***ՆԱԽԱԳԻԾ***

**ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ**

**Օ Ր Ե Ն Ք Ը**

**ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ**

**Գ Լ ՈՒ Խ  1.**

***ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ***

 Սույն օրենքի նպատակն Հայաստանի Հանրապետությունում կենսական նշանակության ծառայությունների մատուցման համար կիրառվող տեղեկատվական համակարգերում և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգ միջավայրի ստեղծումն է:

**Հոդված 1․ Օրենքի կարգավորման առարկան և գործողության ոլորտը**

1․ Սույն օրենքը կարգավորում է կենսական նշանակության ծառայությունների մատուցման համար կիրառվող տեղեկատվական համակարգերում և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման հետ կապված հարաբերությունները, մասնավորապես՝ սույն օրենքի իմաստով ծառայություն մատուցող համարվող սուբյեկտների շրջանակը, կենսական նշանակության ծառայությունների ոլորտները, կիբեռմիջադեպերի հայտնաբերման, դրանց մասին ծանուցման, կանխարգելման և լուծման, կիբեռանվտանգության ոլորտի պետական կառավարման մարմինների և դրանց լիազորությունների շրջանակի, սույն օրենքի պահանջների պահպանման նկատմամբ հսկողության, վերահսկողության, կիբեռանվտանգության աուդիտի, ինչպես նաև կիբեռանվտանգության հետ կապված այլ հարաբերությունները։

2. Ցանկացած այլ իրավաբանական անձ, որը սույն օրենքի իմաստով չի համարվում ծառայություն մատուցող, Հայաստանի Հանրապետության կառավարության կողմից սահմանված կարգով կարող է կամավոր ստանձնել սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամ հրաժարվել դրանցից:

3. Սույն օրենքի գործողությունը տարածվում է «Փոքր և միջին ձեռնարկատիրության պետական աջակցության մասին» օրենքով սահմանված չափանիշների համաձայն միջին դասակարգված իրավաբանական անձանց և անհատ ձեռնարկատերերի և միջին դասակարգման համար սահմանված չափանիշները գերազանցող իրավաբանական անձանց և անհատ ձեռնարկատերերի նկատմամբ, ովքեր ծառայություն են մատուցում սույն օրենքի 16-րդ հոդվածի 2-րդ մասում թվարկված ոլորտներից մեկում կամ մի քանիսում միաժամանակ և պետական կառավարման կամ տեղական ինքնակառավարման մարմինների նկատմամբ՝ բացառությամբ սույն հոդվածի 4-րդ մասով թվարկված դեպքերի։

4. Անկախ սույն հոդվածի 3-րդ մասում նշված չափանիշներին բավարարելուց՝ սույն օրենքի գործողությունը տարածվում է այն անձի նկատմամբ, ով բավարարում է հետևյալ պայմաններից առնվազն մեկին․

1) հանդիսանում է հանրային էլեկտրոնային հաղորդակցության ծառայություն մատուցող․

2) հանդիսանում է ինտերնետ հասանելիության ծառայություն մատուցող․

3) հանդիսանում է հավաստագրման կենտրոն՝ մատուցելով էլեկտրոնային թվային ստորագրության հավաստագրեր տրամադրող և էլեկտրոնային թվային ստորագրությունների հետ կապված այլ ծառայություններ․

4) հանդիսանում է Հայաստանի վերին մակարդակի ազգային դոմեյն հանդիսացող դոմենային տիրույթի ռեգիստր կամ մատուծում է դոմենային անվանումների գրանցման ծառայություն․

5) հանդիսանում է սույն օրենքի 16-րդ հոդվածի 2-րդ մասում թվարկված որևէ ոլորտում մենաշնորհ կամ գերիշխող դիրք ունեցող կազմակերպություն․

6) որևէ հիմքով շահագործում է կրիտիկական տեղեկատվական ենթակառուցվածք․

7) Ֆիզիկական կամ իրավաբանական անձինք, ովքեր կառավարում, շահագործում, սպասարկում կամ որևէ այլ հիմքով օգտագործում են այլ ծառայություն մատուցողների տեղեկատվական համակարգը կամ կրիտիկական տեղեկատվական ենթակառուցվածքը կամ ապահովում են դրանց փոխգործելիությունը այլ տեղեկատվական համակարգերի հետ.

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

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

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

8. Սույն օրենքով սահմանված կիբեռանվտանգության ապահովմանն ուղղված միջոցառումներ իրականացնելիս ծառայություն մատուցողները անձնական տվյալների հետ կապված ցանկացած գործողություն իրականացնելիս պետք է առաջնորդվեն անձնական տվյալներ մշակելու հետ կապված հարաբերությունները կարգավորող օրենսդրության պահանջներին համապատասխան։

9․ Սույն օրենքով սահմանված կիբեռանվտանգության ապահովմանն ուղղված միջոցառումներ իրականացնելիս ծառայություն մատուցողները պետական գաղտնիք, ինչպես նաև օրենքով պահպանվող այլ գաղտիք 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, Հայաստանի Հանրապետության վավերացրած 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.
2. **կիբեռանվտանգություն՝** կազմակերպչական, տեխնիկական, ծրագրային միջոցների ամբողջություն, որն ապահովում է համակարգչում, համակարգչային սարքավորումում, թվային հիշողության կրիչներում, տեղեկատվական համակարգում, կրիտիկական տեղեկատվական ենթակառուցվածքում, էլեկտրոնային հաղորդակցության ցանցում մշակվող, պահվող և փոխանցվող տեղեկատվության հասանելիությունը, ամբողջականությունը, իսկությունը, գաղտնիությունը և անհերքելիությունը պատահական կորստից,  չարտոնված մուտքից, օգտագործումից, բացահայտումից, խափանումից, փոփոխումից, ոչնչացումից, հարձակումից, կրկնօրինակումից, ձայնագրումից, տարածումից և այլ անօրինական ներթափանցումից կամ միջամտությունից.
3. **տեղեկատվական համակարգ՝**

ա.էլեկտրոնային հաղորդակցության ցանց,

բ. 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 նշված միջոցներով` նրանց շահագործման, օգտագործման, պաշտպանության և սպասարկման նպատակով.

3) **տեղեկատվական համակարգի անվտանգություն**՝ տեղեկատվական համակարգի կարողություն՝ դիմակայելու ցանկացած իրադրության, որը վտանգում է այդ համակարգում պահպանված, փոխանցված կամ մշակված տվյալների հասանելիությունը, իսկությունը, ամբողջականությունը, գաղտնիությունը և անհերքելիությունը կամ այդ համակարգով առաջարկվող և/կամ այդ համակարգի միջոցով հասանելի դարձվող ծառայությունները․

**4) կրիտիկական տեղեկատվական ենթակառուցվածք՝** ավտոմատացված կառավարման համակարգեր, տեղեկատվական համակարգեր, սարքավորումներ կամ դրանց մի մասը, որոնց խափանումը կամ ոչնչացումը կարող է սպառնալիքներ ստեղծել ազգային անվտանգության, պաշտպանության, տնտեսության, սոցիալական բարեկեցության, բնակչության առողջության, շրջակա միջավայրի համար և անհրաժեշտ են կենսական նշանակության այլ ծառայությունների մատուցման համար.

**5) կենսական նշանակության ծառայություն՝ այնպիսի ծառայություն, որն** առանցքային է բնակչության բնականոն կենսական գործունեության, տնտեսական ակտիվության, հանրային առողջության և անվտանգության կամ շրջակա միջավայրի պահպանման, Հայաստանի Հանրապետության կենսական նշանակության այլ շահերի պաշտպանության համար.

**6) ծառայություն մատուցող**՝ սույն օրենքի 16-րդ հոդվածի 2-րդ մասով սահմանված մեկ կամ մի քանի ոլորտներում կենսական նշանակության ծառայություն մատուցող պետական մարմիններ կամ տեղական ինքնակառավարման մարմիններ կամ անհատ ձեռնարկատերեր կամ իրավաբանական անձինք, ովքեր բավարարում են սույն օրենքի 1-ին հոդվածի 3-րդ և 4-րդ մասերով նշված չափանիշներից առնվազն մեկին,

**7) թվային ենթակառուցվածք՝** սույն օրենքի իմաստով էլեկտրոնային առևտրային հարթակ, առցանց որոնման համակարգ, ամպային հաշվողական համակարգ, էլեկտրոնային թվային ստորագրության ստեղծման կամ ստուգման միջոցներ, էլեկտրոնային հաղորդակցության ծառայություն, հանրային էլեկտրոնային հաղորդակցության ծառայություն, ինտերնետային հասանելիության ծառայություն․

**8) 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,

**9) 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.

**10) 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.

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

**12) կիբեռհարձակում՝** տեղեկատվական համակարգերի աշխատանքը խափանելու, դրանցում մշակվող տվյալներին հասանելիություն ստանալու կամ ամբողջականության վրա բացասաբար ազդելու նպատակով դիտավորությամբ (ուղղորդված) իրականացվող գործողությունների ամբողջություն, որն իրականացվում է առանց տեղեկատվական համակարգը տնօրինողի հետ օրինական կարգով ձեռք բերված պայմանավորվածության.

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

**14) համակարգչային արտակարգ իրավիճակների արձագանքման թիմ** **(CERT)՝** փորձագետների խումբ, որին հանձնարարված է կիբեռմիջադեպերի կառավարումը՝ համակարգումը, վերլուծությունը, կանխումը, արձագանքումը, լուծումը, հետևանքների վերացումը.

**15) վերահսկող մարմին`** ծառայություն մատուցողին լիցենզավորող (նշանակող կամ այլ կերպ գործունեության թույլտվություն տրամադրող) և/կամ վերահսկողություն իրականացնող մարմին և/կամ օրենքով լիազորված այլ մարմին.

**16) կիբեռանվտանգության ապահովման ծառայություն մատուցող՝** իրավաբանական կամ ֆիզիկականանձ, ով մատուցում է կիբեռանվտանգության ապահովման ծառայություններ.

**17) 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.

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

 **19) խոցելիություն՝** տեղեկատվական համակարգի թույլ կողմ կամ թերություն, որն հնարավորություն է ստեղծում կիբեռսպառնալիքի համար:

**Հոդված 4. Կիբեռանվտանգության ապահովման սկզբունքները**

1․ Կիբեռանվտանգության ապահովումն իրականացվում է հետևյալ սկզբունքներով․

1. անհատականության սկզբունք` տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգության ապահովումը կազմակերպում է ծառայություն մատուցողը.
2. համապարփակ պաշտպանության սկզբունք՝ ծառայություն մատուցողը պետք է գնահատի իր կողմից օգտագործվող տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի վրա հնարավոր ռիսկերը, կազմի ռիսկերի գնահատման սանդղակ, որոշի հավանական կիբեռմիջադեպի հետևանքների ծանրությունը, ազդեցության մաշտաբները, տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի անխափան շահագործման կամ հետևանքների վերացման համար անհրաժեշտ ֆինանսական միջոցների չափը և մշակի կիբեռմիջադեպերի կանխարգելման միջոցառումների ծրագիր.
3. բացասական ազդեցությունը նվազագույնի հասցնելու սկզբունք՝ կիբեռմիջադեպի դեպքում ծառայություն մատուցողը պետք է սույն օրենքով և կիբեռանվտանգության ապահովման ներքին կանոնակարգով սահմանված համապատասխան քայլեր և միջոցներ ձեռնարկի կիբեռմիջադեպի արագ սրացումը (ազդեցության մասշտաբների ընդլայնումը), այլ համակարգերում դրա հնարավոր տարածումը կանխելու համար.
4. նվազագույն հասանելիության սկզբունք (least privilege)՝ ծառայություն մատուցողը պետք է ապահովի, որ յուրաքանչյուր ոք կամ որևէ ավտոմատացված գործընթաց տեղեկատվական համակարգին կամ կրիտիկական տեղեկատվական ենթակառուցվածքին կամ դրանում պահպանվող տվյալների ունենա այնքան հասանելիություն, որքան անհրաժեշտ է իր աշխատանքային պարտականությունների կամ գործառույթների պատշաճ իրականացման համար.
5. գաղտնիության սկզբունք՝ տվյալները պետք է հասանելի լինեն միայն այն անձանց համար, ովքեր ունեն համապատասխան մուտքի թույլտվություն․
6. համագործակցության սկզբունքը` կիբեռանվտանգության ապահովման, կիբեռհարձակումների, կիբեռսպառնալիքների կանխման և խափանման, ինչպես նաև կիբեռմիջադեպերի լուծման, հետևանքների վերացման կամ մեղման ընթացքում ծառայություն մատուցողները պետք է ապահովեն բավարար համագործակցություն պետական իրավասու մարմինների և հասարակության հետ, ինչպես նաև միմյանց միջև՝ հաշվի առնելով նաև տեղեկատվական համակարգերի կամ կրիտիկական տեղեկատվական ենթակառուցվածքների միջև փոխադարձ կապն ու փոխգործելիությունը.
7. ամբողջականության սկզբունք՝ ծառայություն մատուցողները պետք է պաշտպանեն տեղեկությունը չարտոնված փոփոխումից կամ ոչնչացումից՝ ապահովելով դրա անխաթարությունը, իսկությունը, հուսալիությունը, ամբողջականությունը և անհերքելիությունը.
8. հասանելիության սկզբունք՝ ծառայություն մատուցողները պետք է ապահովեն տեղեկության ժամանակին և հեշտ հասանելիությունը և օգտագործումը իրավասու անձանց կողմից:

**Գ Լ ՈՒ Խ 2.**

**ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԵՏԱԿԱՆ ԿԱՌԱՎԱՐՈՒՄԸ ԵՎ ԿԱՐԳԱՎՈՐՈՒՄԸ**

**Հոդված 5. Կիբեռանվտանգության ոլորտի պետական կառավարումը**

* + - 1. Կիբեռանվտանգության ոլորտում պետության լիազորություններն իրականացվում են այդ բնագավառում Կառավարության քաղաքականությունը (այսուհետ՝ պետական քաղաքականություն) մշակող և իրականացնող մարմնի, կիբեռանվտանգության ոլորտում քաղաքականության իրականացումն ապահովող լիազորված պետական մարմինների միջոցով։

**Հոդված 6. Կիբեռանվտանգության ոլորտում պետական քաղաքականությունն մշակող և իրականացնող մարմնի լիազորությունները**

1. Կիբեռանվտանգության ոլորտի պետական քաղաքականությունը մշակում և իրականացնում է «Կառավարության կառուցվածքի և գործունեության մասին» օրենքով լիազորված մարմինը (այսուհետ՝ իրավասու մարմին):
2. Իրավասու մարմնի գործառույթներն են՝
3. կիբեռանվտանգության ապահովման ոլորտի ռազմավարության և դրանից բխող միջոցառումների ծրագրի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը,
4. կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկի սահմանման համար համապատասխան մեթոդաբանության մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
5. ծառայություն մատուցողների և կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկը սահմանելու մասին Հայաստանի Հանրապետության կառավարության որոշման նախագծի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը․
6. ռիսկերի գնահատման չափանիշների, կիբեռմիջադեպերի կանխարգելման և լուծման միջոցառումների կազման մեթոդաբանության մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը,
7. ծառայություն մատուցողների կողմից կիբեռանվտանգության ապահովման ներքին կանոնակարգերին ներկայացվող պահանջների մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
8. ծառայություն մատուցողների կողմից կիրառվող տեղեկատվական համակարգերի (այդ թվում՝ կիրառվող տեխեկատվական տեխնոլոգիաների, ծառայությունների, գործընթացների և արտադրանքների մասով՝ հաշվի առնելով սույն օրենքի 16-րդ հոդվածի 2-րդ մասով թվարկված ոլորտների, ենթաոլորտների կամ ծառայության տեսակների առանձնահատկությունները) և կրիտիկական տեղեկատվական ենթակառուցվածքների կիբեռանվտանգության ապահովման նվազագույն պահանջների մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
9. ծառայություն մատուցող չհամարվող իրավաբանական անձի կողմից սույն օրենքից բխող կիբեռանվտանգության ապահովման պարտավորություններ կամավոր ստանձնելու և դրանցից հրաժարվելու դեպքերի սահմանման մասին կարգի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
10. կիբեռմիջադեպերի գնահատման չափանիշների մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը,
11. կիբեռմիջադեպերի վերաբերյալ տեղեկության հավաքագրման և պահպանման կարգի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
12. ծառայություն մատուցողների կողմից կիբեռմիջադեպերի հաշվետությունների ներկայացման կարգի մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
13. կիբեռանվտանգության աուդիտի իրականացման կարգի և կիբեռանվտանգության աուդիտորների որակավորմանը ներկայացվող պահանջների մշակում և ներկայացում Հայաստանի Հանրապետության կառավարության հաստատմանը.
14. ծառայություն մատուցողների կողմից կիբեռմիջադեպերի ծանուցման կարգի հաստատում.
15. լիազոր մարմնի կողմից կիբեռմիջադեպերի գրանցամատյանի վարման կարգի հաստատում.
16. լիազոր մարմնի կողմից Ծառայություն մատուցողների գրանցամատյանի վարման կարգի հաստատում․
17. կիբեռմիջադեպերը կանխելու կամ ազդեցությունը նվազեցնելու նպատակով լիազոր մարմնի կողմից հասցեատերերին իրազեկման կարգի հաստատում.
18. կիբեռանվտանգության ոլորտում վարչական հաշվետվությունների վարման կարգի հաստատում.
19. կիբեռանվտանգության ոլորտում Հայաստանի Հանրապետության ստանձնած միջազգային հանձնառությունների իրականացում, միջազգային համագործակցության ապահովում,
20. միջազգային վարկանիշային զեկույցներում կիբեռանվտանգության ցուցանիշների մասնագիտական վերլուծություն, առաջընթացի ապահովում.
21. միջազգային ստանդարտների հիման վրա կիբեռանվտանգության ապահովման ազգային ստանդարտների մշակում և ներկայացում ստադարտացման ազգային մարմնի հաստատմանը

**Հոդված 7. Կիբեռանվտանգության ոլորտում քաղաքականության իրականացումն ապահովող մարմնի գործառույթները**

1. Սույն օրենքով Կիբեռանվտանգության ոլորտում քաղաքականության իրականացումն ապահովող մարմնի գործառույթները և սույն օրենքի ու դրա հիման վրա ընդունված իրավական ակտերի պահանջների պահպանման նկատմամբ հսկողությունն իրականացում է «Հանրային տեղեկությունների մասին» օրենքով սահմանված լիազոր մարմինը (այսուհետ՝ լիազոր մարմին)։
2. Լիազոր մարմինը՝ որպես միասնական կոնտակտային կետ, կարգավորում և կառավարում է կիբեռմիջադեպերի գրանցման, կանխարգելման և լուծման, հետևանքների վերացմանն ուղղված գործողությունները, իրականացնում սույն օրենքով նախատեսված լիազորություններ:
3. Լիազոր մարմինն իրականացնում է հետևյալ գործառույթները.
4. կիբեռմիջադեպերին արձագանքելը,
5. կիբեռմիջադեպերի արձագանքման առաջնահերթությունների սահմանումը և դասակարգումը.
6. կիբեռմիջադեպերի գրանցումը, կիբեռմիջադեպերի գրանցամատյանի վարումը.
7. կիբեռմիջադեպերի վերլուծությունը.
8. կիբեռմիջադեպերի կանխարգելման միջոցառումների համակարգումը.
9. ծառայություն մատուցողների կողմից ռիսկերի գնահատման մեթոդական աջակցության ցուցաբերում.
10. կիբեռանվտանգության ոլորտում վարչական-վիճակագրական հաշվետվությունների վարում.
11. կիբեռանվտանգության խնդիրների վերաբերյալ հասարակության տարբեր խմբերի շրջանում իրազեկվածության բարձրացում՝ այդ թվում կիբեռհիգիենայի պահպանման մասով, իրազեկման և կրթական ծրագրերի մշակում և իրականացում՝ համագործակցելով իրավասու մարմնի և կրթության ոլորտում պատասխանատու պետական մարմինների հետ.
12. կիբեռվարժանքների տարեկան ծրագրերի մշակում, հաստատում և իրականացում.
13. տեղեկատվական համակարգեր կամ կրիտիկական տեղեկատվական ենթակառուցվածքներ օգտագործող պետական մարմիններում կիբեռվարժանքների իրականացման տարեկան ծրագրով նախատեսված միջոցառումների համակարգում.
14. հնարավոր կիբեռմիջադեպերը կանխելու կամ ազդեցությունը նվազեցնելու նպատակով իրազեկման ապահովում.
15. սույն օրենքի և դրա հիման վրա ընդունված ենթաօրենսդրական իրավական ակտերով սահմանված պահանջների պահպանմանն առնչվող ուղեցույցների մշակում.
16. ծառայություն մատուցողների կողմից սույն օրենքով սահմանված պահանջների պահպանման նկատմամբ հսկողության իրականացում.
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 նախապես համաձայնեցնում է իրավասու մարմնի հետ.
18. իր գործունեության ընթացքում կիբեռմիջադեպի քրեաիրավական բնույթի վերաբերյալ կասկածներ ունենալու կամ բավարար հիմքեր ի հայտ գալու դեպքում իրավապահ մարմիններին հաղորդման ներկայացնում.
19. սույն օրենքով սահմանված կարգով և դեպքերում ծառայություն մատուցողների նկատմամբ վերահսկողություն իրականացում, այլ վերահսկող մարմինների կողմից իրականացվող վերահսկողությանն օժանդակում, այդ թվում՝ պատասխանատվություն կիրառելու միջնորդություն ներկայացնելը.
20. սույն օրենքի պահանջներին կիբեռանվտանգության ապահովման ծառայություն մատուցողների գործունեության համապատասխանության ապահովման նկատմամբ վերահսկողության իրականացում.
21. համագործակցելով այլ անձանց հետ՝ կիբեռանվտանգության մոնիտորինգի իրականացման ազգային օպերատիվ կենտրոնի ստեղծում և կառավարում.
22. ըստ անհրաժեշտության առաջարկությունների ներկայացում իրավասու մարմնին՝ ՀՀ կառավարության որոշմամբ հաստատված կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկում փոփոխություններ կամ լրացումներ կատարելու վերաբերյալ․
23. կիբեռանվտանգության վերաբերյալ հարցերով փորձագիտական աջակցության ցուցաբերում Հայաստանի Հանրապետության կառավարությանը․

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

1. Լիազոր մարմնը վարում է Ծառայություն մատուցողների գրանցամատյան։ Ըստ անհրաժեշտության, բայց ոչ պակաս քան երկու տարին մեկ անգամ լիազոր մարմինը վերանայում և թարմացնում է իր կողմից հաստատված Ծառայություն մատուցողների գրանցամատյանի տվյալները:
2. Սույն օրենքի 16-րդ հոդվածի 2-րդ մասում թվարկված ոլորտներում պետական քաղաքականություն մշակող և իրականացնող մարմինները իրենց իրավասությունների շրջանակում լիազոր մարմնին ցուցաբերում են տեղեկատվական և խորհրդատվական աջակցություն՝ սույն հոդվածի 4-րդ մասում նշված Ծառայություն մատուցողների գրանցամատյանի վարման համար։
3. Լիազոր մարմնի ղեկավարի ներքին իրավական ակտերով սահմանվում են լիազոր մարմնի կողմից կիբեռմիջադեպերի գրանցման, դրանց արձագանքման և լուծման, ներքին աշխատանքային ընթացակարգերը, և գործունեությանն առնչվող այլ կանոններ:

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

Արտակարգ իրավիճակ հայտարարվելու, ռազմական դրության պարագայում դրա տևողության ամբողջ ընթացքում տեղեկատվական համակարգերի և կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման միջոցառումների ձեռնարկման և դրանց վերահսկման գործընթացի պատասխանատու պետական մարմին է հանդիսանում իրավասու մարմինը՝ համագործակցելով ազգային անվտանգության հարցերով լիազորված պետական մարմնի հետ:

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

**ԳԼՈՒԽ 3.**

**ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԿԱՆՈՆՆԵՐ**

**Հոդված 9․ Ծառայություն մատուցողի պարտականությունները**

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

* 1. կիբեռսպառնալիքները հայտնաբերելու և կառավարելու.
	2. կիբեռմիջադեպը կանխելու, հայտնաբերելու, լուծելու.
	3. տեղեկատվական համակարգերի և կրիտիկական 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 իրավական ակտերով սահմանված պահանջների պահպանման մանրամասն նկարագրությունը:

3․ Ծառայություն մատուցողը՝

1. նշանակում է կիբեռանվտանգության մասնագետին կամ մասնագետներին (կիբեռանվտանգության պահանջների պահպանման համար պատասխանատու).
2. իրականացնում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի ռիսկերի գնահատում, կազմում ռիսկերի գնահատման սանդղակ, որոշում հավանական կիբեռմիջադեպի հետևանքների ծանրությունն ու ազդեցության մասշտաբները, մշակում կիբեռմիջադեպի կանխարգելման և լուծման միջոցառումների ծրագիր՝ հիմնվելով Օրենքի 6-րդ հոդվածի 2-րդ մասի 4-րդ կետի համաձայն Հայաստանի Հանրապետության կառավարության կողմից հաստատված ռիսկերի գնահատման չափանիշների, կիբեռմիջադեպերի կանխարգելման և լուծման միջոցառումների կազման մեթոդաբանության հիման վրա և հաստատում այն.
3. ձեռնարկում է կազմակերպչական և տեխնիկական միջոցներ տեղեկատվական համակարգի ռիսկերի կառավարման համար՝ այդ թվում ապահովելով տեղեկատվական համակարգերի ֆիզիկական անվտանգությունը՝ կանխելով համակարգիչներին կամ տեղեկատվություն մշակող, պահպանող կամ փոխանցող այլ սարքավորումներին չթույլատրված ֆիզիկական մուտքը, վնասը կամ միջամտությունը․
4. ապահովում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի վրա գնահատված հնարավոր կիբեռսպառնալիքների փաստաթղթավորումը, անվտանգության կանոնների և միջոցների կիրառման նկարագրությունը․
5. 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 տեխեկատվական տեխնոլոգիաները, ծառայությունները, գործընթացները և արտադրանքները, որոնց վնասումը կամ խափանումը սպառնում է տեղեկատվական համակարգի և կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգությանը)․
6. կիբեռմիջադեպերի մասին սույն օրենքի 11-րդ հոդվածով սահմանված կարգով և դեպքերում ծանուցում է լիազոր մարմնին, ինչպես նաև կիբեռմիջադեպի հետևանքով հնարավոր ազդեցության ենթարկված անձանց կամ հանրությանը․
7. միջոցներ է ձեռնարկում կիբեռմիջադեպի հետևանքները մեղմացնելու, դրա արագ սրացումը (ազդեցության մասշտաբների ընդլայնումը) կանխելու համար՝ անհրաժեշտության դեպքում իրականացնելով տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործման, հասանելիության, մուտքի ամբողջական կամ մասնակի սահմանափակում.
8. վերահսկում է կիբեռմիջադեպին արձագանքելու, լուծելու, հետևանքները մեղմացնելու ուղղությամբ ձեռնարկված գործընթացները, գնահատում է դրանց կիրառման բավարար ու համարժեք լինելը կիբեռմիջադեպի հետևանքների ծանրությանն ու ազդեցության մաշտաբներին, փաստաթղթավորում է արդյունքները ևկազմում է հաշվետվություններ, որոնք ենթակա են պահպանման ոչ պակաս, քան երեք տարի ժամկետով․
9. հավաքագրում է կիբեռմիջադեպերի վերաբերյալ տեղեկությունը և պահպանում այն դրա ստեղծման պահից ոչ պակաս, քան երեք տարի ժամկետով․
10. իր անձնակազմի համար կազմակերպում է կիբեռանվտանգության վերաբերյալ ընդհանուր և հատուկ դասընթացներ, իրականացնում է կիբեռվարժանքներ՝ համագործակցելով լիազոր մարմնի հետ, ապահովում է իր մասնակցությունը լիազոր մարմնի կողմից կազմակերպվող վերապատրաստումներին, կիբեռվարժանքներին և կիբեռանվտանգության ոլորտում կարողությունների զարգացման այլ դասընթացներին.
11. կիբեռմիջադեպի արդյունքում կամ դրա ընթացքում հանցագործության հատկանիշներ ի հայտ գալու դեպքում օրենքով սահմանված կարգով հաղորդում է ներկայացնում իրավասու մարմիններին․

12) 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 մասին տեղեկացվածության բարձրացումը․

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

4. Ծառայություն մատուցողները պարտավոր են ապահովել տեղեկատվական համակարգերում և կրիտիկական տեղեկատվական ենթակառուցվածքներում Հայաստանի Հանրապետության կառավարության կողմից սահմանված կիբեռանվտանգության նվազագույն պահանջները:

5. Այն ծառայություն մատուցողները, ովքեր հանդիսանում են կրիտիկական տեղեկատվական ենթակառուցվածքի շահագործողներ, սույն հոդվածի 4-րդ մասում նշված պահանջներից բացի պարտավոր են բավարարել նաև կիբեռանվտանգության ոլորտում միջազգային ստանդարտին (ինչպիսին է օրինակ՝ ստանդարտացման միջազգային կազմակերպության (ISO) ստանդարտը) և/կամ ազգային ստանդարտներով սահմանված պահանջներին: Միջազգային ստանդարտի նկատմամբ պահանջնեը սահմանում է ՀՀ կառավարությունը։

6. Եթե ծառայություն մատուցողը տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կառավարումը կամ շահագործումը (host of the system) կամ փոխգործելիությունը պատվիրակվում է մեկ այլ անձի, ապա այդ անձի կողմից կիրառված կիբեռանվտանգության ապահովման միջոցների համար պատասխանատու է ծառայություն մատուցողը: Տվյալ անձի վրա նույնպես տարածվում է սույն հոդվածի 4-րդ և 5-րդ մասերով սահմանված պահանջները:

7. Եթե ծառայություն մատուցողը տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովումը պատվիրակում է կիբեռանվտանգության ապահովման ծառայություն մատուցողին, ապա մինչև համապատասխան պայմանագրի կնքումը և դրանից հետո.

1. ծառայություն մատուցողը պարտավոր է գնահատել և կառավարել այն ռիսկերը, որոնք կարող են ազդել ծառայություն մատուցողի տեղեկատվական համակարգում կամ կրիտիկական տեղեկատվական ենթակառուցվածքում պահվող տվյալների գաղտնիությանը, հասանելիությանը կամ ամբողջականությանը,
2. ծառայություն մատուցողը հավաստիանում է, որ կիբեռանվտանգության ապահովման ծառայություն մատուցողի աշխատողների համար ստեղծված են բավարար պայմաններ՝ սույն օրենքի 4-րդ հոդվածով սահմանված սկզբունքների պահպանման համար,
3. ծառայություն մատուցողը լիազոր մարմնի հետ համաձայնեցնում է կիբեռանվտանգության ապահովման ծառայության գնման տեխնիկական առաջադրանքը, որն իր մեջ ներառում է սույն օրենքի 18-րդ հոդվածի 1-ին մասով նախատեսված համապատասխանությունը հավաստող փաստաթուղթ ներկայացնելու պարտադիր պահանջ:

**Հոդված 10. Կիբեռանվտանգության համար պատասխանատու անձը**

1. Ծառայություն մատուցողը պարտավոր է նշանակել տեղեկատվական համակարգի և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովման համար պատասխանատու անձ (կամ անձինք)(կիբեռանվտանգության մասնագետ):
2. Կիբեռանվտանգության մասնագետի պարտականություններն են.
3. մշակում է ծառայություն մատուցողի՝ կիբեռանվտանգության ապահովման ներքին կանոնակարգի նախագիծը և ներկայացում ծառայություն մատուցողի իրավասու պաշտոնատար անձի հաստատմանը.
4. իրականացնում է տեղեկատվական համակարգի և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռսպառնալիքների գնահատում, կազմում կիբեռսպառնալիքների գնահատման սանդղակ, կիբեռմիջադեպերի կանխարգելման միջոցառումների ծրագիր.
5. իրականացնում է տեղեկատվական համակարգի և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքիամենօրյա մշտադիտարկում և գնահատում.
6. իրականացնում է կիբեռմիջադեպերի նույնականացում և արձագանքում.
7. լիազոր մարմնի հետ սույն օրենքով նախատեսված պահանջների պահպանման նպատակով համագործակցության ապահովում.
8. կիբեռմիջադեպի մասին սույն օրենքի 11-րդ հոդվածով սահմանված դեպքերում և կարգով ծանուցել լիազոր մարմնին,
9. համաձայնեցնելով ծառայություն մատուցողի իրավասու պաշտոնատար անձի հետ, անհրաժեշտության դեպքում, իրականացնում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործման, հասանելիության, մուտքի ամբողջական կամ մասնակի սահմանափակում.
10. ծանուցում է մուտքի հնարավորության կամ անհնարինության մասին լիազոր մարմնի հարցմանը սույն օրենքի 13-րդ հոդվածի 7-րդ մասով նախատեսված դեպքում անհապաղ կամ նման հնարավորության բացակայության դեպքում 24 ժամվա ընթացքում ուսումնասիրելուց հետո.
11. լիազոր մարմնին տրամադրում է կիբեռմիջադեպերի և անվտանգության միջոցառումների վերլուծություն և հաշվետվություններ.
12. մասնակցում է լիազոր մարմնի կողմից կազմակերպվող վերապատրաստումներին, կիբեռվարժանքներին և կիբեռանվտանգության ոլորտում կարողությունների զարգացման այլ դասընթացների.
13. կատարում է սույն օրենքով, դրա հիման վրա ընդունված ենթաօրենսդրական իրավական ակտերով, ծառայություն մատուցողի ներքին կանոնակարգով սահմանված այլ պարտականություններ:
14. Կիբեռանվտանգության մասնագետը պետք է հասանելի լինի ցանկացած ժամանակ, ներառյալ աշխատանքային ժամից հետո, ապահովի անհրաժեշտ փոխգործակցություն լիազոր մարմնի հետ ծառայություն մատուցողի դեմ շարունակվող կիբեռմիջադեպը լուծելու կամ հնարավոր այլ կիբեռմիջադեպերը կանխելու, ինչպես նաև դրանց հետևանքների վերացմանն առնչվող գործընթացներում:
15. Եթե շարունակվող կիբեռմիջադեպը սույն օրենքի 11-րդ հոդվածի 2-րդ մասի համաձայն համարվում է էական ազդեցություն ունեցող, ապա լիազոր մարմինը ծառայություն մատուցողի համաձայնությամբ կարող է լիազորվել ժամանակավորապես համակարգելու կիբեռանվտանգության մասնագետի աշխատանքը՝ կիբեռմիջադեպը լուծելու կամ դրա հետևանքները վերացնելու համար:

**Հոդված 11. Կիբեռմիջադեպի մասին ծանուցումը**

1․ Ծառայություն մատուցողը պարտավոր է կիբեռմիջադեպի մասին իրեն հայտնի դառնալուց հետո անհապաղ, բայց ոչ ուշ, քան 24 ժամվա ընթացքում իրավասու մարմնի կողմից սահմանված կարգով լիազոր մարմնին ծանուցել այն կիբեռմիջադեպի մասին,

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

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

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

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 2-րդ 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 պատճառով տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի միջոցով մատուցվող ծառայության դադարեցման դեպքում կարգավորող օրենսդրության կամ ծառայության մատուցման համար կնքված պայմանագրով նախատեսվածառավելագույն թույլատրելի ժամանակահատվածում հնարավոր չէ վերականգնել ծառայության շարունակական, անխափան, անվտանգ մատուցումը.
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 կիբեռմիջադեպի պատճառով կրել կամ կարող են կրել զգալի նյութական կամ ոչ նյութական վնաս:
7. ցանկացած այլ անօրինական միջամտություն (գործողություն), որը ելնելով իր բնույթից, նպատակից, ծագման աղբյուրից, մասշտաբից կամ քանակից կամ դրա կանխարգելման համար պահանջվող ռեսուրսներից և միջոցներից կամ դրանց բավարար համակցությամբ սպառնում է տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի շարունակական և անխափան գործունեությանը կամ անվտանգ օգտագործմանը:

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

4․ Եթե ​​ծառայություն մատուցողի տեղեկատվական համակարգը կամ կրիտիկական տեղեկատվական ենթակառուցվածքը շահագործվում է այլ անձի կողմից կամ տեղակայված է այլ անձի մոտ, ապա ծառայություն մատուցողը պետք է ապահովի, որ այդ անձն իրեն և լիազոր մարմնին սույն հոդվածի 1-ին մասում նշված ժամկետում տեղեկացնի կիբեռմիջադեպերի մասին:

5. Կիբեռմիջադեպի մասին իրեն հայտնի դառնալուց հետո, բայց ոչ ուշ քան 72 ժամվա ընթացքում ծառայություն մատուցողը լիազոր մարմին է ներկայացնում կիբեռմիջադեպի վերաբերյալ թարմացված տեղեկատվություն՝ ներառյալ կիբեռմիջադեպի ծանրության և ունեցած հետևանքների մասով։

6**.** Լիազոր մարմինը կարող է սեփական հայեցողությամբ ծառայություն մատուցողից պահանջել ներկայացնել թարմացված տեղեկատվություն կիբեռմիջադեպի ծանրության, ձեռնարկված միջոցառումների և ունեցած հետևանքների մասին։

7. 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։

8. Ծառայություն մատուցողը պարտավորվում է անհապաղ կամ նման հնարավորության բացակայության դեպքում երկու օրվա ընթացքում ծանուցել կիբեռմիջադեպի հնարավոր ազդեցությանը ենթարկված անձանց կամ հանրությանը, եթե հնարավոր չէ կիբեռմիջադեպից տուժած անձանց անհատապես ծանուցել։: Սույն մասով նախատեսված ծանուցման կարգը սահմանում է իրավասու մարմինը։ Ծառայություն մատուցողը լիազոր մարմնի ցուցումով կիբեռմիջադեպի հետևանքների մասին հանրությանը կամ հնարավոր ազդեցության ենթարկված անձանց չի ծանուցում, եթե ծանուցումը կարող է սպառնալիքներ ստեղծել ազգային անվտանգության, պաշտպանության, տնտեսության համար։

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

10. Սույն հոդվածի 5-րդ մասում նշված տեղեկատվության ներկայացման պահից հետո մեկ ամսվա ընթացքում ծառայություն մատուցողը լիազոր 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) լիազոր մարմնին կարող են ծանուցել կիբեռմիջադեպի, կիբեռհարձակման, կիբեռսպառնալիքի, կամ տեղեկատվական համակարգի և կրիտիկական տեղեկատվական ենթակառուցվածքի խոցելիության մասին։

2․ Սույն հոդվածի 1-ին մասով և 11-րդ հոդվածի 7-րդ մասով նախատեսված ծանուցումները լիազոր մարմինը դիտարկում է սույն օրենքի 6-րդ հոդվածի 2-րդ մասի 11-րդ կետի համաձայն հաստատված կարգով, ընդ որում լիազոր մարմինը պարտավոր է ապահովել ծանուցող անձի գաղտնիությունը: Միևնույն ժամանակ կիբեռմիջադեպերի վերաբերյալ մեկից ավելի ծանուցումներ ներկայացվելու դեպքում լիազոր 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 լիազոր մարմին կամավոր ծանուցում չներկայացնեին, բացառությամբ այն պարտավորությունների, որոնք կապված են հանցագործությունների բացահայտման, նախաքննության և կանխարգելման հետ կապված միջոցառումների իրականացման հետ:

**ԳԼՈՒԽ 4.**

**ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄԸ**

**Հոդված 13. Կիբեռմիջադեպերի հայտնաբերումը, կանխարգելումը և լուծումը**

1. Հայաստանի Հանրապետությունում (ազգային մակարդակում) կիբեռմիջադեպերի հայտնաբերումը, կանխարգելումն ու լուծումը, ինչպես նաև կիբեռմիջադեպերի լուծման ուղղությամբ ծառայություն մատուցողների գործողություների համակարգումը սույն օրենքով սահմանված կարգով ապահովում է լիազոր մարմինը, որի կազմում ձևավորվում է ազգային համակարգչային արտակարգ իրավիճակների արձագանքման թիմը (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. Իր խնդիրները լուծելիս CERT-ը 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/կամ սույն օրենքով սահմանված կարգով։

4.Լիազոր մարմինը կրիտիկական տեղեկատվական ենթակառուցվածք տիրապետող ծառայություն մատուցողների մոտ, որպես կանոն նախապես տեղեկացնելով այդ մասին, կարող է իրականացնել խոցելիության գնահատում և ներթափանցման թեստավորում, որն ուղղված է ստուգելու ծառայություն մատուցողների տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի պաշտպանվածությունը արտաքին ռիսկերից և հնարավոր խոցելիության մասին տեղեկացնել համապատասխան ծառայություն մատուցողին:

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

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

7. CERT-ը կարող է ծառություն մատուցողից պահանջել մուտք դեպի տեղեկատվական համակարգեր կամ կրիտիկական տեղեկատվական ենթակառուցվածքներ, եթե այդպիսի մուտքն անհրաժեշտ է կիբեռմիջադեպին պատշաճ արձագանքելու համար:

8. Լիազոր մարմինը ծառայություն մատուցողների կամ կիբեռանվտանգության ապահովման ծառայություն մատուցողների վերաբերյալ տեղեկություն փոխանցելիս պարտավորվում 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 անհրաժեշտ տեխնիկական և ծրագրային պայմաններ: Այդ տվյալները կարող են հասանելի լինել միայն օրենքով սահմանված կարգով իրավասու մարմինների կամ անձանց համար:

**Հոդված 14. Հսկողության իրականացումը**

1. Ծառայություն մատուցողների կողմից տեղեկատվական համակարգերում և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման միջոցների կիրառման և սույն օրենքով նախատեսված այլ պահանջների պահպանման նկատմամբ հսկողությունն իրականացնում է լիազոր մարմինը:
2. Լիազոր մարմնի կողմից ծառայություն մատուցողի մոտ հսկողությունն իրականացվում է հետևյալ եղանակներով.
3. տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի արտաքին ռիսկերից պաշտպանվածության և հնարավոր խոցելիության գնահատում՝ սույն օրենքի 13-րդ հոդվածի 4-րդ մասով սահմանված կարգով.
4. Հայաստանի Հանրապետության կառավարության կողմից սահմանված կիբեռանվտանգության նվազագույն պահանջների ապահովման համապատասխանության գնահատում.
5. ռիսկերի գնահատման հիման վրա կազմված կիբեռմիջադեպերի կանխարգելման միջոցառումների ծրագրով նախատեսված առանձին միջոցառումների կատարման համապատասխանության գնահատում.
6. որակավորված աուդիտորի կողմից կիբեռանվտանգության աուդիտի արդյունքներով կազմված հաշվետվության պահանջների կատարման համապատասխանության գնահատում.
7. նախօրոք չպլանավորված համապատասխանության գնատում՝ պայմանավորված կիբեռմիջադեպով կամ տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի խոցելիության վերաբերյալ երրորդ անձանցից ստացված տեղեկությամբ կամ ծառայություն մատուցողի կողմից սույն օրենքի պահանջները խախտելու հանգամանքով․
8. Լիազոր մարմինն իր կողմից իրականացվող մշտադիտարկման շրջանակներում կարող է մուտք գործել և սահմանափակել ծառայություն մատուցողի կողմից կիրառվող տեղեկատվական համակարգի և/կամ կրիտիկական տեղեկատվական ենթակառուցվածքի օգտագործումը՝ հետևյալ պայմանների համաժամանակյա առկայության դեպքում.
	1. կիբեռմիջադեպը վտանգի է ենթարկում կամ վնասում է այլ տեղեկատվական համակարգի և/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. լիազոր 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։
9. Սույն հոդվածի 3-րդ մասով նախատեսված միջոցի կիրառության մասին ծառայություն մատուցողը անհապաղ տեղեկացվում է:
10. Սույն հոդվածի 3-րդ մասով նախատեսված միջոցի կիրառության դեպքում կազմվում է հաշվետվություն:
11. Սույն հոդվածի 2-րդ մասով նախատեսված դեպքերում համապատասխանության գնահատում իրականացնելու ընթացքում լիազոր մարմինը կարող է ծառայություն մատուցողից պահանջել անհրաժեշտ տեղեկատվություն, տվյալներ, փաստաթղթեր, որոնք ծառայություն մատուցողը պարտավոր է տրամադրել լիազոր մարմնի ղեկավարի կողմից ներկայացված գրության հիման վրա՝ տվյալ գրությամբ նշված ժամկետում:

7․ Սույն հոդվածի 2-րդ մասով նախատեսված դեպքերում ծառություն մատուցողի մոտ իրականացված համապատասխանության գնահատման արդյունքներով լիազոր մարմինը տալիս է ծառայություն մատուցողի համար պարտադիր կատարման ենթակա ցուցումներ, սահմանում է ժամանակացույց՝ ծառայություն մատուցողի կողմից տրված ցուցումների կատարման կամ թերությունների վերացման նպատակով: Ծառայություն մատուցողը պարտավորվում է սահմանված ժամանակացույցի համաձայն կատարել լիազոր մարմնի տրված ցուցումները կամ վերացնել արձանագրված թերությունները և այդ մասին տեղեկացնել լիազոր մարմնին՝ ներկայացնելով ապացույցներ։

**Հոդված 15. Կիբեռմիջադեպերի գրանցամատյան**

1. Կիբեռմիջադեպերի գրանցամատյանը լիազոր մարմնի կողմից վարվող տվյալների շտեմարան է, որտեղ մուտքագրվում են կիբեռմիջադեպերը նկարագրող տվյալներ՝ կիբեռմիջադեպերը վերլուծելու, դրանք վերացնելու համար ծանուցումներ ուղարկելու, հսկողությանև լիազոր մարմնի՝ սույն օրենքից բխող այլ գործառույթների իրականացման նպատակով։

2. Կիբեռմիջադեպերի գրանցամատյանում ստացվող, վերլուծվող և տրամադրվող տվյալները համարվում են գաղտնիք 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 օրենսդրությամբ: Կիբեռմիջադեպերի գրանցամատյանի տեղեկությունները կարող են օգտագործվել միայն սույն օրենքով սահմանված նպատակներով:

3. Լիազոր մարմնի աշխատողները, 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.**

**ԿՐԻՏԻԿԱԿԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐՈՒՄ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԱՌԱՆՁՆԱՀԱՏԿՈՒԹՅՈՒՆՆԵՐԸ, ԿԵՆՍԱԿԱՆ ՆՇԱՆԱԿՈՒԹՅԱՆ ԾԱՌԱՅՈՒԹՅՈՒՆՆԵՐԸ**

**Հոդված 16. Կրիտիկական տեղեկատվական ենթակառուցվածքները**

1. Կենսական նշանակության ծառայության մատուցման համար կիրառվող կրիտիկական տեղեկատվական ենթակառուցվածքների սահմանման համար մեթոդաբանությունը, կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկն ըստ կիբեռանվտանգության ոլորտում քաղաքականության իրականացումն ապահովող լիազորված պետական մարմինների, հաստատվում է ՀՀ կառավարության կողմից՝ մշակման համար հիմք ընդունելով հետևյալ չափանիշները՝
2. տեղեկատվական համակարգում տեղի ունեցող կիբեռմիջադեպի հնարավոր ազդեցությունը մեկ կամ մի քանի կենսական նշանակության ծառայությունների մատուցման վրա.
3. տեղեկատվական համակարգում տեղի ունեցող կիբեռմիջադեպի տևողությունը և վտանգավորության աստիճանը տնտեսական ակտիվության, շրջակա միջավայրի, բնակչության բնականոն կենսագործունեության ապահովման համար, ազգային անվտանգության կամ բնակչության առողջության վրա.
4. տեղեկատվական համակարգում անսարքության կամ խափանման հետևանքով հնարավոր հետևանքների մաշտաբները (համակարգային էֆեկտ).
5. տեղեկատվական համակարգից օգտվողների թիվը.
6. տեղեկատվական համակարգի տվյալ պահի հաշվեկշռային արժեքը և կիբեռմիջադեպի հետևանքով կրիտիկական տեղեկատվական ենթակառուցվածքի վերականգման կամ նորի ստեղծման համար անհրաժեշտ ֆինանսական ծախսերի չափի գնահատականը:
7. Սույն օրենքի իմաստով կենսական նշանակության ծառայությունները մատուցվում են հետևյալ ոլորտներում՝

1) էներգետիկա, որը ներառում է էլեկտրաէներգետիկական համակարգը, ջերմամատակարարման համակարգերը, գազամատակարարման համակարգը, միջուկային էներգետիկան.

ա) էլեկտրական էներգիայի (հզորության)

նը, ջերմային էներգիայի արտադրությունը կամ էլեկտրական և ջերմային էներգիայի համակցված արտադրությունը.

բ) էլեկտրական էներգիայի հաղորդումը, ջերմային էներգիայի հաղորդումը կամ բնական գազի փոխադրումը.

գ) էլեկտրական էներգիայի բաշխումը, ջերմային էներգիայի բաշխումը կամ բնական գազի բաշխումը.

դ) էլեկտրական էներգիայի մատակարարումը, էլեկտրական էներգիայի երաշխավորված մատակարարումը.

ե) էլեկտրաէներգետիկական համակարգի օպերատորի կամ գազամատակարարման համակարգի օպերատորի ծառայությունը.

զ) էլեկտրաէներգետիկական շուկայի օպերատորի ծառայությունը.

է) Էլեկտրական էներգիայի մեծածախ առևտուրը.

ը) բնական գազի ներկրումը կամ բնական գազի արտահանումը․

2) ջրային համակարգ, որը ներառում է խմելու, ոռոգման, տեխնիկական արդյունաբերական ջրի մատակարարումը, ջրահեռացումը և կեղտաջրերի մաքրումը.

3) հեռահաղորդակցություն (էլեկտրոնային հաղորդակցություն), որը ներառում է հանրային էլեկտրոնային հաղորդակցության ծառայությունը, ինտերնետ հասանելիության ծառայությունը, ամրակցված հեռախոսակապի ծառայությունը, շարժական հեռախոսակապի ծառայությունը,

4) տրանսպորտ, որը ներառում է․

ա․ «Ավիացիայի մասին» Հայաստանի Հանրապետության օրենքով նախատեսված աերոդրոմի շահագործողը, որն ապահովում է միջազգային կանոնավոր առևտրային և (կամ) ներքին կանոնավոր առևտրային փոխադրումներ, Հայաստանի Հանրապետությունում գրանցված օդանավ շահագործողները, լիազորված մարմնի կողմից թույլտվություն ստացած (սերտիֆիկացված) Հայաստանի Հանրապետության օդային տարածքում օդային երթևեկության սպասարկման ծառայություններ մատուցող կազմակերպությունը և անօդաչու թռչող սարքերի ծառայություններ մատուցող կազմակերպությունները,

բ․ երկաթուղային տրանսպորտ, որը ներառում է ընդհանուր օգտագործման երկաթուղային տրանսպորտի ենթակառուցվածքի կառավարիչը, որն ունի երկաթուղային տրանսպորտի գործունեության կազմակերպման լիցենզիա և երկաթուղային տրանսպորտի ենթակառուցվածքն օգտագործում է երկաթուղային տրանսպորտի ծառայություններ մատուցելու նպատակով․

5) փոստային կապ, որը ներառում է փոստային կապի ծառայությունները, սուրհանդակային կապի ծառայությունը,

6) տիեզերական գործունեություն,

7) առողջապահություն, որը ներառում է բժշկական օգնության և սպասարկման ծառայություններ մատուցումը,

8) շրջակա միջավայր,

9) թափոնների կառավարում,

10) արտադրություն,

11) հանրային կառավարում, ներառյալ պետական կառավարման համակարգի մարմինները, Կառավարության կողմից հանրությանը մատուցվող էլեկտրոնային սպասարկման ծառայությունները,

12) թվային ենթակառուցվածքներ,

13) բանկային և ֆինանսական ոլորտ, որը ներառում է հետևյալ անձանց՝ ՀՀ կենտրոնական բանկ, ՀՀ տարածքում գործող բանկեր, ապահովագրական ընկերություններ, վճարահաշվարկային ծառայություններ մատուցող կազմակերպություններ, կենտրոնական դեպոզիտարիա, կարգավորող շուկայի օպերատոր, վարկային բյուրոներ, լեվերիջով գործարքների, այդ թվում՝ ֆորեքս գործարքների հետ կապված ներդրումային և ոչ հիմնական ծառայություններ մատուցող անձինք, ավտոտրանսպորտային միջոցների օգտագործումից բխող պատասխանատվության պարտադիր ապահովագրություն իրականացնող ապահովագրական ընկերությունների բյուրոն, քրաուդֆանդինգի հարթակի օպերատորները:

3. Լիազոր մարմինը սույն հոդվածի 1-ին մասում նշված մեթոդաբանության հիման վրա կարող է առանձին տեղեկատվական համակարգեր, որոնք ներառված չեն սույն հոդվածի 1-ին մասում նշված ցանկում, սահմանել որպես կենսական նշանակության ծառայությունների մատուցման համար կրիտիկական նշանակություն ունեցող՝ ծանուցելով այդ մասին համապատասխան ծառայություն մատուցողին։ Այդ դեպքում Ծառայություն մատուցողը պարտավորվում է բավարարել ՀՀ կառավարության որոշմամբ սահմանված կիբեռանվտանգության նվազագույն պահանջներին (եթե արդեն իսկ տվյալ ծառայություն մատուցողը չի հանդիսանում կրիտիկական տեղեկատվական ենթակառուցվածքի շահագործող՝ բավարարելով օրենքով նախատեսված ավելի խիստ պահանջների)։

4․ Սույն հոդվածի 3-րդ մասում նշված ծանուցումից չորս ամիս անց լիազոր մարմինը կամ ներկայացնում է առաջարկություն սույն հոդվածի 1-ին մասում նշված ցանկում համապատասխան տեղեկատվական համակարգը՝ որպես կրիտիկական տեղեկատվական ենթակառուցվածք ներառելու մասին, կամ ծանուցում է համապատասխան ծառայություն մատուցողին՝ տեղեկացնելով, որ լիազոր մարմնի կողմից որոշված տեղեկատվական համակարգը այլևս չի հանդիսանում կենսական նշանակության ծառայությունների մատուցման համար կրիտիկական նշանակություն ունեցող։

**Հոդված 17. Կրիտիկական տեղեկատվական ենթակառուցվածքներում կիբեռանվտանգության ապահովման առանձնահատկությունները**

1. Կրիտիկական տեղեկատվական ենթակառուցվածքում կիբեռանվտանգության պետական կառավարումը և կարգավորումը իրականացվում է հաշվի առնելով սույն օրենքի 16-րդ հոդվածի 1-ին մասի չափանիշների հիման վրա սահմանված 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 18. Կիբեռանվտանգության ապահովման ծառայություն մատուցողներին ներկայացվող պահանջները**

1. Եթե ծառայություն մատուցողը տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի կիբեռանվտանգության ապահովումը պատվիրակում է կիբեռանվտանգության ապահովման ծառայություն մատուցողին, ապա այդ անձը պետք է ունենա կիբեռանվտանգության ոլորտում միջազգային ստանդարտով կամ ազգային ստանդարտով սահմանված չափանիշներին և պահանջներին համապատասխանությունը հավաստող փաստաթուղթ:
2. Եթե ծառայություն մատուցողը կիբեռանվտանգության ապահովումը պատվիրակում է այլ պետություններում գործունեություն իրականացնող կիբեռանվտանգության ապահովման ծառայություն մատուցողի, ապա նրանց համապատասխանությունը հավաստող փաստաթուղթը լիազոր մարմնի թույլտվությամբ կհամարվի Հայաստանի Հանրապետությունում կիրառելի՝ միջազգային համագործակցության մասին համաձայնագրերի (պայմանագրերի) հիման վրա:
3. Կիբեռանվտանգության ապահովման ծառայություն մատուցողը պարտավոր է սույն օրենքի 19-րդ հոդվածով սահմանված կարգով անցնել կիբեռանվտանգության աուդիտ:

**ԳԼՈՒԽ 7.**

**ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՈՒԴԻՏ**

**Հոդված 19. Կիբեռանվտանգության աուդիտ**

1. Ծառայություն մատուցողը պարտավոր է երկու տարին մեկ անցնել կիբեռանվտանգության աուդիտ և աուդիտի արդյունքներով կազմված հաշվետվությունը այն ստանալուց հետո մեկ ամսվա ընթացքում ներկայացնի լիազոր մարմնին։
2. Ծառայություն մատուցողի կողմից կիրառվող տեղեկատվական համակարգի կամ կրիտիկական տեղեկատվական ենթակառուցվածքի առանձնահատկություններով պայմանավորված ծառայություն մատուցողը կարող է իր ինքնուրույն որոշմամբ սույն հոդվածի 1-ին մասում նշված ժամկետից շուտ անցնել կիբեռանվտանգության աուդիտ:
3. Կիբեռանվտանգության աուդիտի արդյունքում գնահատվում է ծառայության մատուցողի կիբեռանվտանգության ապահովման ներքին կանոնակարգի և դրա կիրարկման համապատասխանությունը սույն օրենքի պահանջներին:
4. Այն դեպքում, երբ լիազոր մարմինն ունի ողջամիտ կասկած, որ ծառայություն մատուցողը պատշաճ չի իրականացրել կիբեռանվտանգության աուդիտ կամ ներկայացված տեղեկությունները կեղծ են, թերի կամ ոչ ճշգրիտ, կարող է ծառայություն մատուցողից պահանջել՝ անցնել կիբեռանվտանգության նոր աուդիտ՝ լիազոր մարմնի կողմից նշանակված աուդիտորի կողմից։
5. Լիազոր մարմինը վարում է կիբեռանվտանգության աուդիտ իրականացնող կազմակերպությունների միասնական գրանցամատյան, որը հրապարակվում է լիազոր մարմնի պաշտոնական կայքէջում։
6. Կիբեռանվտանգության աուդիտ իրականացնող անձը վճարվում է ծառայություն մատուցողի կողմից։

**ԳԼՈՒԽ 8.**

**ՕՐԵՆՔԻ ԵՎ ԴՐԱ ՀԻՄԱՆ ՎՐԱ ԸՆԴՈՒՆՎԱfԾ ԻՐԱՎԱԿԱՆ ԱԿՏԵՐԻ ՊԱՀԱՆՋՆԵՐԻ ԿԱՏԱՐՄԱՆ ՆԿԱՏՄԱՄԲ ՎԵՐԱՀՍԿՈՂՈՒԹՅՈՒՆԸ, ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ**

**Հոդված 20. Վերահսկողության իրականացումը**

1. Ծառայություն մատուցողի նկատմամբ սույն օրենքի և դրա հիման վրա ընդունված իրավական ակտերի պահանջների կատարման նկատմամբ վերահսկողությունն իրականացնում են համապատասխան վերահսկող մարմինները:
2. Ծառայություն մատուցող որևէ տեսակի անձի նկատմամբ վերահսկող մարմին առկա չլինելու կամ վերահսկող մարմնին կիբեռանվտանգության ապահովման ոլորտում վերապահված գործառույթների իրականացման իրավական կարգավորման բացակայության դեպքում ծառայություն մատուցողի նկատմամբ սույն օրենքի և դրա հիման վրա ընդունված իրավական ակտերի պահանջների կատարման նկատմամբ վերահսկողությունն իրականացնում է լիազոր մարմինը՝ կիրառելով Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգիրքով նախատեսված վարչական պատասխանատվության միջոցներ:

**Հոդված 21. Պատասխանատվությունը սույն օրենքի պահանջների խախտման համար**

1. Սույն օրենքի պահանջների խախտումն առաջացնում է օրենքով սահմանված վարչական կամ քրեական պատասխանատվություն:
2. Ծառայություն մատուցողը կամ նրա աշխատողները (ղեկավարները) չեն կարող ենթարկվել գույքային, վարչական պատասխանատվության՝ սույն օրենքից բխող իրենց պարտականությունների պատշաճ կատարման համար: Լիազոր մարմինը կամ նրա աշխատակիցները չեն կարող ենթարկվել գույքային, վարչական պատասխանատվության սույն օրենքով նախատեսված իրենց պարտականությունների պատշաճ կատարման համար:

**ԳԼՈՒԽ 9.**

**ԵԶՐԱՓԱԿԻՉ ՄԱՍ ԵՎ ԱՆՑՈՒՄԱՅԻՆ ԴՐՈՒՅԹՆԵՐ**

**Հոդված 22. Եզրափակիչ մաս և անցումային դրույթներ**

1. Սույն օրենքն ուժի մեջ է մտնում պաշտոնական հրապարակմանը հաջորդող օրվանից, բացառությամբ.
2. սույն օրենքի 8-րդ հոդվածի, որն ուժի մեջ է մտնում նշված հոդվածի 2-րդ մասով սահմանված կարգի հաստատումից հետո,
3. սույն օրենքի 9-րդ հոդվածի 2-րդ մասի, 3-րդ մասի 1-2-րդ, 4-6-րդ կետերի, 4-րդ մասի, որոնք ուժի մեջ են մտնում համապատասխան ենթաօրենսդրական իրավական ակտերի ուժի մեջ մտնելուց հետո,
4. Ծառայություն մատուցողները, ովքեր շահագործում են կրիտիկական տեղեկատվական ենթակառուցվածքներ, օրենքի ուժի մեջ մտնելուց հետո քսանչորսամսյա ժամկետում լիազոր մարմին են ներկայացնում կիբեռանվտանգության ոլորտում միջազգային ստանդարտով կամ ազգային ստանդարտով սահմանված չափանիշներին և պահանջներին համապատասխանությունը հավաստող փաստաթուղթ:
5. Կիբեռանվտանգության ապահովման ծառայություն մատուցողները կիբեռանվտանգության աուդիտ անցնում են կիբեռանվտանգության ոլորտում միջազգային կամ ազգային ստանդարտներով սահմանված համապատասխանություն հավաստող փաստաթուղթ ստանալուց հետո մեկ տարի անց:
6. Սույն օրենքից բխող ենթաօրենսդրական իրավական ակտերն ընդունվում են սույն օրենքն ուժի մեջ մտնելուց հետո՝ տասերկուամսյա ժամկետում, որոնց ուժի մեջ մտնելուց հետո ուժի մեջ են մտնում սույն օրենքի համապատասխան նորմերը:
7. Ծառայություն մատուցողներն իրենց կիբեռանվտանգության ապահովման ներքին կանոնակարգերը ընդունում, իրենց կողմից կիրառվող տեղեկատվական համակարգերում կամ կրիտիկական տեղեկատվական ենթակառուցվածքներում ռիսկերի գնահատումը, կիբեռմիջադեպի կանխարգելման միջոցառումների ծրագրի մշակումն իրականացնում են սույն օրենքի ուժի մեջ մտնելուց հետո՝ տասութամսյա ժամկետում:

**Հայաստանի Հանրապետության
Նախագահ**

2023 թ. ……. … Երևան

ՀՕ-…..-