ՈՉ ՊԱՇՏՈՆԱԿԱՆ

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԵՎ ՏԵՂԵԿԱՏՎԱԿԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ ՀԱՅԵՑԱԿԱՐԳԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ

Ղեկավարվելով 2005 թվականի փոփոխություններով Հայաստանի Հանրապետության Սահմանադրության 56-րդ հոդվածով և հաշվի առնելով Ազգային անվտանգության խորհրդի 2017 թվականի սեպտեմբերի 27-ի նիստի արձանագրությունը՝

ո ր ո շ ու մ է մ.

1. Հաստատել Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության հայեցակարգը՝ համաձայն հավելվածի:

2. Հայաստանի Հանրապետության կառավարությանը՝ մինչև 2018 թվականի մարտի 31-ը ապահովել սույն կարգադրության 1-ին կետում նշված հայեցակարգից բխող ռազմավարության և միջոցառումների ծրագրի ընդունումը:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
Ն Ա Խ Ա Գ Ա Հ Ս. ՍԱՐԳՍՅԱՆ

2017թ. հոկտեմբերի 23
Երևան
ՆԿ- 146 -Ա

Հավելված

ՀՀ Նախագահի
2017թ. հոկտեմբերի 23-ի
ՆԿ- 146 -Ա կարգադրության

ՀԱՅԵՑԱԿԱՐԳ
ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԵՎ ՏԵՂԵԿԱՏՎԱԿԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅԱՆ

I. ՆԵՐԱԾՈՒԹՅՈՒՆ

1. Գլոբալ փոխակերպումների և գիտատեխնիկական առաջընթացի արդյունքում աննախադեպ աճել են տեղեկատվական տիրույթի, այդ թվում՝ տեղեկատվական տեխնոլոգիաների դերն ու նշանակությունը: Թափանցելով հանրային կյանքի և պետության գործունեության բոլոր ոլորտներ՝ տեղեկատվական տեխնոլոգիաները դարձել են քաղաքական, ռազմական, տնտեսական, կրթական, գիտատեխնոլոգիական և մշակութային ոլորտների առանցքային գործոն:

2. Տեղեկատվական տեխնոլոգիաների ներկայիս ծանրակշիռ ազդեցությունը կառավարման բոլոր ոլորտների բնականոն ու արդյունավետ գործունեության վրա ավելի է մեծացնում տեղեկատվական անվտանգության ապահովման հայեցակարգային և նորմատիվ իրավական փաստաթղթերի մշակման ու արդիականացման անհրաժեշտությունը:

3. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության հայեցակարգը (այսուհետ՝ Հայեցակարգ) տեղեկատվական տիրույթում պետության մոտեցումների ամբողջություն է, որը կազմում է պետական քաղաքականության առանցքային մասը և հիմք է Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման ոլորտում պետական քաղաքականության հիմնական ուղղությունների և գերակայությունների մշակման ու իրականացման, նորմատիվ-իրավական բազայի կատարելագործման համար:

4. Հայեցակարգի իրավական հիմքերն են՝ Հայաստանի Հանրապետության Սահմանադրությունը և գործող օրենսդրությունը, ինչպես նաև Հայաստանի Հանրա-

պետության կողմից վավերացված միջազգային պայմանագրերով ստանձնած պարտավորությունները:

II. ՀԱՅԵՑԱԿԱՐԳՈՒՄ ՕԳՏԱԳՈՐԾՎՈՂ ՀԻՄՆԱԿԱՆ ԵԶՐՈՒՅԹՆԵՐԸ

5. Հայեցակարգում օգտագործվում են հետևյալ հիմնական եզրույթները՝

տեղեկություն՝ անձի, առարկայի, փաստի, հանգամանքի, իրադարձության, եղելության, երևույթի վերաբերյալ ստացված և ձևավորված տվյալներ՝ անկախ դրանց ներկայացման և տնօրինման ձևից,

տեղեկատվություն՝ տեղեկություններ կամ հաղորդակցություններ՝ անկախ դրանց փոխանցման և պահպանման ձևից,

տեղեկատվական տիրույթ՝ տեղեկատվական ռեսուրսների, ենթակառուցվածքների և փոխգործակցության միջոցների համախումբ, որոնց միջոցով ստեղծվում, մշակվում, հաղորդվում և (կամ) պահպանվում է տեղեկությունը,

տեղեկատվական ենթակառուցվածք՝ պետության տարածքում, ինչպես նաև նրա իրավազորության ներքո գտնվող, միջազգային իրավունքի նորմերով նրա կողմից վերահսկվող տարածքներում տեղակայված և տեղեկատվության ստեղծմանը, օգտագործմանը, տեղափոխմանը և պահպանմանը մասնակցող անձանց, գործընթացների, տեղեկատվական տեխնոլոգիաների, օբյեկտների, համակարգերի, համացանցային կայքերի ու հեռահաղորդակցության ցանցերի ամբողջություն,

կրիտիկական տեղեկատվական ենթակառուցվածք՝ տեղեկատվության ձևավորման, վերամշակման, փոխանցման, կիրառման և պահպանման տեխնիկական միջոցների ու համակարգերի ամբողջություն, որոնք կենսականորեն կարևոր են պետության և հասարակության համար, և որոնց վնասումը, խափանումը կամ ոչնչացումը վտանգավոր կամ աղետալի հետևանքներ կարող են ունենալ ազգային անվտանգության, պետական կառավարման, հանրային կարգի և առողջության, տնտեսական զարգացման և հասարակության բարեկեցության վրա,

տեղեկատվական անվտանգություն՝ առկա սպառնալիքներից անձի, հասարակության, պետության և նրանց շահերի պաշտպանվածության վիճակը տեղեկատվական տիրույթում,

տեղեկատվական անվտանգության սպառնալիք՝ գործողություններ, գործոններ, անգործություն և (կամ) դրանց ամբողջություն, որոնք ուղղված են տեղեկատվական տիրույթում պետության և հանրության շահերին վնասելուն կամ դրա վտանգի ստեղծմանը,

տեղեկատվական անվտանգության ապահովում՝ տեղեկատվական անվտանգության դեմ ուղղված սպառնալիքների բացահայտմանը, դրանց իրագործման կանխարգելմանը, հակազդմանը, զսպմանը և հետևանքների չեզոքացմանն ուղղված քաղաքական, տնտեսական, իրավական, տեխնիկական և կազմակերպական բնույթի միջոցառումների ամբողջություն,

տեղեկատվական անվտանգության ապահովման սուբյեկտներ՝ պետական և տեղական ինքնակառավարման մարմիններ, լրատվական գործակալություններ, հասարակական կազմակերպություններ, տեղեկատվական տիրույթում գործունեություն իրականացնող այլ ֆիզիկական և իրավաբանական անձինք,

կիբեռտարածություն՝ էլեկտրոնային համակարգերի օգտագործմամբ փոխկապակցված տեղեկատվական ենթակառուցվածքների, անձանց, գործընթացների, տվյալների, տեղեկատվության և տեխնոլոգիաների ամբողջություն,

կիբեռանվտանգություն՝ անվտանգության սկզբունքներ, քաղաքականություն, անվտանգության երաշխիքներ, մեթոդական ուղեցույցներ, ռիսկերի կառավարման մոտեցումներ, գործողություններ, մասնագիտական պատրաստվածություն, ապահովագրման միջոցներ և տեխնոլոգիաներ կամ դրանց ամբողջություն, որոնք կարող են օգտագործվել կիբեռտարածության և դրանից օգտվողների պաշտպանության համար,

կիբեռհանցագործություն՝ տեղեկատվական տեխնոլոգիաների կիրառմամբ կիբեռանվտանգության դեմ ուղղված ցանկացած հակաիրավական գործողություն,

կիբեռհարձակում՝ պետությունների, խմբավորումների կամ կազմակերպությունների, անհատների կողմից տեղեկատվական տեխնոլոգիաների միջոցով իրականացվող ցանկացած վնասակար գործողություն, որը նպատակաուղղված է ներթափանցելու համակարգչային տեղեկատվական համակարգեր, կրիտիկական և ռազմական ենթակառուցվածքների համակարգչային ցանցեր և անհատական համակարգչային սարքեր,

կիբեռահաբեկչություն՝ կիբեռտարածությունում հանցավորության դրսևորումներ, որոնք ուղղված են հասարակության ահաբեկմանը, վախի մթնոլորտի ստեղծմանն ու տարածմանը, ահաբեկչական և ծայրահեղական հայացքների քարոզչությանը, պետության տնտեսության և պետականության քայքայմանը:

III. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՀԻՄՆԱՐԱՐ ԱՐԺԵՔՆԵՐԸ ԵՎ ՍԿԶԲՈՒՆՔՆԵՐԸ

6. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման ոլորտի հիմնարար արժեքները Հայաստանի Հանրապետության ազգային անվտանգության ռազմավարությունից բխող՝ անհատի, հասարակության ու պետու-

թյան գոյության, պաշտպանվածության, անվտանգության, զարգացման և կենսական պահանջմունքների բավարարման տեսանկյունից կարևոր իրողություններ, հանգամանքներ ու երևույթներ են:

7. Հայաստանի Հանրապետության տեղեկատվական անվտանգության հիմնարար արժեքներն են՝

- տեղեկատվական տիրույթում անհատի, հասարակության և պետության շահերի հավասարակշռումն ու պաշտպանվածությունը, պետության և անհատի հանդեպ հավասար վերաբերմունքը,
- տեղեկատվական տիրույթում բոլոր սուբյեկտների միջև տեղեկատվական փոխգործակցության երաշխավորումը, հանրային իրազեկվածության և տեղեկատվության թափանցիկության ապահովումը,
- միջազգային տեղեկատվական տիրույթում Հայաստանի Հանրապետության տեղեկատվական տիրույթի լիարժեք ներգրավվածությունը և արդյունավետ համագործակցությունը:

8. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման սկզբունքները Հայաստանի Հանրապետության տեղեկատվական անվտանգության արժեքների ապահովմանն ուղղված քաղաքականության հիմքերն են:

9. Հայաստանի Հանրապետության տեղեկատվական անվտանգության հիմնարար սկզբունքներն են՝

- Հայաստանի Հանրապետության կենսագործունեության բոլոր ոլորտներում տեղեկատվական տեխնոլոգիաների կիրառման համար նպաստավոր պայմանների ապահովումը,
- տեղեկատվական տիրույթում սպառնալիքների և մարտահրավերների համակարգված չեզոքացումը, դրանց օպերատիվ, հասցեական ու համարժեք արձագանքումը,
- տեղեկատվական տիրույթում բոլոր սուբյեկտների անհատական տվյալների պաշտպանությունը,
- Հայաստանի Հանրապետության Սահմանադրությամբ, գործող օրենսդրությամբ և Հայաստանի Հանրապետության կողմից վավերացված միջազգային պայմանագրերով ամրագրված տեղեկատվական անվտանգության ապահովման համընդհանուր մոտեցումների պահպանումը:

IV. ՊԵՏՈՒԹՅԱՆ, ՀԱՍԱՐԱԿՈՒԹՅԱՆ ԵՎ ԱՆՀԱՏԻ ՇԱՀԵՐԸ ՏԵՂԵԿԱՏՎԱԿԱՆ ՏԻՐՈՒՅԹՈՒՄ

10. Տեղեկատվական տիրույթում Հայաստանի Հանրապետության շահը անհատի, հասարակության և պետության պաշտպանվածության ու տեղեկատվության փոխգործակցության ապահովումն է:

11. Տեղեկատվական տիրույթում անհատի, հասարակության ու պետության հիմնական շահերն են՝

- տեղեկատվական փոխգործակցության ապահովումը,
- տեղեկատվական տեխնոլոգիաների կիրառմամբ պետության տնտեսական, սոցիալական և մշակութային կայուն զարգացման խթանումը,
- անձնական տվյալների պաշտպանությունը,
- բազմակողմանի միջազգային համագործակցության զարգացումը,
- միջազգային տեղեկատվական տիրույթում Հայաստանի Հանրապետությանն առնչվող ամբողջական և ճշգրիտ տեղեկատվության ներկայացումը,
- Հայաստան-Արցախ-սփյուռք տեղեկատվական կապի ապահովումը:

V. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՈԼՈՐՏՈՒՄ ԱՌԿԱ ԻՐԱՎԻՃԱԿԸ

12. Վերջին տարիներին, միջազգային ասպարեզում ընթացող գործընթացներով պայմանավորված, պետություններն ավելի մեծ և առաջնային ուշադրություն են դարձնում տեղեկատվական անվտանգության ապահովմանը, օրենսդրական կարգավորումների ներդաշնակեցմանը, այդ ոլորտում հնարավոր սպառնալիքների և մարտահրավերների հակազդմանը, ինչպես նաև տեղեկատվական իրավահարաբերությունների կարգավորմանը:

13. 2009 թվականի հուլիսի 25-ին Հայաստանի Հանրապետության Նախագահի կարգադրությամբ հաստատվել է Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգը: Ընդունվել են նաև էլեկտրոնային հասարակության ձևավորմանը, կիբեռահաբեկչության դեմ պայքարին, կիբեռանվտանգության ապահովմանը, անձնական տվյալների պաշտպանությանը և տեղեկատվական անվտանգության ապահովմանն առնչվող հայեցակարգային, ռազմավարական և այլ իրավական փաստաթղթեր:

14. Հայաստանի Հանրապետությունը տեղեկատվական անվտանգության ապահովման ոլորտում վավերացրել է պայմանագրեր միջազգային կազմակերպությունների և առանձին պետությունների հետ, իրականացնում է համատեղ ծրագրեր միջպետական, ինչպես նաև ԱՊՀ-ի, ՀԱՊԿ-ի, ԵՄ-ի, ԵԽ-ի, ՆԱՏՕ-ի հետ համագործակցության շրջանակներում:

15. Հայաստանի Հանրապետության կողմից տեղեկատվական անվտանգության ապահովման ոլորտում իրականացված միջոցառումները լիարժեք չեն կան-

խարգելել և չեզոքացրել տեղեկատվական անվտանգության նոր սպառնալիքները և մարտահրավերները:

16. Հայաստանի Հանրապետությունում՝

- դեռևս լիարժեք կարգավորված չեն և իրավական կարգավորման կարիք ունեն տեղեկատվության ստեղծման ու տարածման, տեղեկատվական տեխնոլոգիաների կիրառման, տեղեկատվական համակարգերի ստեղծման և շահագործման, ինչպես նաև տեղեկատվության պաշտպանության հետ կապված հարաբերությունները,
- հստակեցման կարիք ունեն պետական և մասնավոր հատվածներում տեղեկատվության ձևավորմանն ու օգտագործմանը վերաբերող փոխհարաբերությունները,
- պատշաճ սահմանված չեն տեղեկատվության դասակարգումը, տեղեկատվական տեխնոլոգիաների և տեղեկատվության պաշտպանության կառավարման շրջանակները,
- ամրագրման կարիք ունեն միջազգային համագործակցության և փոխօգնության ապահովմանն ուղղված իրավակարգավորումները և դրանց իրականացման հստակ միջոցները:

VI. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՍՊԱՌՆԱԼԻՔՆԵՐԸ ԵՎ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ

17. Տեղեկատվական տեխնոլոգիաների լայն կիրառումը հանրային կենսագործունեության գրեթե բոլոր ոլորտներում առաջ է բերել տեղեկատվական անվտանգության նոր սպառնալիքներ և մարտահրավերներ:

18. Հայաստանի Հանրապետության տեղեկատվական անվտանգության սպառնալիքներն են՝

- պետությունների, ահաբեկչական կազմակերպությունների, հանցավոր խմբավորումների և անհատների կողմից Հայաստանի Հանրապետության տարածքում գտնվող տեղեկատվական ռեսուրսների նկատմամբ կիբեռհարձակումները,
- տեղեկություններ փնտրելու, ստանալու և տարածելու ազատության, մասնավոր և ընտանեկան կյանքի, պատվի ու բարի համբավի անձեռնմխելիության, հաղորդակցության ազատության և գաղտնիության, անձնական տվյալների պաշտպանության դեմ կատարվող ոտնձգությունները,
- անհատական, խմբային և հանրային գիտակցության վրա ներազդեցության միջոցների կիրառմամբ տեղեկատվական ապակողմնորոշումը,

- կիբեռհարձակումների համար տարբեր սուբյեկտների կողմից Հայաստանի Հանրապետության տեղեկատվական տիրույթի օգտագործումը,
- անհատների, կազմակերպությունների և պետությունների կողմից կրիտիկական տեղեկատվական ենթակառուցվածքների վրա կիբեռհարձակումները,
- ներքին և արտաքին լսարանների իրազեկմանն ուղղված զանգվածային լրատվության միջոցների գործունեության խոչընդոտումը և (կամ) արգելափակումը,
- օտարերկրյա տեղեկատվական դաշտից հանրային կենսագործունեության ոլորտների կախվածությունը և ներքին տեղեկատվական տիրույթից ազգային տեղեկատվական գործակալությունների ու զանգվածային լրատվության միջոցների դուրսմղումը,
- չարտոնագրված և չհավաստագրված տեղեկատվական համակարգերի, տեղեկատվության պաշտպանության միջոցների, հեռահաղորդակցության և ծրագրային ապահովման միջոցների օգտագործումը,
- մտավոր սեփականության իրավունքների խախտումները,
- այլընտրանքային կապ չունենալու պայմաններում անհաղթահարելի ուժի հետևանքով կամ դիտավորությամբ հեռահաղորդակցական ցանցերի ֆիզիկական խափանումը և (կամ) ընդհատումը,
- պետական կառույցների, մասնավոր հատվածի և անհատների դեմ ուղղված՝ օտարերկրյա պետությունների, կազմակերպությունների ու անհատների կողմից իրականացվող, ֆինանսավորվող և հանրային տեղեկատվական տիրույթի կիրառմամբ կիբեռհարձակումները,
- տեղեկատվական տեխնոլոգիաների կիրառմամբ ահաբեկչական և ծայրահեղական գործունեության իրականացումը, ահաբեկչական կազմակերպությունների կողմից հանրության շրջանում ծայրահեղական գաղափարների և ահաբեկչական գործողությունների իրականացման քարոզումը:

19. Հայաստանի Հանրապետությունում տեղեկատվական անվտանգության մարտահրավերներն են՝

- տեղեկատվական տիրույթում միջազգային համագործակցության ոչ բավարար մակարդակը,
- տեղեկատվական տիրույթում ոչ բավարար համակարգված պետական քաղաքականությունը,
- տեղեկատվական տիրույթում հարաբերությունների համապարփակ կարգավորմանն ուղղված իրավանորմատիվային բազայի բացակայությունը,
- տեղեկատվական ռեսուրսների և ենթակառուցվածքների անվտանգության ապահովման ցածր մակարդակը,

- տեղեկատվական տիրույթում պետություն-մասնավոր հատված փոխգործակցության արդյունավետության ոչ բավարար մակարդակը,
- տեղեկատվական անվտանգության ապահովման ոլորտի համակարգումն ապահովող հավաստագրված մարմինների, այդ թվում՝ համակարգչային պատահարներին արձագանքման թիմերի ոչ արդյունավետ աշխատանքը,
- տեղեկատվական անվտանգության ապահովման ոլորտի մասնագետների պատրաստման և վերապատրաստման ոչ բավարար մակարդակը, մտավոր ներուժի արտահոսքը,
- տեղեկատվական անվտանգության ոլորտի միջազգային փորձի և ստանդարտների ներդրման և կիրառման պակասը,
- արտասահմանյան արտադրության տեղեկատվական տեխնոլոգիաների, սարքավորումների ու ծրագրային ապահովման միջոցների լայնածավալ կիրառումը,
- հանրային իրազեկվածության ցածր մակարդակը:

VII. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՆՊԱՏԱԿՆԵՐԸ ԵՎ ԽՆԴԻՐՆԵՐԸ

20. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման նպատակներն են՝

- արտաքին և ներքին տեղեկատվական տիրույթներում Հայաստանի Հանրապետության անկախության, սահմանադրական կարգի ու ինքնիշխանության անխախտելիությունն ու պաշտպանվածությունը,
- տեղեկատվական տիրույթում անհատի հիմնական իրավունքների ու ազատությունների ապահովումն ու պաշտպանությունը,
- արտաքին և ներքին տեղեկատվական հարթակներում Հայաստանի Հանրապետության պետական քաղաքականության վերաբերյալ ամբողջական և ճշգրիտ իրազեկումը,
- Հայաստանի Հանրապետության հեղինակության պաշտպանվածությունը,
- միջազգային տեղեկատվական տիրույթում Հայաստանի Հանրապետության լիարժեք ներգրավվածությունը, բազմակողմ ու արդյունավետ համագործակցությունը,
- Հայաստան-Արցախ-սփյուռք տեղեկատվական փոխգործակցության արդյունավետության բարձրացումը,
- հայկական պատմամշակութային արժեքների և գիտական ժառանգության պաշտպանվածությունն ու զարգացումը, հայապահպանությունը,

- տեղեկատվական տիրույթում լիցենզավորված ծրագրերի և (կամ) բաց կոդով ծրագրային ապահովումների ձեռքբերումն ու կիրառումը:

21. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման խնդիրներն են՝

- տեղեկատվական անվտանգության ապահովման ոլորտում միասնական քաղաքականության ուղենիշների սահմանումը,
- կրիտիկական տեղեկատվական ենթակառուցվածքների դասակարգումը և օբյեկտների անվանացանկի (ռեեստրի) ստեղծումը,
- Հայաստանի Հանրապետության կրիտիկական տեղեկատվական ենթակառուցվածքների անվտանգության ապահովման մեխանիզմների կատարելագործումը,
- պետական և տեղական ինքնակառավարման մարմինների ու կազմակերպությունների միջև տեղեկատվական համակարգերի էլեկտրոնային փոխկապակցման և դրանցում ներառված տվյալների փոխանակման անվտանգության ապահովումը,
- տեղեկատվական անվտանգության ապահովման ոլորտում ներգրավված սուբյեկտների պատասխանատվության բաշխումը,
- տեղեկատվական անվտանգության միջազգային ստանդարտների և հավաստագրման համակարգի ներդրումը, ազգային ստանդարտների մշակումը և կիրարկումը,
- տեղեկատվական սպառնալիքների և մարտահրավերների մշտադիտարկման, վերլուծության, գնահատման համալիր գործիքակազմի կատարելագործումը,
- տեղեկատվական անվտանգության ոլորտի սպառնալիքների և մարտահրավերների վերաբերյալ հանրային իրազեկման ապահովումը,
- տեղեկատվական անվտանգության ապահովման ոլորտում համակարգչային պատահարներին արձագանքման խմբերի ստեղծումը և զարգացումը,
- տեղեկատվական անվտանգության ապահովման ոլորտում անհրաժեշտ մասնագիտական որակյալ ներուժի ձևավորման համար անհրաժեշտ ծրագրերի մշակումը և ներդրումը,
- տեղեկատվական անվտանգության ապահովման ոլորտում մտավոր սեփականության պաշտպանության համակարգի կատարելագործումը,
- սոցիալական, ռասայական, ազգային և կրոնական ատելության հրահրմանը նպաստող քարոզչական գործունեության կանխարգելումը և հակազդումը,
- տեղեկատվական տիրույթում բոլոր սուբյեկտների միջև տեղեկատվական հոսքերի փոխանակման արդյունավետության բարձրացումը,

- տեղեկատվական տիրույթում հայալեզու տեղեկատվության զարգացումը և համացանցում դրա տարածմանն օժանդակությունը,
- տեղեկատվական անվտանգության ապահովման ոլորտում գիտահետազոտական աշխատանքների և փորձարարական աշխատանքների իրականացումն ու կիրառումը, գիտակրթական կարողությունների զարգացումը,
- պետական կառավարման մարմիններում տեղեկատվական տեխնոլոգիաների ենթակառուցվածքների, դրանց պաշտպանության համակարգերի ներդրման և զարգացման համար անհրաժեշտ ռեսուրսների ապահովումը,
- կիբեռհանցագործությունների ու կիբեռահաբեկչության դեմ պայքարի բնագավառում միջազգային համագործակցության արդյունավետության բարձրացումը,
- տեղեկատվական անվտանգության ապահովման նպատակով միջազգային և տարածաշրջանային համագործակցությունը։

VIII. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ՏԵՂԵԿԱՏՎԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄԸ

22. Կիբեռանվտանգության և տեղեկատվական ենթակառուցվածքների անվտանգության ապահովման համար անհրաժեշտ է ստեղծել իրավական, կազմակերպական և տեխնիկական միջոցներ, որոնք ուղղված կլինեն նվազեցնելու կիբեռհարձակումների հնարավորությունները, կանխատեսելու կիբեռհարձակումների հնարավոր օբյեկտները և հնարավոր վնասի չափը, բարձրացնելու տեղեկատվական տեխնոլոգիաներով մշակվող և պահպանվող, հեռահաղորդակցական ցանցերով փոխանցվող և ստացվող էլեկտրոնային տեղեկատվության պաշտպանվածության և անվտանգության ընդհանուր մակարդակը:

23. Տեղեկատվական ենթակառուցվածքներում շրջանառվող էլեկտրոնային տեղեկատվության արտահոսքը կամ կորզումը հնարավորինս բացառելու նպատակով անհրաժեշտ է՝

- սահմանել տեղեկատվության անվտանգության ապահովման մակարդակի համապատասխան պահանջները և դրանց կատարման մշտադիտարկման ու վերահսկման իրավական կարգավորումը, կազմակերպական և տեխնիկական մեխանիզմները,
- սահմանել էլեկտրոնային տեղեկատվության, տեղեկատվական տեխնոլոգիաների և տեղեկատվության պաշտպանության կառավարման շրջանակները,
- կանոնակարգել էլեկտրոնային տեղեկատվության ստեղծման, մշակման, պահպանման, տրամադրման, տարածման և պաշտպանության, տեղեկատվական

համակարգերի ստեղծման և շահագործման հետ կապված հարաբերությունները:

24. Կիբեռանվտանգության և տեղեկատվական ենթակառուցվածքների անվտանգության ապահովման համար առաջնային կարևորություն ունեն կրիտիկական տեղեկատվական ենթակառուցվածքների սահմանումը և դասակարգումը, ռեեստրի ստեղծումը, ինչպես նաև պետության և կրիտիկական տեղեկատվական ենթակառուցվածքների տնօրինողների միջև փոխհարաբերությունները սահմանող իրավական ակտի մշակումը:

IX. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՈԼՈՐՏՈՒՄ ՊԵՏՈՒԹՅՈՒՆ-ՄԱՍՆԱՎՈՐ ՀԱՏՎԱԾ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅՈՒՆԸ

25. Հայաստանի Հանրապետությունը հետամուտ է պետության և մասնավոր հատվածի միջև կառուցողական համագործակցության զարգացմանն ուղղված մեխանիզմների մշակմանն ու կիրառմանը:

Տեղեկատվական անվտանգության ապահովման ոլորտում պետություն-մասնավոր հատվածի միջև համագործակցության ամրապնդմանը նպաստելու են՝

- կողմերի մասնակցությամբ համատեղ միջոցառումների անցկացումը,
- մասնավոր հատվածի կողմից տեղեկատվական անվտանգության միջազգային և ազգային ստանդարտների ներդրման մեխանիզմների մշակումը,
- պետության և մասնավոր հատվածի միջև փոխգործակցության համար նպաստավոր, բազմակողմանի, բազմաբնույթ պայմանների ստեղծումը:

X. ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԿԱԶՄԱԿԵՐՊԱԻՐԱՎԱԿԱՆ ՀԻՄՔԵՐԸ

26. Տեղեկատվական անվտանգության ապահովման համակարգի կազմակերպաիրավական հիմքերի հիմնական բաղադրիչներն են՝

- Հայաստանի Հանրապետության օրենսդիր, գործադիր, դատական իշխանության և տեղական ինքնակառավարման մարմինները,
- հասարակական միավորումները,
- Հայաստանի Հանրապետության տեղեկատվական անվտանգության խնդիրների լուծմանը ներգրավված իրավաբանական և ֆիզիկական անձինք:

27. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման կազմակերպաիրավական միջոցառումները պետք է նախատեսեն՝

- տեղեկատվության արտահոսքի, կորստի և կեղծման կանխում,

- տեղեկատվական համակարգեր անօրինական միջամտության կանխում,
- տեղեկատվական համակարգերում անձնական տվյալների պաշտպանություն,
- տեղեկատվական անվտանգության ապահովման ոլորտի կադրերի պատրաստում և վերապատրաստում,
- կրիտիկական տեղեկատվական ենթակառուցվածքների պաշտպանության, այդ թվում՝ կրիպտոգրաֆիկական միջոցների ստեղծում և կիրառում:

XI. ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՈԼՈՐՏՈՒՄ ՄԻՋԱԶԳԱՅԻՆ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅՈՒՆԸ

28. Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման ոլորտում միջազգային համագործակցությունն ընդգրկում է՝

- կիբեռհանցագործություններին և տեղեկատվական տեխնոլոգիաներին առնչվող հանցագործությունների դեմ պայքարը,
- ռազմավարությունների, զարգացման ծրագրերի և ընթացակարգերի մշակումը,
- տեխնիկատեխնոլոգիական մշակումներն ու արտադրության կազմակերպումը,
- գիտահետազոտական աշխատանքները,
- մասնագիտական կրթական ծրագրերի իրականացումը, փորձի փոխանակումը:

Միջազգային համագործակցության հիմնական ուղղություններն են՝

- միջազգային տեղեկատվական համակարգերում, հեռահաղորդակցային ցանցերում և կապուղիներում անդրսահմանային կազմակերպված հանցավորության, միջազգային ահաբեկչության, զենքի անօրինական վաճառքի և թմրանյութերի տարածման, ինչպես նաև մարդկանց առևտրի դեմ պայքար տանող միջազգային իրավապահ կազմակերպությունների պաշտոնական տեղեկատվության չարտոնված հասանելիության կանխարգելումը,
- գործընկեր երկրների և կազմակերպությունների հետ դաշնակցային շահերի հիմքով և պայմանագրային պարտավորություններով սահմանված տեղեկատվական փոխգործակցության ապահովումը,
- միջազգային տեղեկատվական փոխանակման, այդ թվում՝ տեղական հեռահաղորդակցային ցանցերով և կապուղիներով տեղեկատվության փոխանցման անվտանգության ապահովումը,
- կիբեռհանցագործությունների կանխարգելման, ինչպես նաև տեղեկատվական անվտանգության ապահովման ուղղությամբ այլ երկրների իրավապահ մարմինների հետ համագործակցության համակարգումը,

- տեղեկատվության և տեղեկատվության պաշտպանության միջոցների ստանդարտացման և հավաստագրման ոլորտում միջազգային գործընթացներին Հայաստանի Հանրապետության ակտիվ մասնակցության ապահովումը:

XII. ՀԱՅԵՑԱԿԱՐԳԻ ԴՐՈՒՅԹՆԵՐԻՑ ԲԽՈՂ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆԸ, ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ԾՐԱԳԻՐԸ ԵՎ ՄՇՏԱԴԻՏԱՐԿՄԱՆ ԿԱԶՄԱԿԵՐՊՈՒՄԸ

29. Հայեցակարգի դրույթների հիման վրա կմշակվեն Հայաստանի Հանրապետության տեղեկատվական անվտանգության ռազմավարությունը և դրանից բխող միջոցառումների ծրագիրը, որոնցով կսահմանվեն տեղեկատվական անվտանգության ապահովման ուղղությամբ իրականացվելիք միջոցառումները, դրանց իրականացման ժամկետները, պատասխանատուները և ֆինանսավորման աղբյուրները:

30. Հայեցակարգի, դրանից բխող ռազմավարության և միջոցառումների ծրագրի կատարման ընթացքի նկատմամբ կանցկացվեն մշտադիտարկումներ, որոնց արդյունքները թույլ կտան գնահատել իրականացված միջոցառումների արդյունավետությունը ու հիմք կհանդիսանան համակարգի հետագա կատարելագործման և արդիականացման համար:

31. Հայեցակարգի դրույթներից բխող ռազմավարությունների, ծրագրերի ու միջոցառումների մշակման և իրականացման արդյունավետությունն ապահովելու համար կարող է ստեղծվել միջգերատեսչական հանձնաժողով:

XIII. ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

32. Հայեցակարգի ընդունման արդյունքում կապահովվեն Հայաստանի Հանրապետությունում տեղեկատվական անվտանգության ապահովման ոլորտում առկա սպառնալիքներին և մարտահրավերներին դիմակայելու, դրանք կանխարգելելու և հաղթահարելու համար անհրաժեշտ կառուցակարգերը, տեղեկատվական տիրույթի զարգացման, պետություն-մասնավոր հատվածի, ինչպես նաև միջազգային համագործակցության անհրաժեշտ մոտեցումները և մեխանիզմները:

ՀՀ ՆԱԽԱԳԱՀԻ ԱՇԽԱՏԱԿԱԶՄԻ
Ղ Ե Կ Ա Վ Ա Ր Ա. ԳԵՎՈՐԳՅԱՆ