ՀՀ կառավարության «Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ

ՆԱԽԱԳԻԾ

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԿԱՌԱՎԱՐՈՒԹՅՈՒՆ

ՈՐՈՇՈՒՄ

-Ն

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ

Հիմք ընդունելով Հայաստանի Հանրապետության Նախագահի 2017 թվականի հոկտեմբերի 23-ի «Հայաստանի Հանրապետության տեղեկատվական անվտանգության և տեղեկատվական քաղաքականության հայեցակարգը հաստատելու մասին» ՆԿ-146-Ա կարգադրության 2-րդ և Հայաստանի Հանրապետության կառավարության 2017 թվականի հունվարի 12-ի N122-Ն որոշման 1-ին հավելվածի 16-րդ կետերը՝ **Հայաստանի Հանրապետության կառավարությունը *որոշում է.***

1. Հաստատել Կիբեռանվտանգության ռազմավարությունը՝ համաձայն 1-ին հավելվածի,

2. Հաստատել Կիբեռանվտանգության ռազմավարությունից բխող միջոցառումների ժամանակացույցը՝ համաձայն 2-րդ հավելվածի:

Հավելված N 1

Հայաստանի Հանրապետության կառավարության

2017 թ. N որոշման

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆ

I. ՆԵՐԱԾՈՒԹՅՈՒՆ

1. Տեղեկատվական հասարակության զարգացմանը զուգահեռ, ինչպես աշխարհում, այնպես էլ Հայաստանում ակտիվ գործընթացներ են ծավալվում

տեղեկատվական համակարգերի և հեռահաղորդակցական ցանցերի զարգացման ուղղությամբ: Տեղեկատվական համակարգերը, տեղեկատվական ծառայությունները, էլեկտրոնային հաղորդակցության ցանցերը լայն տարածում են ստանում հասարակության շրջանում: Պետական մարմիններում և կրիտիկական տեղեկատվական ենթակառուցվածքներում ավելի լայն կիրառություն են ստանում տեղեկատվական և հեռահաղորդակցական համակարգերի ստեղծումն ու շահագործումը, որոնց միջոցով հավաքվում և մշակվում են օրենքով պաշտպանության ենթակա ինչպես հանրամատչելի, այնպես էլ սահմանափակ հասանելիություն ունեցող էլեկտրոնային տվյալներ:

2. Տեղեկատվական հեռահաղորդակցական ցանցերի միջոցով արտադրական գործընթացների (պրոցեսների) ավտոմատ կառավարման համակարգերը լայն կիրառում են ստանում նաև բանկային ու ֆինանսական, էներգառեսուրսների, տրանսպորտի, ջրամատակարարման, արդյունաբերության և հեռահաղորդակցության ոլորտների ենթակառուցվածքներում, որոնց գործունեությունը ուղղակի կախվածություն է ձեռք բերում այդ համակարգերի աշխատանքից: Դրանց անվտանգության ապահովումը և վստահելիությունը առանցքային են տնտեսության և պետության այլ բնագավառների կենսագործունեության համար:

3. Տեղեկատվական տեխնոլոգիաների զարգացմանը զուգահեռ՝ դրական միտումների հետ մեկտեղ, առաջ են գալիս նոր մարտահրավերներ, որոնք պայմանավորված են կիբեռպատահարների ծավալների աճի, ՀՀ տեղեկատվական համակարգերի վրա դրանց ազդեցության, կարևոր տեղեկատվական ենթակառուցվածքների, տեղեկատվական համակարգերի, էլեկտրոնային ծառայությունների վրա հակառակորդի հավանական կիբեռհարձակումների՝ դրանք շարքից հանելու, բնականոն աշխատանքը խաթարելու և/կամ հասանելիությունը էապես նվազեցնելու ուղղությամբ:

4. Կիբեռանվտանգության ռազմավարությունը (այսուհետև՝ Ռազմավարություն) Հայաստանի Հանրապետության կիբեռանվտանգության ոլորտում պետության մոտեցումների ամբողջություն է, որը հիմք է հանդիսանում կիբեռանվտանգության ոլորտում պետական քաղաքականության հիմնական ուղղությունների և սկզբունքների մշակման ու իրականացման, իրավա-նորմատիվային բազայի կատարելագործման և օգտվողների կիբեռանվտանգության մակարդակի բարձրացման համար:

5. Սույն հայեցակարգում օգտագործվող հասկացությունները սահմանված են Հայաստանի Հանրապետության Նախագահի «Հայաստանի Հանրապետության տեղեկատվական անվտանգության և տեղեկատվական քաղաքականության հայեցակարգը հաստատելու մասին» ՆԿ-146-Ա կարգադրությունում:

II. ՌԱԶՄԱՎԱՐՈՒԹՅԱՆ ՆՊԱՏԱԿԸ

6. Կիբեռանվտանգության ռազմավարության անհրաժեշտությունը բխում է ֆիզիկական և վիրտուալ տարածքներում ենթակառուցվածքների ապահով և հուսալի գործունեության անհրաժեշտությունից: Կիբեռտարածության

անվտանգության ապահովումից է բխում բոլոր բնագավառներում հուսալի ծառայությունների մատուցումը, ներառյալ հեռահաղորդակցությունը, արագ արձագանքման ծառայությունները, էներգետիկան, ֆինանսական համակարգը, սննդի անվտանգությունը, պետական կառավարումը, տեղական ինքնակառավարումը, առողջապահությունը, տրանսպորտը և ջրամատակարարումը: Հետևաբար, երկրի տնտեսական անվտանգության և ժողովրդավարության նպատակներին հասնելու համար, անհրաժեշտ է ունենալ հուսալի ֆիզիկական և թվային ենթակառուցվածքներ` ապահովելով կիբեռտարածության հուսալիության նույն աստիճանը ժամանակակից պահանջներին համապատասխան: Այս առումով կարևոր է նկատի ունենալ, որ ֆիզիկական ենթակառուցվածքների աշխատանքը առավելապես կախված է թվային ենթակառույցների և կրիտիկական տեղեկատվական ենթակառուցվածքների հուսալիությունից` ծառայությունները մատակարարելու և բնականոն աշխատանք ապահովելու նպատակով: Հետևաբար, կրիտիկական տեղեկատվական ենթակառույցների աշխատանքի ցանկացած խափանում կարող է անմիջական և թուլացնող ազդեցություն ունենալ պետության համար, որի արդյունքում կխափանեն բազմաթիվ բնագավառներում կենսական գործառույթները: Այսպիսով, կրիտիկական տեղեկատվական ենթակառուցվածքների պաշտպանությունը տարբեր կազմակերպությունների պատասխանատվությունն է:

7. Սույն փաստաթուղթը հաստատում է Հայաստանի Հանրապետության «Կիբեռանվտանգության ռազմավարությունը»: Այն երկարաժամկետ ծրագիր է, որը կոչված է ապահովել երկրի պաշտպանությունը` կիբեռսպառնալիքներից, կառավարման ռիսկերից և մարտահրավերներից:

8. Սույն Ռազմավարությունը բխում է Հայաստանի Հանրապետության Նախագահի «Հայաստանի Հանրապետության տեղեկատվական անվտանգության և տեղեկատվական քաղաքականության հայեցակարգը հաստատելու մասին» ՆԿ-146-Ա կարգադրության պահանջներից, որի նպատակն է ձևավորել համապարփակ տեսլական համակարգելով կիբեռտարածությունը` պետության, մասնավոր հատվածի, հասարակություն և միջազգային ջանքերը, ապահովելով Հայաստանի Հանրապետության անվտանգությունն և բարեկեցությունն:

9. Կիբեռանվտանգության ազգային ռազմավարությունն ուրվագծում է երկրի կիբեռտարածության կամ կրիտիկական տեղեկատվական ենթակառույցների ռիսկերի կառավարման գործողությունների կազմակերպման և նախապատվության համակարգը:

10. Վերոնշյալ նպատակներին հասնելու համար, Ռազմավարությունը նշանակալիորեն բարձրացնում է կիբեռանվտանգության դերը պետական կառավարման համակարգում և սահմանում հստակ դերեր ու պատասխանատվություն:

11. Նկատի ունենալով կիբեռխոցելիությունների համապարփակ բնույթը, Ռազմավարությունը նաև պետություն-մասնավոր հատված համագործակցության պահանջ է դնում, ինչը հնարավոր կդարձնի մասնավոր հատվածի սեփականություն հանդիսացող կրիտիկական տեղեկատվական ենթակառուցվածքների պաշտպանությունը կիբեռհարձակումներից` ներառյալ

բանկային հատվածը, հանրային ծառայությունները և հեռահաղորդակցությունը:

12. Կիբեռանվտանգությունը կրում է անդրսահմանային բնույթ և, որպես այդպիսին, միջազգային լուծումների կարիք ունի: Հետևաբար, Հայաստանի Հանրապետությունը տեղական և միջազգային համագործակցության մաս դառնալու պարտավորություն է ստանձնում, մշակելով կիբեռանվտանգության մարտահրավերներին դիմակայելու լուծումներ, անկախ սպառնալիքից:

III. ՌԱԶՄԱՎԱՐՈՒԹՅԱՆ ԱՆՀՐԱԺԵՇՏՈՒԹՅԱՆ ՀԻՄՆԱՎՈՐՈՒՄԸ

13. Վերջին տարիներին Հայաստանի Հանրապետությունը ծավալուն աշխատանքներ է իրականացրել էլեկտրոնային առցանց ծառայությունների զարգացման ուղղությամբ: Այս աշխատանքները առավել զարգացման միտում ունեն, նկատի ունենալով ներկայիս՝ դեպի «Թվային Հայաստան» վերափոխվելու ուղղվածությունը: Հարկ է նշել, որ «Թվային Հայաստան»-ի զարգացումը և էլեկտրոնային ծառայությունների տարածումը հնարավոր չեն լինի, եթե դրանք չզուգորդվեն համացանցի և կիբեռտարածության հուսալիության բարձրացմամբ:

14. Ներկայիս սպառնալիքները կիբեռտարածությունում բազմաթիվ և բազմաբնույթ են: Դրանց ազդեցությունը զգացվում է առօրյա գործունեության գրեթե բոլոր բնագավառներում՝ ինչպես կառավարության գործունեության, այնպես էլ գործարար շրջանակների և քաղաքացիների վրա: Սպառնալիքները կարող են ներառել քաղաքական և տնտեսական լրտեսությունից մինչև զեղծարարություն, որի արդյունքում քաղաքացիներից կորզում են տեղեկություններ իրենց բանկային հաշիվների և այլ անհատական տվյալների վերաբերյալ: Համացանցի կառուցվածքը խթանում է որոշ կիբեռսպառնալիքների տարածմանը: Սակայն հուսալի համացանցը հանդիսանում է բազմաթիվ պետական և մասնավոր ծառայությունների մատուցման հիմք:

15. Մեծ նշանակություն ունի տեղեկատվական ենթակառուցվածքների պաշտպանությունը: Կիբեռտարածության զարգացումների շնորհիվ նորանոր ենթակառուցվածքների կառավարումը իրականացվում է էլեկտրոնային եղանակով, և այդ կառավարման համակարգերի սպառնալիքները կարող են վտանգել այնպիսի կրիտիկական տեղեկատվական ենթակառուցվածքներ, ինչպիսիք են հանրային ծառայությունները, խելացի ցանցերը, չափորոշիչներ և այլն:

IV. ՌԱԶՄԱՎԱՐՈՒԹՅԱՆ ՏԵՍԼԱԿԱՆԸ

16. Համատեղ աշխատանքի արդյունքում երկրի վրա ազդող կիբեռսպառնալիքների սպառնալիքների կանխարգելում, հետևանքների վերացում և անվտանգության մակարդակի բարձրացում, անկախ դրանց ծագումից և տեսակից, ինչի արդյունքում կստեղծվեն արդյունավետ պետական կառավարումը, զարգացող տնտեսությունը, ազգային անվտանգությունը, ներառական հասարակությունը և ազգային արժեքները ձևավորող՝ անվտանգ, ապահով և առաձգական կրիտիկական տեղեկատվական ենթակառուցվածքներ:

17. Ընդունելով կիբեռսպառնալիքների, ռիսկերի և մարտահրավերների ազդեցությունը երկրի ազգային արժեքների և շահերի վրա, Ռազմավարությունը կարևորում է այս արագ զարգացող վտանգներին դիմակայելու համար պետություն-մասնավոր հատված համատեղ աշխատանքի անհրաժեշտությունը: Այս համապարփակ մոտեցումը առավելագույնս կօգտագործի պետական կառավարման, տարբեր բնագավառներ ներկայացնող կազմակերպությունների, քաղաքացիների և միջազգային գործընկերների կարողությունները՝ կիբեռտարածության սպառնալիքները նվազեցնելու նպատակով: Ռազմավարությունը նաև նկարագրում է այն կազմակերպական կառուցվածքը, որը կապահովի պետական և տեղական ինքնակառավարման մարմինների, մասնավոր կազմակերպությունների և անհատների բարեկեցությանը և ազգային անվտանգությանը սպառնացող ռիսկերը արդյունավետ չեզոքացումը և պաշտպանությունը:

18. Պետություն-մասնավոր հատված համագործակցության միջոցով բացահայտել առկա մարտահրավերները և ռիսկերը, դրան համապատասխան մշակել կրթական ծրագրեր և դրանք տրամադրել շահագրգիռ կառույցներին:

V. ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԵՆՏՐՈՆԻ ՍՏԵՂԾՈՒՄ

19. Տեղեկտվական տեխնոլոգիաների զարգացման զուգահեռ առաջանում է նորանոր մարտահրավերներ: Այդ մարտահրավերներից կարևորագույնը կիբեռհարձակումներից տեղեկատվական համակարգերի պաշպանությունն է՝ անկախ հասանելի և սահմանափակ հասանելիության տեղեկատվության հավաքագրման և մշակման բնույթից:

20. Տարիների ընթացքում այս ոլորտում տարբեր գերատեսչությունների կողմից իրականացվել է որոշակի գործունեություն, ընդունվել են տեղեկատվական անվտանգության առանձին ուղղությունները կանոնակարգող հայեցակարգային և իրավական փաստաթղթեր, այդուհանդերձ կիբեռանվտանգության ոլորտը պահանջում է հստակ կանոնակարգում: Կիբեռսպառնալիքները կանխարգելելու, կանխելու և դրանց դեմ հակազդման մեխանիզմներ մշակելու, կիբեռանվտանգության արդյունավետ համակարգ ձևավորելու համար անհրաժեշտ է իրականացնել կիբեռանվտանգության ոլորտում պետական միասնական քաղաքականության, որին հասնելու համար անհրաժեշտ է ստեղծել կիբեռանվտանգության կենտրոն:

21. Կիբեռանվտագության կենտրոնը լինելու է առանձնացված կառույց:

22. Կիբեռանվտագության կենտրոնի հիմնական գործառույթներն են կիբեռանվտանգության միասնական և անհատական՝ ըստ ոլորտային նշանակության ռազմավարության և քաղաքականության մշակման ու համակարգման, կիբեռանվտանգության կանխարգելման գործընթացների աուդիտի և համակարգման, պետական մարմինների հետ աշխատանքների փոխկապակցության ապահովման և մասնագիտական խորհրդատվության տրամադրման, կրթական գործընթացների կազմակերպման, միջազգային

փորձի ուսումնասիրման և տեղայնացման աշխատանքների իրականացումը:

23. Կիբեռանվտանգության կենտրոնը կարող է ստեղծվել 2 տարբերակով.

1) Կենտրոն ստեղծվում է ՀՀ կառավարությանը կից մարմնի տեսքով՝ իր աշխատակազմով, գույքով, կանոնադրությամբ և պետական բյուջեով նախատեսված հատկացումների հիման վրա:

2) Կենտրոնը ստեղծվում է արդեն իսկ գործող պետական մարմնի կամ պետական մարմնի կողմից ստեղծված կազմակերպության (հիմնադրամի) վերամիավորման շրջանակներում:

VI. ՌԱԶՄԱՎԱՐՈՒԹՅԱՆ ՄՈՏԵՑՈՒՄՆԵՐ

24. Օրենսդրություն

1) Կիբեռանվտանգության ոլորտը կանոնակարգելու, միասնական քաղաքականություն իրականացնելու, մարտահրավերների դեմ պայքար իրականացնելու նպատակով անհրաժեշտ է միջազգային լավագույն փորձի հիման վրա մշակել, լրամշակել և կատարելագործել կիբեռանվտանգության ոլորտի ՀՀ օրենսդրությունը և ապահովել դրա իրականացումը:

25. Կիբեռանվտանգության ենթակառուցվածք

1) Թվայնացման գործընթացների կազմակերպման կարևոր հանգամանքներից մեկը նրա անվտանգության, չթույլատրված մուտքից հեռահաղորդակցության ու տեղեկատվական ռեսուրսների պաշտպանության, փոխանցվող տեղեկատվության գաղտնիության և արտակարգ իրավիճակներում տեղեկատվական համակարգերի հուսալի աշխատանքի ապահովումն է:

2) Այդ նպատակով անհրաժեշտ է բարձրացնել մասնագիտական կարողությունները, ներդնել միջազգայնորեն ճանաչված ստանդարտներ և ձևավորել համակարգչային պատահարների արագ արձագանքման կենտրոն:

26. Կառավարման համակարգի ձևավորում

1) Կիբեռանվտանգության միասնական քաղաքականության մշակման և համակարգման, կիբեռանվտանգության կանխարգելման գործընթացների համակարգման, կրթական գործընթացների կազմակերպման, միջազգային փորձի ուսումնասիրման և տեղայնացման գործընթացի կազմակերպման նպատակով ստեղծել Կիբեռանվտանգության կենտրոն:

2) Կիբեռանվտանգության կենտրոն կապահովի նաև կիբեռանվտանգության ոլորտի միջազգային համագործակցությունը և տեղեկատվության անվտանգ փոխանցման գործընթացները:

27. Կրթություն, հետազոտություններ, մասնագիտական զարգացում, հանրային իրազեկում

1) Կիբեռանվտանգության դեմ պայքարի մարտահրավեր է ինչպես

Հայաստանում, այնպես էլ ամբողջ աշխարհում: Պայքարը հնարավոր չէ արդյունավետ կազմակերպել առանց որակյալ և բանիմաց հասարակության առկայությամբ: Վերջինիս լուծման լավագույն տարբերակը ոլորտի զարգացմանը համապատասխան կրթական ծրագրերի մշակումն ու իրականացումն է, ինչպես նաև հանրային իրազեկման միջոցառումների անցկացումն է:

Հավելված N 1

Հայաստանի Հանրապետության

կառավարության

2017 թ. N որոշման

Ժ Ա Մ Ա Ն Ա Կ Ա Ց ՈՒ Յ Ց

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆԻՑ ԲԽՈՂ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ

	Խնդիր	Իրա
1.	Օրենսդրություն	
1.1.	Կիբեռհանցագործությունների դեմ արդյունավետ պայքար ապահովող օրենդրության վերլուծություն և համապատասխան օրենսդրական փոփոխությունների առաջարկների ներկայացում	2018
1.2.	Կիբեռանվտանգությանը և համապատասխանության ապահովմանը վերաբերող լավագույն միջազգային փորձի ուսումնասիրում և անհրաժեշտ կարգերի մշակում և ներկայացում ՀՀ կառավարություն	2018
1.3.	Կրիտիկական տեղեկատվական ենթակառուցվածքների ընտրության չափանիշների սահմանում և հաստատում	2018

1.4.	Կրիտիկական տեղեկատվական ենթակառուցվածքների ցանկի սահմանում, դրանց կայունության վերլուծություն, անհրաժեշտ պաշտպանական միջոցների մշակում և իրականացում	2018
2.	Կիբերանվտանգության ենթակառուցվածք	
2.1.	Պետության կողմից ճանաչված՝ համակարգչային անվտանգության պատահարների արձագանքման կենտրոնի (CSIRT) ձևավորում	2018
2.2.	Կիբեռանվտանգության՝ միջազգայնորեն ճանաչված ստանդարտների ներդրման համակարգերի ձևավորում	2018
2.3.	Կիբեռանվտանգության բնագավառում գործող պետական մարմինների և մասնագետների հավաստագրման համակարգի նախագծում և հիմնում	2018
3.	Կառավարման համակարգի ձևավորում	
3.1.	Կիբեռանվտանգության կենտրոնի ձևավորում	2018
3.2.	Կիբեռանվտանգության գնահատման ազգային համակարգի նախագծում	2018

4.	Կրթություն, հետազոտություններ, մասնագիտական զարգացում, հանրային իրա	
4.1.	Կիբեռանվտանգության կրթական ծրագրերի մշակում և իրագործում	2018
4.2.	Կիբեռանվտանգության վերաբերյալ հանրային իրազեկման միջոցառումների մշակում և իրագործում	2018
4.3.	Կիբեռանվտանգության բնագավառում հետազոտական ծրագրերի մշակում և իրագործում	2018
4.4.	Համապատասխան պետական ծառայողների համար կիբեռանվտանգության ոլորտում միջազգայնորեն ճանաչված կրթական և հավաստագրման ծրագրերում մասնակցության գործընթացի սահմանում և կազմակերպում	2018
4.5.	ՀՀ պետական մարմինների դասակարգում ըստ առաջնայնության և դրանց միջազգայնորեն ճանաչված կիբեռանվտանգության ստանդարտներին համապատասխան հավաստագրման ժամանակացույցի մշակում և իրագործում	2018
5.	Պետական կառավարում, միջազգային համագործակցություն	
5.1.	Այլ պետությունների հետ կիբեռանվտանգության ապահովման միջոցների համատեղ օգտագործման և տեղեկատվության փոխանակման նպատակով գործընկերության հաստատում	2018

5.2.	Պետական կառավարման համակարգում կիբեռանվտանգության ապահովման միջոցների համատեղ օգտագործման և տեղեկատվության փոխանակման ծրագրի մշակում	2018
5.3.	Պետության և մասնավոր հատվածի միջև կիբեռանվտանգության ապահովման միջոցների համատեղ օգտագործման և տեղեկատվության փոխանակման ծրագրի մշակում	2018
5.4.	Կիբեռանվտանգության բնագավառում տարածաշրջանային և միջազգային կառույցներում մասնակցության ընդլայնում և ամրապնդում	2018