների իրականացման նպատակով ձևավորում է աշխատանքային խմբեր, հանձնաժողովներ, սույն օրենքի 16-րդ հոդվածի 1-ին մասով սահմանված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման նպատակով ստեղծում է միջգերատեսչական հանձնաժողով.

30) սույն օրենքի 16-րդ հոդվածի 1-ին մասով նախատեսված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշների հիման վրա նույնականացնում է կրիտիկական տեղեկատվական ենթակառուցվածքները, նախնական մշակում է նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկն՝ ըստ դրանք շահագործող ծառայություն մատուցողների և ներկայացնում Լիազոր մարմնին.

31) սույն օրենքի 16-րդ հոդվածի 5-րդ մասի համաձայն նախնական մշակում է կենսական նշանակության ոլորտներում ծառայությունների տեսակների ցանկը՝ ըստ տնտեսական գործունեության տեսակների դասակարգիչների և ներկայացնում է Լիազոր մարմնին.

32) 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 հաստատված ընթացակարգերին համապատասխան փոխանցել բացառապես 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 մասի 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 4-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 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:

8. Ինքնավար մարմինը տեղեկատվական տեխնոլոգիաների ակտիվների ռեեստրի ստեղծման և կառավարման համակարգի ներդրման Կառավարության կողմից սահմանած կարգին համապատասխան դրանում նշված մարմիններին և

կազմակերպություններին տրամադրում է գույքագրման գործիքակազմ, իրականացնում է տեղեկատվական տեխնոլոգիաների ռեեստրի աուդիտ, ինչպես նաև կատարում է մեթոդական վերլուծություն:

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 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 շահագործման, 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, հիմք ընդունելով սույն օրենքի 9-րդ հոդվածի 3-րդ մասի 1-ին կետով սահմանված իր տեղեկատվական համակարգերի ռիսկերի գնահատումը, ռիսկերի գնահատման սանդղակը և կիբեռանվտանգության գործառնության (operational) մոդելը, պարտավոր է նշանակել կիբեռանվտանգության մասնագետ կամ մասնագետներ, բացառությամբ սույն օրենքի 19-րդ հոդվածով նախատեսված կիբեռանվտանգության ապահովումն ամբողջությամբ կիբեռանվտանգության ապահովման ծառայություն մատուցողին պատվիրակելու դեպքի:

2. Կիբեռանվտանգության մասնագետի որակավորման կարգը և որակավորման ճանաչման կարգը սահմանվում է Ինքնավար մարմնի կողմից հաստատվող կիբեռանվտանգության ապահովման նվազագույն պահանջներով: Ինքնավար մարմինը սահմանում է կիբեռանվտանգության մասնագետին

օտարերկրյա որակավորման մարմինների կողմից տրված որակավորման ճանաչման կարգը:

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 շահագործման վրա, կամ

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

2. Կիբեռմիջադեպն 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 շահագործմանը:

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 մատուցողն 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 ծանուցումն 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 մարմինն 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 շահագործող 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 (դոմեյնները)՝ 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, որն 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 ստանալիս կամ 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 կամ համապատասխանում են նույն օրենքով սահմանված տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողներին ներկայացվող հիմնական սահմանափակումներին, կամ ճանաչվել են սնանկ և ունեն չմարված (չներված) պարտավորություններ:

Հոդված 14. Ինքնավար մարմնի կողմից տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի շահագործումը 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 շահագործումը 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 Կառավարությունը, որոնց մշակման համար Ինքնավար մարմինը հիմք է ընդունում հետևյալ հանգամանքները՝

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

2) կիբեռմիջադեպի տևողությունը և վտանգավորության աստիճանը տնտեսական ակտիվության, շրջակա միջավայրի, հասարակական կարգի, բնակչության բնականոն կենսագործունեության ապահովման համար, միջազգային

հարաբերությունների, կառավարման շարունակականության (governance continuity), 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 նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների, դրանք շահագործող ծառայություն մատուցողների և կիբեռանվտանգության պահանջների ապահովման, վերահսկման համար պատասխանատու պետական մարմինների ցանկը հաստատում է Կառավարությունը:

3. Օրենքի ուժով, առանց նույնականացման չափանիշների կիրառման, կրիտիկական տեղեկատվական ենթակառուցվածքներ են համարվում.

1) որակավորված վստահության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

2) բարձր մակարդակի դոմեյնային անունների ռեգիստրի ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

3) դոմեյնային անունների համակարգի (DNS) ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

4) պետական մարմինների, օրենքով սահմանված կարգով խոշորացված համայնքների, Երևանի և Գյումրու համայնքների կողմից հանրությանը ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

5) էլեկտրոնային հաղորդակցության ծառայությունների կամ ինտերնետ հասանելիության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, որոնք շահագործող իրավաբանական անձինք համապատասխանում են «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքով նախատեսված միջին ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշներին:

4. 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:

5. Կենսական նշանակության ոլորտներում ծառայությունների տեսակները, ըստ տնտեսական գործունեության տեսակների դասակարգիչների, սահմանում է Կառավարությունը՝ ծառայություններ մատուցողներին նույնականացնելու համար:

6. 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:

7. Սույն հոդվածի 6-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, դրանց 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 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 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 կամ դրա մի մասը 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 փաստաթուղթը ճանաչում է Ինքնավար մարմինը՝ Հայաստանի Հանրապետությունում կիրառելի՝ միջազգային համագործակցության մասին համաձայնագրերի (պայմանագրերի) հիման վրա:

3. Կիբեռանվտանգության ապահովման ծառայություն մատուցող իրավաբանական անձինք կամ անհատ ձեռնարկատերերը պարտավոր են սույն օրենքի 20-րդ հոդվածի 2-րդ մասով սահմանված կարգով անցնել կիբեռանվտանգության աուդիտ, որի արդյունքում գնահատվում է կիբեռանվտանգության ապահովման ծառայություն մատուցողի ներքին կանոնակարգերի և դրանց կիրարկման համապատասխանությունը սույն օրենքի պահանջներին: Աուդիտի արդյունքներով կազմված հաշվետվությունն այն ստանալուց հետո տասնհինգ օրվա ընթացքում ներկայացվում է Ինքնավար մարմին և ծառայություն մատուցողին:

4. Կիրառելի միջազգային ստանդարտների ցանկը սահմանում է 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 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 նորմատիվ 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.

4) օրենքով նախատեսված այլ դեպքերում:

5. Նախքան ծառայություն մատուցողի տարածքում մշտադիտարկման իրականացումն 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:

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

7. 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 կողմից տրված ցուցումները կամ վերացնել արձանագրված թերությունները և այդ մասին տեղեկացնել Ինքնավար մարմին՝ ներկայացնելով ապացույցներ:

8. 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 մատուցողի 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 մատուցողի կարգավորող և վերահսկող այլ մարմնին՝ համապատասխան վարույթ հարուցելու և ծառայություն մատուցողի նկատմամբ 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 պահից,

2) սույն օրենքի 9-րդ հոդվածի 2-րդ մասի, 3-րդ մասի 1-ին, 4-5-րդ և 13-րդ կետերի, որոնք ուժի մեջ են մտնում համապատասխան ենթաօրենսդրական նորմատիվ իրավական ակտերի ուժի մեջ մտնելուց պահից:

2. Ծառայություն մատուցողները, որոնք 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 շահագործվող տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում ռիսկերի գնահատումը, կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագրի մշակումն իրականացնում են սույն օրենքի ուժի մեջ մտնելուց հետո՝ տասութամսյա ժամկետում:

ՏԵՂԵԿԱՆՔ
ՓՈՓՈԽՎՈՂ ՀՈԴՎԱԾՆԵՐԻ

Կ-1139-20.08.2025-ՊԻ-011/1 Առաջին ընթերցում

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 կամ անհատ ձեռնարկատեր, որը սույն օրենքի իմաստով չի համարվում ծառայություն մատուցող, ~~Հայաստանի Հանրապետության~~ Կկառավարության 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 ~~4~~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 պետական 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 շահագործվող~~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 շահագործմանն~~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 ճշգրտությունը ~~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 ճշգրտությունը ~~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, հասարակական կարգի, միջազգային հարաբերությունների և կառավարման շարունակականության (governance continuity) 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 շահագործման~~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 անձ, անհատ ձեռնարկատեր կամ աշխատանքային պայմանագրով ներգրավված ֆիզիկական անձ, ովքեր մատուցում են 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 կիբեռանվտանգության ապահովումը կազմակերպում է այն շահագործող ծառայություն մատուցողը.

2) **համապարփակ պաշտպանության սկզբունք՝** ծառայություն մատուցողը պետք է գնահատի իր կողմից շահագործվող~~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 տվյալներին ունենա ոչ ավելի

հասանելիություն, ~~որ~~քան անհրաժեշտ է իր աշխատանքային պարտականությունների կամ գործառույթների պատշաճ իրականացման համար.

5) **~~տՏ~~տվյալների գաղտնիության սկզբունք (confidentiality)**՝ տվյալները պետք է հասանելի լինեն միայն այն անձանց համար, ովքեր ունեն համապատասխան ~~մուտքի~~հասանելիության 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) **~~ա~~Ա~~մ~~բողջականության սկզբունք (integrity~~non-repudiation~~) ~~սկզբունք~~**՝ ծառայություն մատուցողները պետք է պաշտպանեն տեղեկությունը չարտոնված փոփոխումից կամ ոչնչացումից՝ ապահովելով դրա անխաթարությունը, իսկությունը, հուսալիությունը և ճշգրտությունը~~, ամբողջականությունը և անհերքելիությունը~~.

8) հասանելիության սկզբունք (availability)՝ 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

1. 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 կամն ~~դրանից բխող~~ գործողությունների ~~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 կՎ~~առավարության հաստատմանը.

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

8) կենսական նշանակության ոլորտներում նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների, ~~ցանկը~~դրանք շահագործող ծառայություն մատուցողների և ~~ըստ~~ կիբեռանվտանգության պահանջների ապահովման, վերահսկման ~~ապահովման~~ համար պատասխանատու պետական մարմինների ցանկը սահմանելու մասին ~~Հայաստանի Հանրապետության կՎ~~առավարության

որոշման նախագծի մշակում և ներկայացում ~~Հայաստանի Հանրապետության կԿ~~առավարության հաստատմանը.

9) կենսական նշանակության ոլորտներում ծառայությունների տեսակներնը ըստ տնտեսական գործունեության տեսակների դասակարգիչների սահմանելու մասին ~~Հայաստանի Հանրապետության կԿ~~առավարության որոշման նախագծի մշակում և ներկայացում ~~Հայաստանի Հանրապետության կԿ~~առավարության հաստատմանը.

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

11) կենսական նշանակության ոլորտում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշները սահմանելու մասին ~~Հայաստանի Հանրապետության կԿ~~առավարության որոշման նախագծի մշակում և ներկայացում ~~Հայաստանի Հանրապետության կԿ~~առավարության 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 պահպանմանն ուղղված մասով, մշակում և իրականացնում է իրազեկման և կրթական ծրագրեր՝ համագործակցելով Լիազոր մարմնի և կրթության ոլորտում պատասխանատու պետական մարմինների, ինչպես նաև իրավաբանական անձանց 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 43-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 շահագործողօգտագործող 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) սույն օրենքով սահմանված կարգով 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) Լիազոր մարմնին ներկայացնում է առաջարկություններ ~~Հայաստանի Հանրապետության կԿ~~առավարության որոշմամբ հաստատված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկում փոփոխություններ կամ լրացումներ կատարելու վերաբերյալ.

22) կիբեռանվտանգության վերաբերյալ հարցերով փորձագիտական աջակցությունն ~~էան~~ ցուցաբերում ~~Հայաստանի Հանրապետության կԿ~~առավարությանը.

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 (Security Operations Center (SOC)) ծառայություններ.

29) -օրենքով նախատեսված լիազորությունների իրականացման նպատակով ձևավորում է աշխատանքային խմբեր, հանձնաժողովներ, սույն օրենքի 16-րդ հոդվածի 1-ին մասով սահմանված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման նպատակով ստեղծում է միջգերատեսչական հանձնաժողով.

30) սույն օրենքի 16-րդ հոդվածի 1-ին մասով նախատեսված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշների հիման վրա նույնականացնում է կրիտիկական տեղեկատվական ենթակառուցվածքները, նախնական մշակում է նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկն՝ ըստ դրանք շահագործող ծառայություն մատուցողների և ներկայացնում Լիազոր մարմնին.

31) սույն օրենքի 16-րդ հոդվածի 5-րդ մասի համաձայն նախնական մշակում է կենսական նշանակության ոլորտներում ծառայությունների տեսակների ցանկը՝ ըստ տնտեսական գործունեության տեսակների դասակարգիչների և ներկայացնում է Լիազոր մարմնին.

32) 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 հաստատված ընթացակարգերին համապատասխան փոխանցել բացառապես 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 մասկետի 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 43-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 կ~~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:

8. Ինքնավար մարմինը տեղեկատվական տեխնոլոգիաների ակտիվների ռեեստրի ստեղծման և կառավարման համակարգի ներդրման Կառավարության

կողմից սահմանած կարգին համապատասխան դրանում նշված մարմիններին և կազմակերպություններին տրամադրում է գույքագրման գործիքակազմ, իրականացնում է տեղեկատվական տեխնոլոգիաների ռեեստրի աուդիտ, ինչպես նաև կատարում է մեթոդական վերլուծություն:

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 կԿ~~առավարությունը:

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 շահագործմանօգտագործման, 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, հիմք ընդունելով սույն օրենքի 9-րդ հոդվածի 3-րդ մասի 1-ին կետով սահմանված իր տեղեկատվական համակարգերի ռիսկերի գնահատումը, ռիսկերի գնահատման սանդղակը և կիբեռանվտանգության գործառնության (operational) մոդելը, ——պարտավոր է նշանակել կիբեռանվտանգության մասնագետ կամ մասնագետներ, բացառությամբ սույն օրենքի 19-րդ հոդվածով նախատեսված կիբեռանվտանգության ապահովումն ամբողջությամբ կիբեռանվտանգության ապահովման ծառայություն մատուցողին պատվիրակելու դեպքի:

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

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 շահագործմանօգտագործման ~~-~~վրա, կամ

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

2. Կիբեռմիջադեպըն 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 շահագործմանը~~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 ծանուցումնը 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 շահագործող~~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 (դոմեյնները)՝ 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 ստանալիս կամ 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~~կամ համապատասխանում են նույն օրենքով սահմանված տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողներին ներկայացվող հիմնական սահմանափակումներին, ~~ինչպես նաև~~ կամ ճանաչվել են սնանկ և ունեն չմարված (չներված) պարտավորություններ:

Հոդված 14. Ինքնավար մարմնի ~~–~~կողմից տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի շահագործումը ~~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 շահագործումը~~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 կ~~Կառավարությունը, որոնց մշակման համար Ինքնավար~~Լիազոր~~ մարմինը հիմք է ընդունում հետևյալ հանգամանքները՝

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

2) կիբեռմիջադեպի տևողությունը և վտանգավորության աստիճանը տնտեսական ակտիվության, շրջակա միջավայրի, հասարակական կարգի, բնակչության բնականոն կենսագործունեության ապահովման համար, միջազգային հարաբերությունների, կառավարման շարունակականության (governance continuity), 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 նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների, դրանք շահագործող ծառայություն մատուցողների և կիբեռանվտանգության պահանջների ապահովման, վերահսկման համար պատասխանատու պետական մարմինների ցանկը~~Կենսական նշանակության ոլորտներում շահագործվող կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկը հաստատում է Հայաստանի Հանրապետության կԿառավարությունը~~, ըստ կիբեռանվտանգության ապահովման համար պատասխանատու պետական մարմինների~~:

3. Օրենքի ուժով, առանց նույնականացման չափանիշների կիրառման, կրիտիկական տեղեկատվական ենթակառուցվածքներ են համարվում.

6) որակավորված վստահության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

7) բարձր մակարդակի դոմեյնային անունների ռեգիստրի ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

8) դոմեյնային անունների համակարգի (DNS) ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

9) պետական մարմինների, օրենքով սահմանված կարգով խոշորացված համայնքների, Երևանի և Գյումրու համայնքների կողմից հանրությանը

ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,

10) էլեկտրոնային հաղորդակցության ծառայությունների կամ ինտերնետ հասանելիության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, որոնք շահագործող իրավաբանական անձինք համապատասխանում են «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքով նախատեսված միջին ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշներին:

4. 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:

54. Կենսական նշանակության ոլորտներում ծառայությունների տեսակները, ըստ տնտեսական գործունեության տեսակների դասակարգիչների, սահմանում է

~~Հայաստանի Հանրապետության կ~~Կառավարությունը՝ ծառայություններ մատուցողներին նույնականացնելու համար:

~~65~~. 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:

~~76~~. Սույն հոդվածի ~~65~~-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, դրանց 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 կԿ~~առավարությունը:

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 կ~~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 կամ դրա մի մասը 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 փաստաթուղթը ճանաչում է Ինքնավար մարմինը՝~~;~~ Հայաստանի Հանրապետությունում կիրառելի՝ միջազգային համագործակցության մասին համաձայնագրերի (պայմանագրերի) հիման վրա:

3. Կիբեռանվտանգության ապահովման ծառայություն մատուցողը իրավաբանական անձինք կամ անհատ ձեռնարկատերերը պարտավոր են~~է~~ սույն օրենքի 20-րդ հոդվածի 2-րդ մասով սահմանված կարգով անցնել կիբեռանվտանգության աուդիտ~~,~~՝ որի արդյունքում գնահատվում է կիբեռանվտանգության ապահովման ծառայություն մատուցողի ներքին կանոնակարգերի և դրանց կիրարկման համապատասխանությունը սույն օրենքի պահանջներին: 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 կ~~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 կ~~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 նորմատիվ 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.

4) օրենքով նախատեսված այլ դեպքերում:

5~~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:

6~~5~~. Մշտադիտարկման արդյունքներով կազմվում է արձանագրություն, որի վերաբերյալ ծառայություն մատուցողը այն ստանալու օրվանից հետո՝ յոթնօրյա ժամկետում, իրավունք ունի Ինքնավար մարմնին ներկայացնելու առարկություններ կամ առաջարկություններ:

7~~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 կողմից տրված ցուցումները կամ վերացնել

արձանագրված թերությունները և այդ մասին տեղեկացնել Ինքնավար մարմին՝ ներկայացնելով ապացույցներ:

8~~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 մատուց~~ծ~~ողի 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 մատուց~~ծ~~ողի կարգավորող և վերահսկող այլ մարմնին՝ համապատասխան վարույթ հարուցելու և ծառայություն մատուցողի նկատմամբ 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 պահից~~հետո~~,

2) սույն օրենքի 9-րդ հոդվածի 2-րդ մասի, 3-րդ մասի 1-ին~~2-րդ~~, 4-5~~6~~-րդ և 13-րդ կետերի, որոնք ուժի մեջ են մտնում համապատասխան ենթաօրենսդրական նորմատիվ իրավական ակտերի ուժի մեջ մտնելուց պահից~~հետո~~:

2. Ծառայություն մատուցողները, որոնքովքեր 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 շահագործվողկիրառվող տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում ռիսկերի գնահատումը, կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագրի մշակումն իրականացնում են սույն օրենքի ուժի մեջ մտնելուց հետո՝ տասութամսյա ժամկետում:

ԱՄՓՈՓԱԹԵՐԹ

ՀՀ ԱԶԳԱՅԻՆ ԺՈՂՈՎՈՒՄ ԱՌԱՋԻՆ ԸՆԹԵՐՑՄԱՄԲ ԸՆԴՈՒՆՎԱԾ «ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ» (Կ-1139-20.08.2025-ՊԻ-011/1), «ՀԱՆՐԱՅԻՆ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐԻ ՄԱՍԻՆ»(Կ-1139[1]-20.08.2025-ՊԻ-011/1), «ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ԿԱՐԳԱՎՈՐՄԱՆ ՄԱՐՄՆԻ ՄԱՍԻՆ» (Կ-1139[2]-20.08.2025-ՊԻ-011/1), «ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԱԶԱՏՈՒԹՅԱՆ ՄԱՍԻՆ» ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[3]-20.08.2025-ՊԻ-011/1), «ՊԵՏԱԿԱՆ ԳԱՂՏՆԻՔԻ ՄԱՍԻՆ» ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ»(Կ-1139[4]-20.08.2025-ՊԻ-011/1), «ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՄԱՍԻՆ» ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ ԵՎ ԼՐԱՑՈՒՄՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[5]-20.08.2025-ՊԻ-011/1), «ԿԱՌԱՎԱՐՈՒԹՅԱՆ ԿԱՌՈՒՑՎԱԾՔԻ ԵՎ ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[6]-20.08.2025-ՊԻ-011/1), «ԷԼԵԿՏՐՈՆԱՅԻՆ ՓԱՍՏԱԹՂԹԻ ԵՎ ԷԼԵԿՏՐՈՆԱՅԻՆ ԹՎԱՅԻՆ ՍՏՈՐԱԳՐՈՒԹՅԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[7]-20.08.2025-ՊԻ-011/1), «ԱԶԳԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՐՄԻՆՆԵՐԻ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ ԵՎ ԼՐԱՑՈՒՄՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[8]-20.08.2025-ՊԻ-011/1), «ՆՈՐՄԱՏԻՎ ԻՐԱՎԱԿԱՆ ԱԿՏԵՐԻ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[9]-20.08.2025-ՊԻ-011/1), «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՔՐԵԱԿԱՆ ԴԱՏԱՎԱՐՈՒԹՅԱՆ ՕՐԵՆՍԳՐՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ»(Կ-1139[10]-20.08.2025-ՊԻ-011/1), «ՀԱՆՐԱՅԻՆ ԾԱՌԱՅՈՒԹՅԱՆ ՄԱՍԻՆ ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[11]-20.08.2025-ՊԻ-011/1), «ԱԶԳԱՅԻՆ ԺՈՂՈՎԻ ԿԱՆՈՆԱԿԱՐԳ ՍԱՀՄԱՆԱԴՐԱԿԱՆ ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[12]-20.08.2025-ՊԻ-011/1), «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆՈՒՄ ՍՏՈՒԳՈՒՄՆԵՐԻ

ԿԱԶՄԱԿԵՐՊՄԱՆ ԵՎ ԱՆՑԿԱՑՄԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[13]-20.08.2025-ՊԻ-011/1), «ՊԵՏԱԿԱՆ ՊԱՇՏՈՆՆԵՐ ԵՎ ՊԵՏԱԿԱՆ ԾԱՌԱՅՈՒԹՅԱՆ ՊԱՇՏՈՆՆԵՐ ՁԲԱՂԵՑՆՈՂ ԱՆՁԱՆՑ ՎԱՐՁԱՏՐՈՒԹՅԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[14]-20.08.2025-ՊԻ-011/1), «ՎԱՐՉԱԿԱՆ ԻՐԱՎԱԽԱԽՏՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՕՐԵՆՍԳՐՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԵՎ ԼՐԱՑՈՒՄՆԵՐ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ» (Կ-1139[15]-20.08.2025-ՊԻ-011/1) ՕՐԵՆՔՆԵՐԻ ՆԱԽԱԳԾԵՐԻ ՎԵՐԱԲԵՐՅԱԼ ՆԵՐԿԱՅԱՑՎԱԾ ԱՌԱՋԱՐԿՆԵՐԻ

№	Առաջարկության (փոփոխության, լրացման) հեղինակը	Հոդվածը, կետը, որին վերաբերում է առաջարկությունը	Առաջարկություն (փոփոխություն, լրացում)	Առաջարկության վերաբերյալ հեղինակի (հիմնական զեկուցողի) եզրակացությունը	Առաջարկությունն ընդունելու կամ մերժելու վերաբերյալ հանձնաժողովի որոշումը
1.	**ՀՀ Ազգային ժողովի պետական-իրավական հարցերի մշտական հանձնաժողովի անդամ, պատգամավոր Արծվիկ Մինասյան**	6-րդ հոդված 4-րդ մաս	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 6-րդ հոդվածի 4-րդ մասը առաջարկել խմբագրել այնպես, որ բացի կառավարությունից՝ Հանձնաժողովի մյուս անդամների թափուր պաշտոններում թեկնածու առաջադրելու իրավունք ունենան Ազգային ժողովի կառավարող խմբակցությունը և Ազգային ժողովի ընդդիմադիր խմբակցությունը: Ըստ այդմ՝ առաջարկել հանձնաժողովի առաջին կազմի կազմավորման շրջափուլում հանձնաժողովի նախագահը պաշտոնավարի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			5 տարի, Կառավարության կողմից առաջադրված մյուս երկու անդամները 4 և 3, իսկ իշխող և ընդդիմադիր խմբակցությունների կողմից առաջադրված անդամները 2 տարի ժամկետով: Հաշվի առնելով վերոգրյալը՝ առաջարկվում է 6-րդ հոդվածի 4-րդ մասը շարադրել հետևյալ խմբագրությամբ. «4. Հանձնաժողովի նախագահի թափուր պաշտոնում թեկնածու առաջադրելու իրավունք ունի Կառավարությունը: Հանձնաժողովի մյուս անդամների թափուր պաշտոններում թեկնածու առաջադրելու իրավունք ունեն Կառավարությունը՝ երկու անդամ, Ազգային ժողովի կառավարող խմբակցությունը և Ազգային ժողովի ընդդիմադիր խմբակցությունը՝ մեկական անդամ: Ընդ որում, եթե Ազգային ժողովի կառավարող կամ ընդդիմադիր խմբակցությունները մեկից ավելի են, ապա Ազգային ժողովի կառավարող կամ ընդդիմադիր խմբակցությունները հանձնաժողովի անդամի համապատասխան թափուր պաշտոնում առաջադրում են նախապես համաձայնեցված մեկ միասնական թեկնածու: Կառավարությունը Հանձնաժողովի անդամների թեկնածուներ առաջադրելիս պետք է առաջնորդվի առավելագույնս տարբեր մասնագիտական կարողություններով և գիտելիքներով օժտված թեկնածուներ առաջադրելու		

			սկզբունքով՝ սույն օրենքով սահմանված իրավասությունների պատշաճ իրականացումն ապահովելու նպատակով:»:		
2.	**ՀՀ Ազգային ժողովի պետական-իրավական հարցերի մշտական հանձնաժողովի անդամ, պատգամավոր Արծվիկ Մինասյան**	61-րդ հոդված, 3-րդ և 5-րդ մասեր	Հաշվի առնելով, որ առաջարկվում է Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 6-րդ հոդվածի 4-րդ մասը խմբագրել այնպես, որ բացի կառավարությունից՝ Հանձնաժողովի մյուս անդամների թափուր պաշտոններում թեկնածու առաջադրելու իրավունք ունենան Ազգային ժողովի կառավարող խմբակցությունը և Ազգային ժողովի ընդդիմադիր խմբակցությունը, հետևաբար առաջարկվում է նաև 61-րդ հոդվածի՝ -3-րդ մասը շարադրել հետևյալ խմբագրությամբ. «3. Հանձնաժողովի առաջին կազմի անդամների պաշտոնավարման ժամկետներն են՝ 1) երկու անդամի համար՝ երկու տարի. 2) մեկ անդամի համար՝ երեք տարի. 3) մեկ անդամի համար՝ չորս տարի. 4) Հանձնաժողովի նախագահի համար՝ հինգ տարի:» -5-րդ մասը շարադրել հետևյալ խմբագրությամբ. «5.Սույն հոդվածի 3-րդ մասի 1-րդ կետով սահմանված ժամկետով Հանձնաժողովի առաջին կազմի երկու անդամներին	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			առաջարկում են համապատասխանաբար Ազգային ժողովի կառավարող խմբակցությունը և Ազգային ժողովի ընդդիմադիր խմբակցությունը, իսկ 2-3-րդ կետերով սահմանված ժամկետները Հանձնաժողովի առաջին կազմի երկու անդամներից ամեն մեկի համար առաջարկում է Կառավարությունը՝ առաջադրման հետ միաժամանակ: »:		
3.	**ՀՀ կառավարություն**	Նախագծերի փաթեթում ներառված առանձին օրենքների նախագծերի հոդվածներ (ըստ ձևակերպման առկայության)	Նախագծերի փաթեթում ներառված բոլոր օրենքների նախագծերի ամբողջ տեքստում (ըստ ձևակերպման առկայության) առաջարկում ենք «Հայաստանի Հանրապետության կառավարություն», «կառավարություն» ձևակերպումները՝ իրենց հոլովաձևերով փոխարինել «Կառավարություն» բառով՝ համապատասխան հոլովաձևերով՝ հիմք ընդունելով Սահմանադրությամբ սահմանված հասկացությունը, ինչպես նաև «Նորմատիվ իրավական ակտերի մասին» օրենքի (այսուհետ՝ Օրենք) 15-րդ հոդվածի 1-ին մասում սահմանված դրույթը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
4.	**ՀՀ կառավարություն**	**Նախագծերի փաթեթում ներառված առանձին օրենքների նախագծերի հոդվածներ (ըստ ձևակերպման առկայության)**	Նախագծերի փաթեթի ամբողջ տեքստում առաջարկում ենք «ՀՈԴԱՎԱԾ» բառերը փոխարինել «Հոդված» բառով՝ հիմք ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 14-րդ հոդվածի 2-րդ մասում սահմանված դրույթը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

5.	**ՀՀ կառավարություն**	Նախագծերի փաթեթում ներառված առանձին օրենքների նախագծերի հոդվածներ (ըստ ձևակերպման առկայության)	Նախագծերի փաթեթում առաջարկում ենք, հիմք ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 2-րդ հոդվածի 1-ին մասի 3-րդ կետի սահմանումը, Սահմանադրության և օրենքների հիման վրա և դրանց իրականացումն ապահովելու նպատակով օրենքով լիազորված լինելու դեպքում Սահմանադրությամբ նախատեսված մարմինների կողմից ընդունվող նորմատիվ իրավական ակտը հիշատակելիս օգտագործել «ենթաօրենսդրական նորմատիվ իրավական ակտ» հասկացությունը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
6.	**ՀՀ կառավարություն**	1-ին հոդվածի 2-6-րդ մասեր	«Կիբեռանվտանգության մասին» օրենքի նախագծի 1-ին հոդվածի՝ 2-րդ մասում առաջարկում ենք «իրավաբանական անձ» բառերից հետո լրացնել «կամ անհատ ձեռնարկատեր» բառերը՝ հնարավորություն տալով, որպեսզի նշված սուբյեկտները ևս կարողանան կամավոր ստանձնել սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամ հրաժարվել դրանցից: -3-րդ մասի 1-ին կետում «3» թիվը փոխարինել «4» թվով, իսկ 2-րդ կետից հանել «կառավարման» բառը, քանի որ օրենքը տարածվելու է նաև ՀՀ Սահմանադրությամբ սահմանված այլ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			պետական մարմինների վրա (մասնավորապես՝ անկախ և ինքնավար մարմինների). տերմինների միատեսակ կիրառություն ապահովելու նպատակով: - 4-րդ մասում առաջարկում ենք «աջակցության» բառից առաջ լրացնել «պետական» բառը՝ հիմք ընդունելով «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքի անվանումը. 5-րդ մասում «օգտագործվող» բառը փոխարինել «շահագործվող» բառով՝ իմաստային տարընկալումներից խուսափելու համար: 6-րդ մասում «օգտագործմանն» բառը փոխարինել «շահագործմանն» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով:		
7.	**ՀՀ կառավարություն**	3-րդ հոդված	«Կիբեռանվտանգության մասին» օրենքի նախագծի 3-րդ հոդվածի 1-ին մասի՝ -1-ին և 4-րդ կետերում «անհերքելիությունը (non repudiation)» բառերը փոխարինել «ճշգրտությունը» բառով՝ հիմք ընդունելով միջազգայնորեն ճանաչված CIA Triad-ի accuracy (ճշգրտություն) տերմինը և «Հանրային տեղեկությունների մասին» օրենքի նախագծի համահունչ ձևակերպումը. -5-րդ կետում «շրջակա միջավայրի» բառերից հետո լրացնել «, հասարակական կարգի, միջազգային հարաբերությունների և կառավարման շարունակականության	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			(governance continuity)» բառերը՝ հիմք ընդունելով կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման նշված չափանիշների կիրառումը՝ ըստ լավագույն միջազգային փորձի և TAG International-ի կողմից ՀՀ-ի համար կազմված մեթոդոլոգիայի. -7-րդ կետից հանել «կառավարման» բառը, քանի որ օրենքը տարածվելու է նաև ՀՀ Սահմանադրությամբ սահմանված այլ պետական մարմինների վրա (մասնավորապես՝ անկախ և ինքնավար մարմինների). -14րդ կետում «օգտագործման» բառը փոխարինել «շահագործման» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով: - 18-րդ կետում « իրավաբանական կամ ֆիզիկական անձ» բառերը փոխարինել «իրավաբանական անձ, անհատ ձեռնարկատեր կամ աշխատանքային պայմանագրով ներգրավված ֆիզիկական անձ» բառերով, «ով» բառը փոխարինել «ովքեր» բառով, «է» բառը «են» բառով՝ հաշվի առնելով այն, որ ֆիզիկական անձինք ինքնուրույն աուդիտ չեն կարող անցնել:		
8.	**ՀՀ կառավարություն**	4-րդ հոդվածի 1-ին մաս	«Կիբեռանվտանգության մասին» օրենքի նախագծի 4-րդ հոդվածի 1-ին մասի՝ - 1-ին կետում «անվտանգության» բառը փոխարինել «կիբեռանվտանգության» բառով, իսկ «կազմակերպում է» բառերից	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հետո լրացնել «այն շահագործող» բառերը: -2-րդ կետում նշված «օգտագործմանն» բառը փոխարինել «շահագործմանն» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով: - 4-րդ կետում «որքան» բառը փոխարինել «քան» բառով, -5-րդ կետում «սկզբունք» բառից հետո լրացնել «(confidentiality)» բառը, իսկ «մուտքի» բառը փոխարինել «հասանելիության» բառով, քանի որ մուտքն ինքնին չի ենթադրում հասանելիության ապահովում: -7-րդ կետում «(non repudiation)» բառերը փոխարինել «(integrity)» բառով և այն գրել «սկզբունք» բառից հետո, իսկ «հուսալիություն, ամբողջականությունը և անհերքելիությունը» բառերը փոխարինել «հուսալիությունը և ճշգրտությունը» բառերով՝ հիմք ընդունելով միջազգայնորեն ճանաչված CIA Triad-ի accuracy (ճշգրտություն) տերմինը և «Հանրային տեղեկությունների մասին» օրենքի նախագծի համահունչ ձևակերպումը.: - 8-րդ կետում «սկզբունք» բառից հետո լրացնել «(availability)» բառը՝ ձևակերպման միջազգայնորեն հայտի տարբերակը նշելու համար:		
9.	**ՀՀ կառավարություն**	5-րդ հոդված 1-ին մաս	«Կիբեռանվտանգության մասին» օրենքի նախագծի 5-րդ հոդվածի առաջին մասն առաջարկում ենք համարակալել հիմք	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 14-րդ հոդվածի 3-րդ մասը:		
10.	**ՀՀ կառավարություն**	6-րդ հոդված 1-ին մաս	«Կիբեռանվտանգության մասին» օրենքի նախագծի 6-րդ հոդվածի 1-ին մասի՝ -1-ին կետում «և դրանից բխող միջոցառումների ծրագրի մշակում» բառերը փոխարինել «կամ գործողությունների ծրագրի մշակում» բառերով՝ հաշվի առնելով, որ ներկայումս վերանայվում է ռազմավարական պլանավորման գործընթացները: Դա հնարավորություն կտա խուսափել հետագայում անվանումների ճիշտ կիրառման խնդիրներից: -7-րդ կետում «համակարգերի» բառը փոխարինել «համակարգերում» բառով: -8-րդ կետը շարադրել հետևյալ խմբագրությամբ՝ «8) կենսական նշանակության ոլորտներում նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների, դրանք շահագործող ծառայություն մատուցողների և կիբեռանվտանգության պահանջների ապահովման, վերահսկման համար պատասխանատու պետական մարմինների ցանկը սահմանելու մասին Կառավարության որոշման նախագծի մշակում և ներկայացում Կառավարության հաստատմանը.»: Նոր խմբագրությամբ տարբերակը հնարավորություն կտա առավել որոշակի ձևակերպել ընդունվելիք ենթա	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			օրենսդրական նորմատիվ իրավական ակտի անվանումը: - 10-րդ կետում առաջարկում ենք «իրավաբանական անձի» բառերից հետո լրացնել «կամ անհատ ձեռնարկատիրոջ» բառերը՝ հնարավորություն տալով, որպեսզի նշված սուբյեկտները ևս կարողանան կամավոր ստանձնել սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամ հրաժարվել դրանցից:		
11.	**ՀՀ կառավարություն**	7-րդ հոդվածի 2-րդ մաս	«Կիբեռանվտանգության մասին» օրենքի նախագծի 7-րդ հոդվածի 2-րդ մասի՝ - 8-րդ կետում առաջարկում ենք «պահպանման մասով» բառերը փոխարինել «պահպանմանն ուղղված» բառերով, «մարմինների» բառից հետո լրացնել «ինչպես նաև իրավաբանական անձանց» բառերը, իսկ «ինչպես նաև» բառերը հանել, ապահովելով նաև մասնավոր հատվածի հետ համագործակցությունը. -9-րդ «3» թիվը փոխարինել «4» թվով՝ ներքին հղումը ճիշտ կատարելու նպատակով. -13-րդ կետում նշված «օգտագործման» բառը փոխարինել «շահագործման» բառով տերմինների միատեսակ կիրառություն ապահովելու նպատակով: -16-րդ կետում «օրենքով սահմանված կարգով» բառերը տեղափոխել նախադասության սկիզբ՝ ձևակերպելով	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հետևյալ կերպ՝ «սույն օրենքով սահմանված կարգով»՝ տարընկալումներից խուսափելու նպատակով: - 21-րդ կետում «ներկայացնում է» բառից առաջ լրացնել «Լիազոր մարմնին» բառերը: -28-րդ կետում «կիբեռանվտանգության գործառնությունների կենտրոնի (SOC)» բառերն առաջարկում ենք փոխարինել «կիբեռանվտանգության գործառնությունների կենտրոնի (Security Operations Center (SOC))» բառերով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով: -22-րդ կետում «աջակցության» բառը փոխարինել «աջակցություն է» բառերով: -29-րդ կետը շարադրել հետևյալ խմբագրությամբ. «29) օրենքով նախատեսված լիազորությունների իրականացման նպատակով ձևավորում է աշխատանքային խմբեր, հանձնաժողովներ, սույն օրենքի 16-րդ հոդվածի 1-ին մասով սահմանված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման նպատակով ստեղծում է միջգերատեսչական հանձնաժողով:»: Դա անհրաժեշտ է՝ հիմք ընդունելով չափանիշները կիրառելու համար հանձնաժողով ստեղծելու անհրաժեշտությունը: Նախագծով նախատեսված սուբյեկտներին		

			նույնականացնելու Ինքնավար մարմնի գործառույթը (իրավասությունը) օրենքում ամրագրելու նպատակով առաջարկվում է -29-րդ կետից հետո լրացնել նոր 30-32-րդ կետեր՝ հետևյալ բովանդակությամբ. «30) սույն օրենքի 16-րդ հոդվածի 1-ին մասով նախատեսված կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման չափանիշների հիման վրա նույնականացնում է կրիտիկական տեղեկատվական ենթակառուցվածքները, նախնական մշակում է նույնականացված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկն՝ ըստ դրանք շահագործող ծառայություն մատուցողների և ներկայացնում Լիազոր մարմնին. 31) սույն օրենքի 16-րդ հոդվածի 5-րդ մասի համաձայն նախնական մշակում է կենսական նշանակության ոլորտներում ծառայությունների տեսակների ցանկը՝ ըստ տնտեսական գործունեության տեսակների դասակարգիչների և ներկայացնում է Լիազոր մարմնին. 32) իրականացնում է օրենքով նախատեսված այլ լիազորություններ:»:		
12.	**ՀՀ կառավարություն**	**7-րդ հոդված 3-րդ և 8-րդ մասեր**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 7-րդ հոդվածի՝ - 3-րդ մասում առաջարկում ենք «սույն կետի» բառերը փոխարինել «սույն մասի» բառերով, «միջազգային կազմակերպություններին» բառերից հետո	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			լրացնել «հաստատված ընթացակարգերին համապատասխան» բառերը, «փոխանցել» բառից հետո լրացնել «բացառապես» բառը: 5-րդ մասում «3»թիվը փոխարինել «4» թվով, -հիմք ընդունելով SS ակտիվների կառավարման միասնական մոտեցման ձևավորման, շահագործման կառուցվածքի հստակեցման հայեցակարգը՝ առաջարկվում է լրացնել նոր 8-րդ մաս՝ հետևյալ բովանդակությամբ. «8. Ինքնավար մարմինը տեղեկատվական տեխնոլոգիաների ակտիվների ռեեստրի ստեղծման և կառավարման համակարգի ներդրման Կառավարության կողմից սահմանած կարգին համապատասխան դրանում նշված մարմիններին և կազմակերպություններին տրամադրում է գույքագրման գործիքակազմ, իրականացնում է տեղեկատվական տեխնոլոգիաների ռեեստրի աուդիտ, ինչպես նաև կատարում է մեթոդական վերլուծություն:»:		
13.	**ՀՀ կառավարություն**	**9-րդ հոդված 3-րդ մաս 6-րդ կետ**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 9-րդ հոդվածի 3-ին մասի 6-րդ կետում նշված «օգտագործման» բառը փոխարինել «շահագործման» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
14.	**ՀՀ կառավարություն**	**10-րդ հոդվածի 1-ին, 2-րդ և 3-րդ մասեր**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 10-րդ հոդվածի՝ 1-ին մասն առաջարկում ենք շարադրել	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հետևյալ խմբագրությամբ. -«1. Ծառայություն մատուցողը, հիմք ընդունելով սույն օրենքի 9-րդ հոդվածի 3-րդ մասի 1-ին կետով սահմանված իր տեղեկատվական համակարգերի ռիսկերի գնահատումը, ռիսկերի գնահատման սանդղակը և կիբեռանվտանգության գործառնության (operational) մոդելը, պարտավոր է նշանակել կիբեռանվտանգության մասնագետ կամ մասնագետներ, բացառությամբ սույն օրենքի 19-րդ հոդվածով նախատեսված կիբեռանվտանգության ապահովումը ամբողջությամբ կիբեռանվտանգության ապահովման ծառայություն մատուցողին պատվիրակելու դեպքի:»՝ հիմք ընդունելով այն հանգամանքը, որ մասնագետների հավաքագրումը պետք է կատարվի ծառայություն մատուցողի ռիսկայնության մակարդակին համապատասխան: -2-րդ մասում առաջարկում ենք «կարգը» բառից հետո լրացնել «և որակավորման ճանաչման կարգը» բառերը, իսկ «կարող է սահմանել» բառերը փոխարինել «սահմանում է» բառերով:		
15.	**ՀՀ կառավարություն**	**11-րդ հոդված 1-ին մաս**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 11-րդ հոդվածի 1-ին մասի՝ 1-ին, 2-րդ և 7-րդ կետերում նշված «օգտագործման» բառը փոխարինել «շահագործման» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			նպատակով: - 2-րդ կետի վերջում «,» կետադրական նշանն առաջարկում ենք փոխարինել «:» կետադրական նշանով:		
16.	**ՀՀ կառավարություն**	**13-րդ հոդվածի 4-րդ, 8-րդ և 10-րդ մաս**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 13-րդ հոդվածի՝ -4-րդ մասում նշված «տիրապետող» բառը փոխարինել «շահագործող» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով: - 8-րդ մասում «տեղեկություն» բառից հետո լրացնել «ստանալիս կամ» բառերը: - 10-րդ մասում առաջարկում ենք «պահանջներին և» բառերը փոխարինել «պահանջներին կամ համապատասխանում են նույն օրենքով սահմանված տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողներին ներկայացվող հիմնական» բառերը՝ հաշվի առնելով, որ սահմանափակումներն այն հատկանիշներն են, որոնք պետք է բացակայեն: Նույն մասում առաջարկում ենք «ինչպես նաև» շաղկապը փոխարինել «կամ» շաղկապով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
17.	**ՀՀ կառավարություն**	**14-րդ հոդված**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 14-րդ հոդվածի՝ վերնագրում և առաջին մասում նշված «օգտագործմանը» բառերը փոխարինել «շահագործումը» բառերով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

18.	**ՀՀ կառավարություն**	**16-րդ հոդվածի 1-ից 7-րդ մասեր**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 16-րդ հոդվածի՝ -վերնագրում «շահագործվող» բառը փոխարինել «շահագործվող» բառով: -1-ին մասում «Լիազոր» բառը փոխարինել «Ինքնավար» բառով: -1-ին մասի 1-ին կետում «նշանակության» բառից հետո լրացնել «ոլորտներում» բառը: -1-ին մասի 2-րդ կետն առաջարկում ենք շարադրել հետևյալ խմբագրությամբ. «2) կիբեռմիջադեպի տևողությունը և վտանգավորության աստիճանը տնտեսական ակտիվության, շրջակա միջավայրի, հասարակական կարգի, բնակչության բնականոն կենսագործունեության ապահովման համար, միջազգային հարաբերությունների, կառավարման շարունակականության (governance continuity), ազգային անվտանգության կամ բնակչության առողջության վրա.»՝ հիմք ընդունելով կրիտիկական տեղեկատվական ենթակառուցվածքների նույնականացման նշված չափանիշների կիրառումը՝ ըստ լավագույն միջազգային փորձի և TAG International-ի կողմից ՀՀ-ի համար կազմված մեթոդոլոգիայի. - 2-րդ մասն առաջարկում ենք շարադրել հետևյալ խմբագրությամբ. «2. Կենսական նշանակության ոլորտներում նույնականացված կրիտիկական	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			տեղեկատվական ենթակառուցվածքների, դրանք շահագործող ծառայություն մատուցողների և կիբեռանվտանգության պահանջների ապահովման, վերահսկման համար պատասխանատու պետական մարմինների ցանկը հաստատում է Կառավարությունը:»: Առաջարկվող խմբագրությունը նպատակ է հետապնդում առավել հստակեցնելու կարգավորումը: Հիմք ընդունելով միջազգայնորեն և NIS2 դիրեկտիվով առանձնահատուկ սահմանված սուբյեկտների ցանկը՝ 3-րդ մասն առաջարկում ենք շարադրել հետևյալ խմբագրությամբ. «3. Օրենքի ուժով, առանց նույնականացման չափանիշների կիրառման, կրիտիկական տեղեկատվական ենթակառուցվածքներ են համարվում. 1) որակավորված վստահության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, 2) բարձր մակարդակի դոմեյնային անունների ռեգիստրի ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, 3) դոմեյնային անունների համակարգի (DNS) ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը,		

			4) պետական մարմինների, օրենքով սահմանված կարգով խոշորացված համայնքների, Երևանի և Գյումրու համայնքների կողմից հանրությանը ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, 5) էլեկտրոնային հաղորդակցության ծառայությունների կամ ինտերնետ հասանելիության ծառայությունների մատուցման համար շահագործվող տեղեկատվական համակարգերը, որոնք շահագործող իրավաբանական անձինք համապատասխանում են «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքով նախատեսված միջին ձեռնարկատիրության սուբյեկտների դասակարգման չափանիշներին:»: 3-րդ մասով նախատեսված կարգավորումն էլ առաջարկում ենք նախատեսել 4-րդ մասով, իսկ մյուս մասերի համարակալումն առաջարկում ենք փոփոխել՝ ապահովելով հաջորդական համարակալում: լրամշակված 7-րդ մասում «5» թիվը փոխարինել «6» թվով:		
19.	**ՀՀ կառավարություն**	**17-րդ հոդված 1-ին մաս**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 17-րդ հոդվածի՝ - 1-րդ մասի 1-ին պարբերությունում «դրա» բառն առաջարկում ենք փոխարինել «դրանց» բառով.	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

20.	**ՀՀ կառավարություն**	**19-րդ հոդվածի 1-ին և 3-րդ մասեր**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 19-րդ հոդվածի 1-մասում «ապահովումը» բառից հետո լրացնել «կամ դրա մի մասը» բառերը: Հիմք ընդունելով այն, որ ֆիզիկական անձինք չեն կարող աուդիտ անցնել՝ նույն հոդվածի 3-րդ մասում «ծառայություն մատուցողը պարտավոր է» բառերը փոխարինել «ծառայություն մատուցող իրավաբանական անձինք կամ անհատ ձեռնարկատերերը պարտավոր են» բառերով, իսկ «աուդիտ:» բառից հետո լրացնել «, որի արդյունքում գնահատվում է կիբեռանվտանգության ապահովման ծառայություն մատուցողի ներքին կանոնակարգերի և դրանց կիրարկման համապատասխանությունը սույն օրենքի պահանջներին:», որպեսզի հստակեցվի որ վերջիններիս աուդիտի արդյունքում ստուգվում է իրենց ներքին կանոնակարգերի համապատասխանությունը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
21.	**ՀՀ կառավարություն**	**22-րդ հոդված 4-րդ և 7-րդ մաս**	Կիբեռանվտանգության մասին» օրենքի նախագծի 22-րդ հոդվածի 7-րդ մասի երկրորդ նախադասությունում «Ինքնավար մարմնի» բառից հետո լրացնել «կողմից» բառը: -4-րդ մասից սկսած վերնայել 22-րդ հոդվածի մասերի համարակալումը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

22.	**ՀՀ կառավարություն**	**23-րդ հոդված 1-ին մաս**	Կիբեռանվտանգության մասին» օրենքի նախագծի 23-րդ հոդվածի 1-ին մասի 2-րդ կետում «պատասխանատվության» բառից առաջ լրացնել «ծառայություն մատուցողի նկատմամբ» բառերը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
23.	**ՀՀ կառավարություն**	**25-րդ հոդվածի 1-ին, 2-րդ և 5-րդ մասեր**	«Կիբեռանվտանգության մասին» օրենքի նախագծի 25-րդ հոդվածի՝ 1-ին մասի 1-ին կետում առաջարկում ենք «հետո» բառը փոխարինել «պահից» բառով: - 1-ին մասի 2-րդ կետում առաջարկում եմ «3-րդ մասի 2-րդ, 4-6-րդ» ձևակերպումը փոխարինել « 3-րդ մասի 1-ին, 4-5-րդ» ձևակերպմամբ, իսկ «հետո» բառն առաջարկում ենք փոխարինել «պահից» բառով: -2-րդ մասի «ովքեր» բառը փոխարինել «որոնք» բառով: -5-րդ մասում «կիրառվող» բառը փոխարինել «շահագործվող» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
24.	**ՀՀ կառավարություն**	Նախագծի առանձին հոդվածներ (ըստ ձևակերպման առկայության)	«Հանրային տեղեկությունների մասին» օրենքի նախագծում առաջարկում ենք վերանայել ամբողջ տեքստում կիրառված և/կամ ձևակերպումները՝ համապատասխանեցնելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 16-րդ հոդվածի բովանդակությանը և հաշվի առնելով, որ «և/կամ» գրելաձեւը կիրառելի չէ:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

25.	**ՀՀ կառավարություն**	3-րդ հոդվածի 1-ին մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 3-րդ հոդվածի 1-ին մասի 2-րդ կետում առաջարկում ենք «(այսուհետ՝ Ինքնավար մարմին)» բառերը հանել, քանզի օրենքի հետագա տեքստում կիրառվելու է սահմանված հասկացությունը, այն է՝ «Ինքնավար մարմին»:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
26.	**ՀՀ կառավարություն**	3-րդ հոդվածի 1-ին մասի և առանձին հոդվածներ (ըստ ձևակերպման առկայության)	«Հանրային տեղեկությունների մասին» օրենքի նախագծի մի շարք հոդվածներում կիրառվում է «հանրային տեղեկություն» հասկացությունը՝ համապատասխան հոլովաձևերով: Մինչդեռ «Հանրային տեղեկությունների մասին» օրենքի նախագծի 3-րդ հոդվածի 1-ին մասի 1-ին կետում «հանրային տեղեկություն» հասկացության համար սահմանվել է կրճատ տարբերակ, այն է՝ «(այսուհետ՝ տեղեկություն)»: Հիմք ընդունելով վերոգրյալն՝ առաջարկում ենք «Հանրային տեղեկությունների մասին» օրենքի նախագծում կիրառել մեկ միատեսակ ձևակերպում:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
27.	**ՀՀ կառավարություն**	6-րդ հոդված 3-րդ և 5-րդ մասեր	Հանրային տեղեկությունների մասին» օրենքի նախագծի 6-րդ հոդվածի՝ -3-րդ մասում «Նշված գումարի» բառերը առաջարկում ենք փոխարինել «Այդ ծախսերի» բառերով՝ դրույթի բովանդակությունն առավել հստակ սահմանելու համար: - 5-րդ մասում «պահանջում է » բառից հետո լրացնել «ստանալ» բառը՝ դրույթի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			բովանդակությունն առավել հստակ սահմանելու համար:		
28.	**ՀՀ կառավարություն**	8-րդ հոդվածի 1-ին մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 8-րդ հոդվածի 1-ին մասում առաջարկում ենք՝ - «անկախ և ինքնավար պետական մարմինները» բառերը փոխարինել «անկախ պետական և ինքնավար մարմինները» բառերով՝ հիմք ընդունելով Սահմանադրությամբ սահմանված հասկացությունները, ինչպես նաև «Նորմատիվ իրավական ակտերի մասին» օրենքի 15-րդ հոդվածի 1-ին մասում սահմանված դրույթը, - «համայնքները» բառից հետո լրացնել «, Երևան և Գյումրի համայնքները» բառերով, քանի որ Երևան և Գյումրի համայնքները չեն հանդիսանում օրենքով սահմանված կարգով խոշորացված համայնքներ և դուրս էին մնացել նշված դրույթի կարգավորման շրջանակից:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
29.	**ՀՀ կառավարություն**	9-րդ հոդված 1-ին մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 9-րդ հոդվածի 1-ին մասում առաջարկում ենք՝ - «հարթակում» բառից հետո լրացնել « ընդգրկված» բառը՝ դրույթի բովանդակությունն ամբողջացնելու համար, - «չափորոշիչները,» բառը և կետադրական	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			նշանը հանել, -«պահանջները, շտեմարանները տեղեկությունների մուտքի հարթակին միացնելու կարգը» բառերը փոխարինել «պահանջները» բառով, քանի որ տեղեկությունների մուտքի միասնական հարթակն, ըստ էության, ապահովում է օգտատերերին թվային ծառայությունների մատուցման միասնական հարթակ, և առանձին շտեմարաններն այդ հարթակին միացնելու անհրաժեշտությունը բացակայում է:		
30.	**ՀՀ կառավարություն**	11-րդ հոդվածի 4-րդ մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 11-րդ հոդվածի 4-րդ մասում առաջարկում ենք «առաջին» բառը փոխարինել «1-ին» թվով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
31.	**ՀՀ կառավարություն**	12-րդ հոդվածի 4-րդ մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 12-րդ հոդվածի 4-րդ մասում առաջարկում ենք «կան» բառը փոխարինել «կամ այդ» բառով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
32.	**ՀՀ կառավարություն**	16-րդ հոդվածի 1-ին մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 16-րդ հոդվածի 1-ին մասում առաջարկում ենք «15-րդ» թվից առաջ լրացնել «սույն օրենքի» բառերը՝ կիրառված հղման հստակությունն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
33.	**ՀՀ կառավարություն**	16-րդ հոդվածի 1-ին մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 19-րդ հոդվածի 1-ին մասում առաջարկում ենք «Նշված» բառը փոխարինել «Տվյալների շտեմարանի կառավարչի հետ կնքվող» բառերով՝ դրույթի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հստակությունն ապահովելու նպատակով:		
34.	**ՀՀ կառավարություն**	20-րդ հոդվածի 4-րդ և 7-րդ մասեր	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 20-րդ հոդվածի՝ - 4-րդ մասում առաջարկում ենք «սույն օրենքի 14-րդ հոդվածի 4-րդ մասում նշված տվյալների շտեմարանների» բառերը փոխարինել «ոչ պետական տեղեկատվական համակարգի՝ սույն օրենքի 14-րդ հոդվածի 5-րդ մասում նշված տվյալների շտեմարանների» բառերով՝ հղման հստակությունն ապահովելու նպատակով: - 7-րդ մասում առաջարկում ենք «Նշված» բառը փոխարինել «Տվյալների փոխանակման շերտին միանալու» բառերով՝ դրույթի հստակությունն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
35.	**ՀՀ կառավարություն**	24-րդ հոդվածի 3-րդ մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 24-րդ հոդվածի 3-րդ մասում առաջարկում ենք «կայքում» բառը փոխարինել «կայքէջում» բառով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
36.	**ՀՀ կառավարություն**	26-րդ հոդվածի 2-րդ մաս	«Հանրային տեղեկությունների մասին» օրենքի նախագծի 26-րդ հոդվածի 2-րդ մասում առաջարկում ենք « վեբ-կայքերը» բառերը փոխարինել «կայքէջերը» բառով՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

37.	**ՀՀ կառավարություն**	Նախագծի ամբողջ տեքստում	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծում առաջարկում ենք համասեռ հոդվածները միավորել համապատասխան գլուխներում՝ հաշվի առնելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 14-րդ հոդվածի 4-րդ մասի կարգավորումները:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
38.	**ՀՀ կառավարություն**	1-ին հոդված, 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 1-ին հոդվածի 1-ին մասում առաջարկում ենք «իրավասությունների» բառից հետո լրացնել «, վերահսկողության» բառը՝ նկատի ունենալով, որ հիշյալ օրենքի նախագծի կարգավորման առարկան ներառում է նաև վերահսկողության հետ կապված հարաբերությունները:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
39.	**ՀՀ կառավարություն**	3-րդ հոդվածի 2-րդ մաս	Առաջարկում ենք «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 3-րդ հոդվածի՝ - 2-րդ մասում «գործառույթները» բառից հետո լրացնել՝ ««Կիբեռանվտանգության մասին» օրենքով նախատեսված» բառերը՝ նկատի ունենալով, որ «կարգավորող և վերահսկող այլ մարմիններ» հասկացության սահմանումը տրված է նշված օրենքով: - 2-րդ մասի 1-ին, 2-րդ կետերում, 3-րդ կետում, նույն կետի «ա» և «բ» ենթակետերում «կարգավորող և վերահսկող մարմիններ» ձևակերպումը համապատասխան հոլովաձևերով փոխարինել «կարգավորող և վերահսկող այլ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			մարմիններ» ձևակերպմամբ՝ համապատասխան հոլովաձևերով՝ ձևակերպումների միատեսակ կիրառություն ապահովելու նպատակով: - 2-րդ մասում «համագործակցությունը հիմնվում է հետևյալ սկզբունքների վրա» բառերը փոխարինել «համագործակցության ձևերն են» բառերով՝ հաշվի առնելով, որ նույն մասի կետերով նախատեսվող կարգավորումները իրենց բնույթով «սկզբունք» չեն հանդիսանում: - 2-րդ մասի 1-ին կետում «մարմն» բառն առաջարկում ենք փոխարինել «մարմնին» բառով՝ բաց թողնված տառը լրացնելու նպատակով:		
40.	**ՀՀ կառավարություն**	**5-րդ հոդվածի 1-ին և 3-րդ մաս**	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 5-րդ հոդվածի 3-րդ մասի 2-րդ կետից հանել «ունեն» բառը, քանի որ 3-րդ մասում արդեն իսկ առկա է «որն ունի» ձևակերպումը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
41.	**ՀՀ կառավարություն**	**6-րդ հոդված 3, 5-րդ մասեր**	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 6-րդ հոդվածի՝ 3-րդ մասի 1-ին կետում «հոդվածով» բառն առաջարկում ենք փոխարինել «հոդվածի 3-րդ մասով» բառերով՝ նկատի ունենալով, որ համապատասխան պահանջները սահմանված են սույն օրենքի նախագծի 5-րդ հոդվածի 3-րդ մասով: 3-րդ մասում լրացնել նոր՝ 7-րդ ենթակետ՝	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հետևյալ բովանդակությամբ. «7) վերջին հինգ տարիների ընթացքում ունեցել է Հանձնաժողովի գործունեության ոլորտներում գործունեություն իրականացնող առևտրային կազմակերպությունների կանոնադրական կապիտալում մասնակցություն (բաժնեմաս, բաժնետոմս, փայ):»: Նման պահանջի սահմանումը հնարավորություն կտա ի սկզբանե խուսափել շահերի բախման հնարավոր դեպքերից: 5-րդ մասը շարադրել հետևյալ խմբագրությամբ. «5. Հանձնաժողովի նախագահի կամ անդամի պաշտոնում թեկնածուն առաջադրվում է սույն օրենքի 12-րդ հոդվածի 6-րդ մասով սահմանված կարգով տեղեկացվելուց, ինչպես նաև Հանձնաժողովի նախագահ կամ անդամ նշանակելու մասին Ազգային ժողովի որոշումը չընդունվելուց հետո՝ մեկամսյա ժամկետում: Եթե Կառավարությանը կամ Ազգային ժողովի կառավարող խմբակցությանը վերապահված հանձնաժողովի անդամի թափուր պաշտոնում սահմանված ժամկետում թեկնածու չի առաջադրվում, ապա նույն մարմինն այդ պաշտոնում թեկնածու առաջադրում է մեկամսյա ժամկետում: Եթե Ազգային ժողովի ընդդիմադիր խմբակցությանը վերապահված՝		

			Հանձնաժողովի անդամի պաշտոնում սահմանված ժամկետում թեկնածու չի առաջադրվում, ապա Ազգային ժողովի կառավարող խմբակցությունն այդ պաշտոնում թեկնածու առաջադրում է մեկամսյա ժամկետում:»՝ հաշվի առնելով, որ փոփոխվել են Հանձնաժողովի անդամի թեկնածու առաջադրելու մարմինների կազմը: 6-րդ մասում լրացնել նոր՝ երկրորդ նախադասություն՝ հետևյալ բովանդակությամբ. «Եթե Հանձնաժողովի անդամ նշանակելու մասին Ազգային ժողովի որոշումը չի ընդունվում, ապա նույն մարմնի կողմից այդ պաշտոնում թեկնածու առաջադրելու իրավունքը պահպանվում է:»՝ նպատակ ունենալով, որպեսզի ԱԺ-ի կողմից որոշում չընդունելու դեպքում պահպանվի Հանձնաժողովի անդամի թեկնածու առաջադրելու տվյալ մարմնի իրավունքը:»:		
42.	**ՀՀ կառավարություն**	**7-րդ հոդված 2-րդ մաս**	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 7-րդ հոդվածի՝ -2-րդ մասում առաջարկում ենք «Հանձնաժողովի» բառից առաջ լրացնել «Եթե» բառը, «նշանակումը» բառից հետո լրացնել «կատարվում է» բառերը, իսկ «կատարվելու դեպքում» բառերը փոխարինել «, ապա» բառով՝ իմաստային հստակեցում մտցնելու համար:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

43.	**ՀՀ կառավարություն**	**10-րդ հոդված 1-ին մաս**	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 10-րդ հոդված 1-ին մասի՝ -6-րդ կետից առաջարկում ենք հանել «, իրականացնում է օրենքով իրեն վերապահված այլ լիազորություններ» բառերը, քանի որ նույն մասի 8-րդ կետում առաջարկվում է լրացնել, որ հանձնաժողովի նախագահը իրականացնում է սույն օրենքով, այլ օրենքներով և ենթաօրենսդրական նորմատիվ իրավական ակտերով նախատեսված այլ լիազորություններ: - 8-րդ կետում «օրենքով» բառից առաջ առաջարկում ենք լրացնել «սույն» բառը, իսկ «օրենքով» բառից հետո լրացնել «այլ օրենքներով և ենթաօրենսդրական նորմատիվ իրավական ակտերով» բառերը՝ կարգավորման հստակ շարադրանք ապահովելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
44.	**ՀՀ կառավարություն**	12-րդ հոդվածի վերնագիր, 6-րդ և 7-րդ մասեր	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 12-րդ հոդվածի՝ -վերնագրում «դադարեցումը» բառից հետո լրացնել «և կասեցումը» բառերը՝ նկատի ունենալով, որ հնարավոր է առաջանա Հանձնաժողովի անդամի լիազորությունները կասեցնելու անհրաժեշտության օբյեկտիվ իրավիճակ, որն առաջարկվում է կանոնակարգել այս հոդվածով: - 6-րդ մասից առաջարկում ենք հանել	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			«վարչապետին և» բառերը, իսկ «Ազգային ժողովի նախագահին» բառերից հետո լրացնել «,ինչպես նաև այն մարմնին, որն իրավասու է տվյալ պաշտոնում թեկնածու առաջադրելու, միաժամանակ՝» հաշվի առնելով, որ առաջարկվում է փոփոխել Հանձնաժողովի անդամի թեկնածու առաջադրելու մարմինների կազմը: - 7-րդ մասում առաջարկում ենք կարգավորումներ նախատեսել նաև Հանձնաժողովի անդամի լիազորությունների կասեցման վերաբերյալ և լրացնել նոր՝ 7-րդ մաս՝ հետևյալ բովանդակությամբ. «7. Հանձնաժողովի անդամի լիազորությունները կասեցվում են սույն հոդվածի 2-րդ մասով նախատեսված եզրակացության ընդունման պահից մինչև «Ազգային ժողովի կանոնակարգ» սահմանադրական օրենքով սահմանված կարգով որոշման ընդունումը:»:		
45.	**ՀՀ կառավարություն**	13-րդ հոդվածի 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 13-րդ հոդվածի 1-ին մասում առաջարկում ենք «մասնագիտական» բառից հետո լրացնել «կառուցվածքային» բառը, քանի որ կարգավորող օրենսդրությամբ կիրառվում է «կառուցվածքային ստորաբաժանում» ձևակերպումը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

46.	**ՀՀ կառավարություն**	14-րդ հոդվածի 1-ին, 2-րդ և 4-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 14-րդ հոդվածի՝ -1-ին մասում առաջարկում ենք «հիմնական» բառից առաջ լրացնել «իսկ» բառը, իսկ «մասնագիտական» բառից հետո «կառուցվածքային» բառը, քանի որ կարգավորող օրենսդրությամբ կիրառվում է «կառուցվածքային ստորաբաժանում» ձևակերպումը: -2-րդ մասում առաջարկում ենք «ՀՀ» հապավումը հանել՝ հաշվի առնելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 18-րդ հոդվածի 3-րդ մասի պահանջը: -2-րդ մասում «կոմպետենցիաների» բառից հետո հանել «(գիտելիքների, ունակությունների, հմտությունների և վարքագծի պարտադիր պահանջների ամբողջություն)» բառերը, քանի որ նշված հասկացության սահմանումը տրված է «Քաղաքացիական ծառայության մասին» օրենքում: - 4-րդ մասում «Հանձնաժողովում» բառը փոխարինել «Տեղեկատվական համակարգերի կարգավորման մարմնում» բառերով, իսկ «պարգևատրումների» բառը փոխարինել «պարգևատրման» բառով՝ կարգավորման հստակեցման նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
47.	**ՀՀ կառավարություն**	**16-րդ հոդվածի 1-ին մաս**	Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի	Կատարվել է համապատասխան	**Ընդունվել է**

			նախագծի 16-րդ հոդվածի՝ - 1-ին մասի 6-րդ կետում առաջարկում ենք «իրականացնում» բառը փոխարինել «կազմակերպում» բառով, իսկ «հոսթինգ» բառից հետո լրացնել «օգտագործումը» բառը՝ կարգավորման հստակեցման նպատակով: -2-րդ մասում առաջարկում ենք «նորմատիվ» բառից հետո լրացնել «իրավական ակտեր» բառերը՝ հաշվի առնելով, որ օրենքով լիազորված լինելու դեպքում նորմատիվ իրավական ակտը հիշատակելիս կիրառվում է «ենթաօրենսդրական նորմատիվ իրավական ակտ» հասկացությունը:	փոփոխություն:	
48.	**ՀՀ կառավարություն**	18-րդ հոդված, 5-րդ մաս, 11-13-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 18-րդ հոդվածի՝ -5-րդ մասում առաջարկում ենք «երեք» բառը փոխարինել «չորս» բառով՝ հաշվի առնելով, որ առաջարկվում է Հանձնաժողովի նիստերում որոշումները և եզրակացություններն ընդունվեն Հանձնաժողովի անդամների ընդհանուր թվի ձայների մեծամասնությամբ: - 1-ին մասում թեև նշվում է Հանձնաժողովի դռնփակ նիստ գումարելու հնարավորության մասին, սակայն մի շարք ընթացակարգային հարցեր կարգավորված չեն: Հետևաբար, առաջարկվում է 18-րդ հոդվածում կարգավորումներ նախատեսել դռնփակ նիստ գումարելու ընթացակարգային	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հարցեր՝ լրացնելով նոր 11-13-րդ մասեր՝ հետևյալ բովանդակությամբ. «11. Շահագրգիռ անձանց շահերի, ներառյալ՝ առևտրային գաղտնիքի, ինչպես նաև պետական անվտանգության, հասարակական կարգի կամ բարոյականության պաշտպանության նպատակով Հանձնաժողովը որոշում է կայացնում նիստը կամ դրա առանձին մասն անցկացնել դռնփակ: 12. Հարցը կամ դրա մասը դռնփակ նիստում քննելու մասին հարցը քննարկվում է դռնփակ: 13. Հարցը կամ դրա մասը դռնփակ նիստում քննելու մասին որոշում կայացվելու դեպքում նիստին կամ դրա առանձին մասին մասնակցելու իրավունք ունեցող անձանց շրջանակը որոշում է Հանձնաժողովի նախագահը:»:		
49.	**ՀՀ կառավարություն**	20-րդ հոդված 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 20-րդ հոդվածի 1-ին մասում առաջարկում ենք փոխել Հանձնաժողովի որոշումների և եզրակացությունների ընդունման համար անհրաժեշտ ձայների քանակը՝ առաջարկելով, որ դրանք ընդունվեն Հանձնաժողովի անդամների ընդհանուր թվի ձայների մեծամասնությամբ: Հետևաբար առաջարկվում է 20-րդ հոդվածի 1-ին մասում «նիստին մասնակցող անդամների» բառերը փոխարինել	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			«Հանձնաժողովի անդամների ընդհանուր թվի» բառերով:		
50.	**ՀՀ կառավարություն**	25-րդ հոդվածի 1-ին և 2-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 25-րդ հոդվածի՝ - 1-ին մասում առաջարկում ենք «Վարչարարության հիմունքների և վարչական վարույթի մասին» օրենքին հղում կատարելիս առաջարկում ենք «օրենքով» բառին նախորդող «Հայաստանի Հանրապետության» բառերը հանել՝ հիմք ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 18-րդ հոդվածի 3-րդ մասի պահանջը: -2-րդ մասում «Հանձնաժաղովի» բառն առաջարկում ենք փոխարինել «Հանձնաժողովի» բառով՝ տառասխալն ուղղելու նպատակով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
51.	**ՀՀ կառավարություն**	28-րդ հոդվածի վերնագիր, 1-4-րդ մասեր, 8-րդ մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 28-րդ հոդվածի՝ -վերնագրում «և համապատասխանության գնահատում» բառերն առաջարկում ենք հանել, քանի որ համապատասխանության գնահատում իրականացնելը վերահսկողության միջոց է: 1-ին մասում «3» թիվն առաջարկում եմ փոխարինել «2» թվով՝ ներքին հղումները ճիշտ կատարելու համար:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			2-րդ և 3-րդ մասերը առաջարկում ենք տեղերով միմյանց հետ փոխել՝ մտքի տրամաբանական հաջորդականությունը ապահովելու նպատակով, 3-րդ մասից հանել «այլ» բառը՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով, 4-րդ մասից «վերահսկող» բառից հետո լրացնել «այլ» բառը՝ տերմինների միատեսակ կիրառություն ապահովելու նպատակով, 8-րդ մասում «3» թիվը փոխարինել «2» թվով, իսկ «այլ» բառը հանել՝ ճիշտ ներքին հղում կատարելու և տերմինների միտեսակ կիրառություն ապահովելու նպատակով:		
52.	**ՀՀ կառավարություն**	30-րդ հոդված 2-րդ մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 30-րդ հոդվածի՝ -1-ին մասի 2-րդ կետում «պարտավոր է» բառերն առաջարկում ենք հանել՝ իմպերատիվ-հրամայական ոճը պահպանելու համար: - 2-րդ մասում երկրորդ նախադասությունն առաջարկում եմ շարադրել հետևյալ խմբագրությամբ. «Գնահատող խմբի անդամները, հրավերի առկայության դեպքում, կարող են մասնակցել վերահսկվող իրավաբանական անձի կառավարման մարմինների նիստերին, ժողովներին և քննարկումներին, ներկայացնել համապատասխանության գնահատման արդյունքները, հնարավոր	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հետևանքները:»՝ հիմք ընդունելով, որ գնահատող խմբի անդամները կարող են մասնացել նիստերին միայն այդպիսի հրավեր ունենալու դեպքում:		
53.	**ՀՀ Կառավարություն**	35-րդ հոդված 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 35-րդ հոդված 1-ին մասից հանել «կամ համապատասխանության գնահատման արձանագրությունը ստորագրելուց հրաժարվելը» բառերը, քան որ արձանագրություն չստորագրելը չի կարող դիտարկվել որպես խոչընդոտում:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
54.	**ՀՀ կառավարություն**	36-րդ հոդված 1-ին և 5-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 36-րդ հոդվածի՝ - 1-ին մասում առաջարկում ենք «այն» բառը փոխարինել «այլ» բառով: -5-րդ մասում «կառավարչին:» բառից հետո լրացնել «, բացառությամբ սույն հոդվածի 1-ին մասով նախատեսված՝ տեղեկատվական համակարգի կառավարչի համաձայնությամբ մշտադիտարկում իրականացնելու դեպքի:» բառերը՝ ներքին հակասություններից խուսափելու համար:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
55.	**ՀՀ կառավարություն**	40-րդ հոդված 1-ին և 2-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 40-րդ հոդվածի՝ 1-ին մասն առաջարկում ենք հանել, քանի որ կրկնվում է «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 17-րդ հոդվածի 4-ի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			րդ մասի կարգավորումը, իսկ մյուս մասերի համարակալումը փոփոխել: 2-րդ մասում առաջարկում ենք «Քաղաքացիական ծառայության մասին» օրենքով» բառերը նախատեսել «Հայաստանի Հանրապետության աշխատանքային օրենսդրությամբ» բառերից առաջ՝ հաշվի առնելով, որ իրավական պրակտիկայի տեսանկյունից «Քաղաքացիական ծառայության մասին» օրենքը պետք է կիրառվի նախքան ՀՀ աշխատանքային օրենսգիրքը: Նշված նաև բխում է «Քաղաքացիական ծառայության մասին» օրենքի 2-րդ հոդվածի պահանջներից: Հաշվի առնելով տեղեկատվական համակարգերի կարգավորման մարմնում ծառայությունն առանձին ծառայության տեսակ է, անհրաժեշտ է կարգավորում նախատեսել, թե տվյալ ծառայության յուրաքանչյուր պաշտոնի անձնագրի չափանիշները և առանձին պաշտոնների անձնագրերը ով է հաստատում: Հետևաբար, առաջարկվում է լրացնել նոր՝ 3-րդ մաս՝ հետևյալ բովանդակությամբ. «3.Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության յուրաքանչյուր պաշտոն ունի պաշտոնի անձնագիր (աշխատատեղի նկարագիր), որը հաստատում է գլխավոր քարտուղարը: Տեղեկատվական համակարգերի		

			կարգավորման մարմնում ծառայության պաշտոնների անձնագրերի չափանիշները հաստատում է Հանձնաժողովի նախագահը:»:		
56.	**ՀՀ կառավարություն**	41-րդ հոդված	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 41-րդ հոդվածն առաջարկում ենք շարադրել հետևյալ նոր խմբագրությամբ. «**Հոդված 41. Տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողների պաշտոնների համակարգը** 1. Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնները դասակարգվում են խմբերի՝ ելնելով այդ պաշտոնները զբաղեցնող անձանց աշխատանքի կազմակերպման և ղեկավարման պատասխանատվության, որոշումներ կայացնելու լիազորությունների, գործունեության ազդեցության, շփումների և ներկայացուցչության, խնդիրների բարդության և դրանց լուծման, ինչպես նաև մասնագիտական գիտելիքների և կոմպետենցիաների տիրապետման տեսանկյունից ներկայացվող պահանջներից: 2. Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնները դասակարգվում են երեք խմբերի, որոնցից յուրաքանչյուրը դասակարգվում է երեք ենթախմբերի: 3.Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			պաշտոնների անվանումները, խմբերը և ենթախմբերը սահմանում է Հանձնաժողովը՝ որի համար սույն օրենքի 43-րդ հոդվածի առաջին մասում նշված որակավորումները կրում են կողմնորոշիչ բնույթ:»: Նշված փոփոխությունները պայմանավորված է նրանով, որ նոր խմբագրությամբ շարադրվող հոդվածի 1-ին մասով նկարագրված պահանջներին համապատասխանելու համար մասնագետները պետք է անցնեն միջազգայնորեն ճանաչում գտած որակավորումներ, որոնք չեն համապատասխանում պաշտոնների ենթախմբերին: Դրա համար առաջարկվում է օրենքով ամրագրել պաշտոնների խմբերի և ենթախմբերի քանակը, իսկ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնների անվանումները, խմբերը և ենթախմբերը կսահմանի Հանձնաժողովը հիմք է ընդունելով 41-րդ և 43-րդ հոդվածների 1-ին մասերի պահանջները:		
57.	**ՀՀ կառավարություն**	42-րդ հոդված 1-ին մասի	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 42-րդ հոդվածի 1-ին մասն առաջարկում եմ շարադրել հետևյալ խմբագրությամբ. «1. Տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողի պաշտոն զբաղեցնելու համար Հայաստանի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			Հանրապետության քաղաքացին. 1) պետք է ունենա առնվազն միջնակարգ կրթություն, բացառությամբ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնների ամենաբարձր խմբի ամենաբարձր ենթախմբի պաշտոնների, որոնք զբաղեցնելու համար Հայաստանի Հանրապետության քաղաքացին պետք է ունենա բարձրագույն կրթություն. 2) պետք է տիրապետի հայերենին. 3) պետք է բավարարի տվյալ պաշտոնի անձնագրով ներկայացվող պահանջներին և առկա չլինի պաշտոնի նշանակման համար օրենքով սահմանված սահմանափակումները. 4) պաշտոնի անձնագրով նախատեսված դեպքերում պետք է ունենա պահանջվող գիտելիքները ու կոմպետենցիաները հիմնավորող փաստաթուղթ (օրինակ՝ որակավորում, սերտիֆիկատ և այլն):»: Նման մոտեցմամբ հնարավորություն կստեղծվի որպեսզի միջազգայնորեն ճանաչում ունեցող և մասնագիտական գիտելիքները ու կոմպետենցիաները հիմնավորող փաստաթուղթ ունեցող մասնագետները դիմեն Հանձնաժողովի մասնագիտական ստորաբաժանումներում աշխատանքի անցնելու համար, իսկ եթե հավակնեն տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության		

			պաշտոնների ամենաբարձր խմբի ամենաբարձր ենթախմբի պաշտոնների, ապա բարձրագույն կրթություն ունենալու պահանջը պարտադիր կհամարվի:		
58.	**ՀՀ կառավարություն**	43-րդ հոդվածի 3-րդ և 6-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 43-րդ հոդվածի՝ -3-րդ մասն առաջարկում ենք շարադրել հետևյալ նոր խմբագրությամբ. «3. Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնները համալրվում են կա՛մ մրցութային կարգով, կա՛մ փոխադրման կարգով, կա՛մ կադրերի ռեզերվից պաշտոնների համալրման կարգով: Տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնները մրցութային կարգով համալրելու կարգը և պայմանները սահմանում է Հանձնաժողովը:»: 3-րդ մասում առաջարկվող խմբագրումը նպատակ ունի հստակեցնել ինքնավար մարմնի լիազորող նորմի շրջանակը՝ տարաբնույթ մեկնաբանություններից խուսափելու նպատակով: - 6-րդ մասն առաջարկում ենք հանել: 6-րդ մասով նախատեսված հարաբերությունների կարգավորումը թողնվել է ինքնավար մարմնի հաստատմանը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

59.	**ՀՀ կառավարություն**	44-րդ հոդված 1-ին և 2-րդ, 4-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 44-րդ հոդվածի՝ - 1-ին մասում առաջարկում ենք «սույն օրենքով սահմանված պահանջները բավարարող կամ բակալավրիատի ուսանող հանդիսացող և սույն օրենքի 46-րդ հոդվածի 1-ին մասի 1-ին կետի պահանջից բացի, մյուս պահանջները բավարարող անձը:» բառերը փոխարինել «և, բացի սույն օրենքի 42-րդ հոդվածի 1-ին մասի 1-ին կետում նախատեսված՝ մասնագիտական գիտելիքները ու կոմպետենցիաները հիմնավորող փաստաթուղթ ունենալու պահանջից, սույն օրենքով սահմանված մյուս պահանջները բավարարող անձը:» բառերով՝ հաշվի առնելով 46-րդ հոդվածի 1-ին մասում առաջարկվող փոփոխությունը: -2-րդ մասում լրացնել նոր նախադասություն՝ հետևյալ բովանդակությամբ. «Սույն մասում նշված վերապատրաստման դասընթացներն անցնելու արդյունքների վերաբերյալ Հանձնաժողովի կողմից տրվում է համապատասխան փաստաթուղթ:»: Առաջարկվող լրացումը հստակեցնում է ինքնավար մարմնի լիազորությունների և սկսնակ մասնագետների իրավունքների շրջանակը: 3-րդ մասում լրացնել նոր նախադասություն՝ հետևյալ բովանդակությամբ. «Տեղեկատվական համակարգերի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			կարգավորման մարմնում սկսնակ մասնագետների աշխատանքի ժամանակահատվածը համարվում է հանրային ծառայության ստաժ:»: Նշված լրացմամբ երաշխիքներ է ստեղծվում սկսնակ մասնագետների համար, որը համահունչ է ինչպես ՀՀ աշխատանքային օրենսդրության, այնպես էլ «Հանրային ծառայության մասին» օրենքի 49-րդ հոդվածի 2-րդ մասի պահանջներին: Լրացնել նոր՝ 4-րդ մաս՝ հետևյալ բովանդակությամբ. «4. Տեղեկատվական համակարգերի կարգավորման մարմնում որպես սկսնակ մասնագետ ներգրավվելու կարգը սահմանում է Հանձնաժողովը:»: 4-րդ մասում կատարվող լրացումը հստակեցնում է ինքնավար մարմնի գործառույթների շրջանակը և լիազորում է ընդունել իրավական ակտ, որը նախկին տարբերակում բացակայում էր:		
60.	**ՀՀ կառավարություն**	45-րդ հոդված 2-րդ մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 45-րդ հոդվածի՝ - 2-րդ մասը շարադրել հետևյալ նոր խմբագրությամբ. «2. Հանձնաժողովի քաղաքացիական ծառայողները պաշտոնի նշանակվում և պաշտոնից ազատվում են «Քաղաքացիական ծառայության մասին» օրենքով սահմանված կարգով:»՝	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			ընթացակարգը հստակեցնելու համար: 2-րդ մասով նախատեսված կարգավորումը շարադրել երրորդ մասում և համապատասխանաբար փոփոխել մյուս մասերի համարակալումը:		
61.	**ՀՀ կառավարություն**	46-րդ հոդվածի 6-րդ և 7-րդ մասեր մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 46-րդ հոդվածի՝ -6-րդ մասն առաջարկում ենք հանել: Նշված հարաբերության կարգավորումը թողնվել է ինքնավար մարմնին, քանի ՀՀ օրենքներով միասնական կարգավորում չկա, մոտեցումները տարբեր են ըստ ծառայության տեսակների: - 7-րդ մասից սկսել փոփոխել մասերի հաջորդական համարակալումը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
62.	**ՀՀ կառավարություն**	47-րդ հոդված 1-3-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 47-րդ հոդվածի՝ -1-ին և 2-րդ մասերն առաջարկում ենք միավորել և շարադրել հետևյալ նոր խմբագրությամբ. «Տեղեկատվական համակարգերի կարգավորման մարմնի ծառայողի (բացառությամբ կադրերի ռեզերվում գտնվող անձանց) առաջխաղացումն առանց մրցույթի իրականացվում է համապատասխան պաշտոնի առանձնահատկություններով պայմանավորված կատարողականի գնահատման գործընթացի արդյունքների հիման վրա:»՝ հաշվի առնելով 45-րդ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հոդվածում առաջարկվող փոփոխությունները: -3-րդ մասի համարակալումը փոխել և «կազմակերպման» բառից հետո հանել «և» շաղկապը:		
63.	**ՀՀ կառավարություն**	49-րդ հոդված 1-ին և 2-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 49-րդ հոդվածի 1-ին մասի՝ 6-րդ կետում «մահացած հայտարարվելու» բառերն անհրաժեշտ է փոխարինել «մահացած ճանաչելու» բառերով՝ նկատի ունենալով Հայաստանի Հանրապետության քաղաքացիական օրենսգրքի 47-րդ հոդվածը: -11-րդ կետն առաջարկում ենք հանել, քանի որ 11-րդ կետի պահանջը տեխնիկական վրիպակ արդյունքում էր նախատեսվել: Այս օրենքում ծառայողների նկատմամբ սահմանված չէ շարունակական մասնագիտական զարգացման կրեդիտներ հավաքելու պայանջ, հետևաբար, չի կարող հիմք հանդիսանալ պաշտոնից ազատման համար: 2-րդ մասում «մահվան» բառից հետո առաջարկում ենք լրացնել «կամ պաշտոնից ազատման» բառերը՝ հաշվի առնելով, որ ծառայողին պաշտոնից ազատելուց ևս դադարում են նրա պարտականությունները:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
64.	**ՀՀ կառավարություն**	50-րդ հոդված 1-ին մասի 3-րդ և 5-րդ կետեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 50-րդ հոդվածի 1-ին մասի՝		

			-3-րդ կետն առաջարկում ենք շարադրել հետևյալ նոր խմբագրությամբ. «3) աշխատանքի համար ստանալ համարժեք վարձատրություն.» -5-րդ կետում «սահմանված կարգով վերապատրաստվելու» բառերը փոխարինել «մասնագիտական գիտելիքների և կոմպետենցիաների բարելավման համար սահմանված կարգով մասնակցել վերապատրաստումների՝» բառերով՝ առավել հստակեցնելով կարգավորումը:		
65.	**ՀՀ կառավարություն**	53-րդ հոդված 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 53-րդ հոդվածի 1-ին մասի 1-ին կետում «գործունեության էթիկայի» բառերը փոխարինել «սահմանված վարքագծի» բառերով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
66.	**ՀՀ կառավարություն**	58-րդ հոդվածի վերնագիր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 58-րդ հոդվածի վերնագրում առաջարկում ենք «ծառայողի» բառից հետո լրացնել «և անդամների» բառերը՝ նկատի ունենալով նշված հոդվածի 2-րդ մասը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
67.	**ՀՀ կառավարություն**	59-րդ հոդված 4-րդ և 9-րդ մաեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 59-րդ հոդվածի՝ 4-րդ մասում «տեղեկատվական համակարգերի կարգավորման մարմնում» բառերն առաջարկում ենք փոխարինել «հանրային» բառով՝ նպատակ ունենալով նախատեսել, որ կադրերի ռեզերվում	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			գրանցված լինելու ժամանակահատվածը համարվելու է հանրային ծառայության ստաժ, քանի որ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայությունն, ինքնին, համարվելու է հանրային ծառայության առանձին տեսակ: 9-րդ մասը շարադրել հետևյալ խմբագրությամբ. «9. Ծառայության կադրերի ռեզերվը վարելու, կադրերի ռեզերվում գրանցելու, կադրերի ռեզերվից հանելու և կադրերի ռեզերվից պաշտոնների համալրման կարգը սահմանում է Հանձնաժողովը»: Առաջարկվող խմբագրությամբ տարբերակում լրացվել է, որ Հանձնաժողովն է սահմանում նաև կադրերի ռեզերվից պաշտոնների համալրման կարգը, քանի որ հիշյալ օրենքի 43-րդ հոդվածի 3-րդ մասով սահմանվել է, որ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության պաշտոնները համալրվում են նաև կադրերի ռեզերվից, իսկ թե ինչ կերպ էր այդ համալրումը կատարվում, կարգավորում չէր նախատեսվել:		
68.	**ՀՀ կառավարություն**	60-րդ հոդված 1-ին մաս	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 60-րդ հոդվածի 1-ին մասում առաջարկում ենք «հաջորդող տասներորդ օրը» բառերը փոխարինել «հաջորդող օրվանից» բառերով՝ նպատակ ունենալով, որպեսզի օրենքն առավել շուտ ուժի մեջ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			մտնի:		
69.	**ՀՀ կառավարություն**	61-րդ հոդված 1-ին, 2-3-րդ, 6-րդ, 8-րդ և 11-րդ մասեր	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 61-րդ հոդվածի՝ - 1-ին մասից առաջարկում ենք հանել «սույն օրենքով նախատեսված» բառերը, քանի որ ինքնին հասկանալի է, թե խոսքն ինչի մասին է: - 2-րդ մասում «Կառավարությունն» բառն առաջարկում ենք փոխարինել « սույն օրենքով նախատեսված մարմիններն» բառերով, իսկ «իրականացնում է» բառերը փոխարինել «իրականացնում են» բառերով՝ հաշվի առնելով, որ առաջարկվում է փոփոխել Հանձնաժողովի անդամի թեկնածու առաջադրող մարմինների կազմը: -6-րդ մասում «հոդվածի 1-ին մասում նշված ժամկետի մեկնարկից հետո երկու ամսվա ընթացքում» բառերը փոխարինել «օրենքի ուժի մեջ մտնելուց երեք ամսվա ընթացքում» բառերով՝ հիմք ընդունելով Հանձնաժողովի անդամների նշանակման գործընթացի համար անհրաժեշտ ժամկետները: -8-րդ մասը շարադրել հետևյալ խմբագրությամբ՝ «Հանձնաժողովը համարվում է ձևավորված, եթե Ազգային ժողովի կողմից նշանակվել են Հանձնաժողովի առնվազն չորս անդամ: Հանձնաժողովն իր կազմավորումից հետո՝ մեկամսյա ժամկետում, հաստատում է իր	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			կանոնադրությունը և կառուցվածքը:»: -8-րդ մասում լրացվող առաջին նախադասությամբ նպատակ ունենք հստակեցնելու, թե կոնկրետ Հանձնաժողովի քանի անդամի նշանակման դեպքում է Հանձնաժողովը համարվելու ձևավորված: Այդ առնչությամբ հաշվի առնելով, որ Հանձնաժողովի նիստի իրավազորության համար նախատեսված է Հանձնաժողովի 4 անդամի պարտադիր ներկայության պահանջ, հետևաբար առաջարկվում է, որ 4 անդամ նշանակվելու դեպքում Հանձնաժողովը համարվի ձևավորված: 11-րդ մասը շարադրել հետևյալ խմբագրությամբ. «11. Հանձնաժողովի կառուցվածքի, պաշտոնների անվանացանկի և հաստիքացուցակի հաստատումից հետո մինչև հաստիքների օրենքով սահմանված կարգով համալրումը Հանձնաժողովի քաղաքացիական ծառայության հաստիքները զբաղեցվում են «Քաղաքացիական ծառայության մասին» օրենքով սահմանված ժամկետային աշխատանքային պայմանագիր կնքելու կարգով, իսկ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության հաստիքները զբաղեցվում են սույն օրենքով սահմանված ժամկետային աշխատանքային պայմանագիր կնքելու կարգով:» Առաջարկվող խմբագրությամբ		

			հնարավորություն կստեղծվի հստակ տարանջատել նախքան Հանձնաժողովի քաղաքացիական ծառայության և տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության հաստիքների օրենքով սահմանված կարգով համալրումը, դրանք զբաղեցվեն ժակետային աշխատանքային պայմանագիր կնքելու եղանակով՝ քաղաքացիական ծառայության հաստիքների դեպքում «Քաղաքացիական ծառայության մասին» օրենքով սահմանված կարգով, իսկ տեղեկատվական համակարգերի կարգավորման մարմնում ծառայության հաստիքների դեպքում այս օրենքով սահմանված կարգով:		
70.	**ՀՀ կառավարություն**	**Նախագծի վերնագիր**	«Տեղեկատվության ազատության մասին» Հայաստանի Հանրապետության օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծում առաջարկում ենք վերնագրից հանել երկրորդ «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ» բառերը՝ ապահովելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 18-րդ հոդվածի 3-րդ մասի պահանջը, իսկ «ՓՈՓՈԽՈՒԹՅՈՒՆ» բառը փոխարինել «ՓՈՓՈԽՈՒԹՅՈՒՆՆԵՐ» բառով՝ հաշվի առնելով, որ նախագծով նախատեսվում են մեկից ավելի փոփոխություն:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
71.	**ՀՀ կառավարություն**	Նախագծի վերնագիր	«Պետական գաղտնիքի մասին» Հայաստանի Հանրապետության օրենքում փոփոխություն կատարելու մասին» օրենքի	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			նախագծում առաջարկում ենք վերնագրից հանել երկրորդ «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ» բառերը՝ ապահովելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 18-րդ հոդվածի 3-րդ մասի պահանջը:		
72.	**ՀՀ կառավարություն**	**1-ին հոդված**	«Պետական գաղտնիքի մասին» Հայաստանի Հանրապետության օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 1-ին հոդվածից առաջարկում ենք հանել «(այսուհետ՝ Օրենք)», «/այսուհետ՝ Օրենք/» ձևակերպումը՝ հիմք ընդունելով այն հանագմանքը, որ «Պետական գաղտնիքի մասին» Հայաստանի Հանրապետության օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծում օրենքին այլևս հղում չի կատարվում:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
73.	**ՀՀ կառավարություն**	**1-ին հոդված 2-րդ մաս**	««Պետական գաղտնիքի մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 1-ին հոդվածով նոր խմբագրությամբ շարադրվող «Պետական գաղտնիքի մասին» օրենքի 7-րդ գլխի 31. 2-րդ հոդվածի 1-ին մասում կիրառվում է «մշակող (կատարող)», իսկ 2-րդ մասում՝ «մշակող /պատրաստող/» ձևակերպումը: Առաջարկվում է նշված հոդվածի 2-րդ մասում «մշակող /պատրաստող/» բառերը փոխարինել «մշակող (կատարող)» բառերով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
74.	**ՀՀ կառավարություն**	**2-րդ հոդված**	««Պետական գաղտնիքի մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածում «մինչև 2026	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			թվականի հունվարի 1-ը» բառերը փոխարինել «սույն օրենքի ուժի մեջ մտնելուց հետո վեցամսյա ժամկետում» բառերով՝ նախատեսելով բավարար ժամանակահատված օրենքից բխող իրավական ակտերի մշակման և ընդունման համար:		
75.	**ՀՀ կառավարություն**	Նախագծի վերնագիր և 1-ին հոդված	«Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի վերնագրից առաջարկում ենք հանել երկրորդ «ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ» բառերը՝ ապահովելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 18-րդ հոդվածի 3-րդ մասի պահանջը: Նաև առաջարկում ենք հիշյալ օրենքի նախագծի 1-ին հոդվածում «Անձնական տվյալների պաշտպանության մասին» օրենքին հղում կատարելիս ևս հանել «Հայաստանի Հանրապետության» բառերը, իսկ «/այսուհետ՝ Օրենք/» բառերը փոխարինել «(այսուհետ՝ Օրենք)» բառերով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
76.	**ՀՀ կառավարություն**	2-րդ հոդվածի 2-րդ մաս	«Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի 2-րդ մասում «մարմինը» բառից հետո առաջարկում ենք լրացնել «:» կետադրական նշանը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

77.	**ՀՀ կառավարություն**	6-րդ հոդվածի 2-րդ մաս	««Անձնական տվյալների պաշտպանության մասին» օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 6-րդ հոդվածի 2-րդ մասում «նորմատիվ» բառից հետո առաջարկում ենք լրացնել «իրավական» բառը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
78.	**ՀՀ կառավարություն**	**1-ին հոդված**	«Պետական պաշտոններ և պետական ծառայության պաշտոններ զբաղեցնող անձանց վարձատրության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 1-ին հոդվածից առաջարկում ենք հանել «(այսուհետ՝ Օրենք)», ձևակերպումը՝ հիմք ընդունելով այն հանագմանքը, որ հիշյալ օրենքի նախագծում «Պետական պաշտոններ և պետական ծառայության պաշտոններ զբաղեցնող անձանց վարձատրության մասին» օրենքին այլևս հղում չի կատարվում:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
79.	**ՀՀ կառավարություն**	**2-րդ հոդված**	Պետական պաշտոններ և պետական ծառայության պաշտոններ զբաղեցնող անձանց վարձատրության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածով նախատեսված կարգավորումն առաջարկում ենք համարակալել:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
80.	**ՀՀ կառավարություն**	1-ին հոդված	«Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 1-ին հոդվածում առաջարկում ենք ուժը կորցրած ճանաչել ոչ թե «տեղեկատվական համակարգ»	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հասկացությունը, այլ համապատասխան չհամարկալված պարբերությունը, ինչպես նշվում է «Նորմատիվ իրավական ակտերի մասին» օրենքի 33-րդ հոդվածի 1-ին մասի 4-րդ կետում:		
81.	**ՀՀ կառավարություն**	**2-րդ հոդված**	«Ազգային անվտանգության մարմինների մասին» օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածով նախատեսվող «Ազգային անվտանգության մարմինների մասին» օրենքի 15-րդ հոդվածում լրացվող նոր 1.2-րդ մասի համարը տեքստից առաջարկում ենք բաժանել միջակետով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
82.	**ՀՀ կառավարություն**	3-րդ հոդված	«Ազգային անվտանգության մարմինների մասին» օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 3-րդ հոդվածում առաջարկում ենք «Ինքնավար մարմնի» բառերից առաջ լրացնել ««Կիբեռանվտանգության մասին» օրենքով նախատեսված» բառերը, քանի որ Ինքնավար մարմնի համակարգչային արտակարգ իրավիճակների արձագանքման թիմերի մասին նշվում է «Կիբեռանվտանգության մասին» օրենքում:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
83.	**ՀՀ կառավարություն**	**1-ին հոդված**	«Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 1-ին հոդվածում առաջարկում ենք ««Տեղեկատվական համակարգերում անձնական տվյալները մշակելու	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			անվտանգությունն ապահովելուն ներկայացվող պահանջները,» բառերը հանել» բառերը փոխարինել ««Տեղեկատվական համակարգերում անձնական տվյալները մշակելու անվտանգությունն ապահովելուն ներկայացվող պահանջները, կենսաչափական» բառերը փոխարինել «Կենսաչափական» բառով:» բառերով՝ ինկորպորացիայի ժամանակ խնդիրներից խուսափելու նպատակով:		
84.	**ՀՀ կառավարություն**	**2-րդ հոդված**	«Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածով Օրենսգրքում լրացվող նոր՝ 189.31-րդ հոդվածի 2-րդ մասում առաջարկում ենք վերանայել և հստակեցնել դիսպոզիցիան՝ «Տեղեկատվական համակարգերում տվյալներ կամ տեղեկություններ մշակելու անվտանգությունն ապահովելուն ներկայացվող միջոցառումներ չիրականացնելը կամ օրենքով» բառերը փոխարինելով «Տեղեկատվական համակարգերի անվտանգության միջոցառումների համակարգով նախատեսված պահանջները չպահպանելը կամ տվյալներ կամ տեղեկություններ մշակելուն օրենքով» բառերով, որպեսզի յուրաքանչյուր անձի համար հստակ և	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			որոշակի լինի իր վրա դրված պարտականությունը, դրա բովանդակությունը, ինչպես նաև կանխատեսելի լինեն իր վրա դրված պարտականության չկատարման հետևանքները:		
85.	**ՀՀ կառավարություն**	**3-րդ հոդված**	«Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 3-րդ հոդվածով Օրենսգրքում լրացվող նոր՝ 193.4-րդ հոդվածի՝ - 3-րդ և 5-րդ մասերում առաջարկում ենք հստակեցնել դիսպոզիցիաները՝ դրանք համապատասխանեցնելով «Կիբեռանվտանգության մասին» օրենքով նախատեսված համապատասխան ձևակերպումներին, ինչպես նաև իրավական որոշակիության ապահովման, իրավական շփոթի և տարաբնույթ մեկնաբանությունների առաջացումից խուսափելու համար: Հետևաբար՝ - 3-րդ մասում «չծանուցելը» բառից հետո առաջարկում ենք լրացնել «կամ կիբեռմիջադեպի վերաբերյալ թարմացված տեղեկատվություն չտրամադրելը՝ ներառյալ կիբեռմիջադեպի ծանրության և ունեցած հետևանքների մասով,» բառերը, իսկ 5-րդ մասում «կարգով» բառից հետո հանել «կիբեռմիջադեպի ծանրության, ձեռնարկված միջոցառումների եւ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			կիբեռմիջադեպի ունեցած հետեւանքների մասին կազմված հաշվետվությունը,» բառերը: - 9-րդ և 10-րդ մասերում կիրառված «և/կամ» ձևակերպումն առաջարկում ենք փոխարինել «կամ» շաղկապով՝ հիմք ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 16-րդ հոդվածի պահանջները:		
86.	**ՀՀ կառավարություն**	**4-րդ հոդված**	«Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 4-րդ հոդվածով Օրենսգրքում լրացվող նոր՝ 171.13-րդ հոդվածի 1-ին մասում առաջարկում ենք «առաջացնում է» բառից հետո լրացնել «նախազգուշացում կամ» բառերը՝ սահմանելով նաև նախազգուշացման կիրառման հնարավորություն իրավաբանական անձի պաշտոնատար անձի նկատմամբ՝ ապահովելու համար համաչափ պատասխանատվություն բոլոր սուբյեկտների նկատմամբ:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
87.	**ՀՀ կառավարություն**	**5-րդ հոդված**	«Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 5-րդ հոդվածով Օրենսգրքում լրացվող նոր՝ 243.1-ին հոդվածի համարն առաջարկում ենք վերնագրից բաժանել միջակետով:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

88.	**ՀՀ կառավարություն**	1-ին հոդվածի 1-ին մասում	««Կառավարության կառուցվածքի և գործունեության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 1-ին հոդվածի 1-ին մասում «արհեստական բանականության» բառից առաջ առաջարկում ենք լրացնել «,» կետադրական նշանը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
89.	**ՀՀ կառավարություն**	2-րդ հոդված	«Հանրային ծառայության մասին» օրենքում լրացումներ կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածում առաջարկում ենք «գլխավոր պաշտոնների 1-ին» բառերը փոխարինել «ամենաբարձր խմբի ամենաբարձր» բառերով՝ նկատի ունենալով, որ «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքում» պաշտոնների խմբերը և ենթախմբերը սահմանող 41-րդ և 42-րդ հոդվածներում կատարվել են փոփոխություններ:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
90.	**ՀՀ կառավարություն**	3-րդ հոդված	«Հանրային ծառայության մասին» օրենքում լրացումներ կատարելու մասին» օրենքի նախագծի 3-րդ հոդվածում առաջարկում ենք ճշգրտել համարակալումը:	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**
91.	**ՀՀ կառավարություն**	Նախագծերի փաթեթում ներառված առանձին օրենքների նախագծերի նշված հոդվածներ	«Տեղեկատվության ազատության մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Պետական գաղտնիքի մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Անձնական տվյալների պաշտպանության մասին» օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 6-րդ	Կատարվել է համապատասխան փոփոխություն:	**Ընդունվել է**

			հոդվածի, «Կառավարության կառուցվածքի և գործունեության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» օրենքում փոփոխություն կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Ազգային անվտանգության մարմինների մասին» օրենքում փոփոխություններ և լրացումներ կատարելու մասին» օրենքի նախագծի 3-րդ հոդվածի, «Նորմատիվ իրավական ակտերի մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Հայաստանի Հանրապետության քրեական դատավարության օրենսգրքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Հանրային ծառայության մասին» օրենքում լրացումներ կատարելու մասին» օրենքի նախագծի 3-րդ հոդվածի, «Ազգային ժողովի կանոնակարգ» սահմանադրական օրենքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի, «Հայաստանի Հանրապետությունում ստուգումների կազմակերպման և անցկացման մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագծի 2-րդ հոդվածի «Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքում փոփոխություն և լրացումներ կատարելու մասին» օրենքի նախագծի 6-րդ		

			հոդվածի վերնագիրն առաջարկում ենք հանել՝ հիմք ընդունելով «Նորմատիվ իրավական ակտերի մասին» օրենքի 14-րդ հոդվածի 8-րդ մասում սահմանված պահանջը:		
92.	**ՀՀ կառավարություն**	Նախագծերի փաթեթում ներառել նոր՝ «Օպերատիվ-հետախուզական գործունեության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագիծ	«Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 20-րդ հոդվածի 1-ին մասի 11-րդ կետով Հանձնաժողովը լիազորվում է օրենքով սահմանված դեպքում դիմել օպերատիվ-հետախուզական գործունեություն իրականացնող մարմիններ տեղեկատվական համակարգերի և կիբեռանվտանգության բնագավառում իրավախախտումների կանխման կամ բացահայտման գործում աջակցություն ստանալու նպատակով: Սակայն օպերատիվ-հետախուզական գործունեություն իրականացնող մարմինները չունեն պարտականություն Հանձնաժողովին աջակցելու, քանզի Նախագծերի փաթեթով լրացում չէր կատարվել «Օպերատիվ-հետախուզական գործունեության մասին» օրենքի 11-րդ հոդվածում: Հետևաբար «Տեղեկատվական		**Ընդունվել է**

			համակարգերի կարգավորման մարմնի մասին» օրենքի նախագծի 16-րդ հոդվածի 1-ին մասի 11-րդ կետի կարգավորման լիարժեքությունը ապահովելու նպատակով առաջարկվում է Նախագծերի փաթեթում ներառել նոր՝ «Օպերատիվ-հետախուզական գործունեության մասին» օրենքում լրացում կատարելու մասին» օրենքի նախագիծ՝ հետևյալ բովանդակությամբ. «		

			<u>ՆԱԽԱԳԻԾ</u> **ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ** **ՕՐԵՆՔԸ** **«ՕՊԵՐԱՏԻՎ-ՀԵՏԱԽՈՒԶԱԿԱՆ ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ՄԱՍԻՆ» ՕՐԵՆՔՈՒՄ ՓՈՓՈԽՈՒԹՅՈՒՆ ԵՎ ԼՐԱՑՈՒՄ ԿԱՏԱՐԵԼՈՒ ՄԱՍԻՆ** ***Հոդված 1.*** «Օպերատիվ-հետախուզական գործունեության մասին» 2007 թվականի հոկտեմբերի 22-ի ՀՕ-223-Ն օրենքի 11-րդ հոդվածի՝ 1) 1-ին մասի 5-րդ կետում «:» կետադրական նշանը փոխարինել «. » կետադրական նշանով:		

			2) 1-ին մասը լրացնել հետևյալ բովանդակությամբ 6-րդ կետով. «6) աջակցել տեղեկատվական համակարգերի կարգավորման մարմնին՝ տեղեկատվական համակարգերի և կիբեռանվտանգության բնագավառում իրավախախտումների կանխման կամ բացահայտման գործում՝ դիմումի հիման վրա հայցվող՝ իրենց հայտնի դարձած տվյալները (տեղեկությունները) տեղեկատվական համակարգերի կարգավորման մարմնին փոխանցելով:»: ***Հոդված 2.*** Սույն օրենքն ուժի մեջ է մտնում «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի ուժի մեջ մտնելու պահից: »:		