DOI: 10.59560/18291155-2024.3-209

ՇՈՂԵՐ ԳՐԻԳՈՐՅԱՆ
ՀՀ ՆԳՆ փրկարար ծառայության
ծառայության կազմակերպման
վարչության հրահանգիչ,
Հայ-ռուսական համալսարանի
քաղաքագիտության ամբիոնի հայցորդ

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՊԵՏԱԿԱՆ ՄԱՐՄԻՆՆԵՐԸ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԳՈՐԾԸՆԹԱՑՈՒՄ

Ամփոփագիր

Ժամանակակից աշխարհում տեղեկատվական անվտանգությունը դարձել է յուրաքանչյուր պետության ազգային անվտանգության կարևորագույն բաղադրիչներից մեկը: Տեխնոլոգիական առաջընթացը, կիբեռսպառնալիքների աճը և թվային տեղեկատվության լայն տարածումը պահանջում են երկրներից ակտիվ միջոցներ ձեռնարկել իրենց տեղեկատվական ռեսուրսները պաշտպանելու համար: Հայաստանի Հանրապետությունը (ՀՀ), ինչպես և շատ այլ պետություններ, առերեսվում են տեղեկատվական անվտանգության ոլորտում լուրջ մարտահրավերների հետ: Այս համատեքստում առանձնահատուկ նշանակություն է ստանում պետական մարմինների դերը, քանի որ հենց նրանք են պատասխանատու քաղաքականության մշակման, ռազմավարությունների ձևավորման և տեղեկատվության պաշտպանության գործնական միջոցառումների իրականացման համար:

Պետական մարմինները հանդես են գալիս ոչ միայն որպես օրենքների և կարգավորումների մշակողներ ու իրականացնողներ, այլև հիմնական

համակարգման կենտրոններ, որոնք պատասխանատու են տարբեր սուբյեկտների՝ մասնավոր հատվածից մինչև միջազգային գործընկերներ, փոխգործակցության համար: Նրանք ապահովում են անվտանգության պահանջների կատարման մոնիտորինգը և վերահսկումը, արձագանքում են միջադեպերին և նպաստում ընդհանուր իրազեկվածության և տեղեկատվության պաշտպանության հմտությունների բարձրացմանը:

Սույն հոդվածում կներկայացվեն պետական մարմինների հիմնական գործառույթները տեղեկատվական անվտանգության ոլորտում, դրանց ազդեցությունը ազգային անվտանգության ապահովման վրա և դերը ժամանակակից սպառնալիքներին դիմակայելու հարցում:

Հիմնաբառեր. տեղեկատվական անվտանգություն, պետական մարմիններ, ազգային անվտանգություն, սպառնալիքներ, մարտահրավերներ, գործառույթներ, կիբեռանվտանգություն:

1. Պետության դերը տեղեկատվական անվտանգության գործընթացում

Յուրաքանչյուր հասարակության բնականոն գոյության և զարգացման անհրաժեշտ պայմանն է արտաքին և ներքին սպառնալիքներից պաշտպանված լինելը, արտաքին ճնշումների փորձերին դիմակայելու ունակությունը, նման փորձերը հետ մղելու և առաջացող սպառնալիքները չեզոքացնելու ունակությունը, ինչպես նաև այնպիսի ներքին և արտաքին պայմաններ ապահովելը, որոնք երաշխավորում են հասարակության և նրա քաղաքացիների կայուն և բազմակողմանի առաջընթացը: Այս վիճակը բնութագրելու համար օգտագործվում է «ազգային անվտանգություն» հասկացությունը[1]:

ՀՀ ազգային անվտանգությունը կենսական ազգային շահերի պաշտպանվածության վիճակն է ներքին և արտաքին սպառնալիքներից, որի պայմաններում ապահովվում են անձի, հասարակության և պետության անվտանգությունը, երկրի տարածքային ամբողջականությունը,

[1] **Вострецова Е.В.** Основы информационной безопасности // Учебное пособие. - Екатеринбург: Издательство Уральского университета, 2019. - С. 208.

ինքնիշխանությունը, սահմանադրական կարգը, տնտեսության բնականոն զարգացումը, հասարակության նյութական և հոգևոր արժեքների, քաղաքացիների իրավունքների և ազատությունների, շրջակա միջավայրի պաշտպանությունը, ՀՀ կայուն սոցիալ-տնտեսական զարգացումը[1]: Ազգային անվտանգությունը ներառում է երկրի պաշտպանությունը և բոլոր այն տեսակի անվտանգության հարցերը, որոնք սահմանված են ՀՀ Սահմանադրությամբ և ՀՀ օրենսդրությամբ, առաջին հերթին՝ պետական, հասարակական, տեղեկատվական, էկոլոգիական, տնտեսական, տրանսպորտային, էներգետիկ անվտանգությունը և անձի անվտանգությունը[2]:

Ուստի, «ազգային անվտանգություն» հասկացության բովանդակության մեջ կարելի է առանձնացնել տարբեր կառուցվածքային տարրեր (կոմպոնենտներ), որոնցից մեկը տեղեկատվական անվտանգությունն է:

Քանի որ երկրի ինֆորմատիզացման, տեղեկատվական տեխնոլոգիաների զարգացման պայմաններում տեղեկատվական ռեսուրսները ձևավորվում են գործունեության բոլոր ոլորտներում, առաջին հերթին՝ քաղաքական, ռազմական, տնտեսական, գիտատեխնիկական ոլորտներում, տեղեկատվական անվտանգությունը պետք է դիտարկել որպես ազգային անվտանգության համալիր ցուցանիշ:

Սրանով է պայմանավորված ժամանակակից պայմաններում տեղեկատվական անվտանգության առաջատար դերերից մեկը երկրի ազգային անվտանգության համակարգում:

Տեղեկատվական անվտանգությունն ապահովվում է ազգային անվտանգության ապահովման շրջանակներում: Ազգային անվտանգությունը ձեռք է բերվում անվտանգության ապահովման ոլորտում միասնական պետական քաղաքականություն վարելու, անձի, հասարակության և պետության կենսական շահերին սպառնացող

[1] Ազգային անվտանգության մասին ՀՀ օրենք (ընդունվել է 2001 թվականի դեկտեմբերի 28-ին):

[2] ՀՀ ազգային անվտանգության ռազմավարություն,
https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf

վտանգներին համապատասխան տնտեսական, քաղաքական և այլ բնույթի միջոցառումների համակարգի միջոցով[1]:

Պետությունն առանցքային դեր է կատարում տեղեկատվական անվտանգության քաղաքականության ձևավորման, տեղեկատվական միջավայրի պաշտպանությանն ուղղված օրենսդրական միջոցառումների մշակման և իրականացման գործում: Այն ներառում է օրենքների մշակում, որոնք կարգավորում են անձնական տվյալների, տեղեկատվական ռեսուրսների, ազգային և մշակութային արժեքների պաշտպանությունը, ինչպես նաև տեղեկատվական սպառնալիքները կանխելու ռազմավարությունների և քաղաքականության ստեղծումը: Պետական քաղաքականությունը պետք է լինի ճկուն և հարմարվող՝ ժամանակին արձագանքելու տեխնոլոգիական ոլորտում փոփոխություններին և նոր սպառնալիքներին, որոնք ի հայտ են գալիս այդ փոփոխությունների արդյունքում:

Տեղեկատվական անվտանգության ոլորտում օրենսդրությունը պետք է հաշվի առնի ինչպես ներքին, այնպես էլ միջազգային ասպեկտները, քանի որ կիբեռսպառնալիքները հաճախ չեն սահմանափակվում մեկ երկրի սահմաններով: Պետությունը պետք է ակտիվ մասնակցություն ունենա միջազգային համաձայնագրերին և նախաձեռնություններին, որոնք ուղղված են կիբեռհանցագործությունների դեմ պայքարին և գլոբալ տեղեկատվական համակարգերի անվտանգությանը[2]:

ՀՀ-ն, իր ազգային անվտանգության ռազմավարության մեջ ընդգրկելով տեղեկատվական անվտանգության և կիբեռանվտանգության կարևորագույն մարտահրավերները, նշել է մի շարք խնդիրներ, որոնք կարգավորում են պահանջում: Նշվում է, որ տեղեկատվական և կիբեռանվտանգության ոլորտը կարգավորող համապարփակ պետական քաղաքականությունը դեռևս անկատար է, ինչը բացասաբար է անդրադառնում երկրի ընդհանուր անվտանգության վրա:

[1] **Вострецова Е.В.** Основы информационной безопасности: Учебное пособие. – Екатеринбург: Издательство Уральского университета, 2019. - С. 208.

[2] **Чеботарева А.А.** Информационное право: Учебное пособие. - Москва, 2014. - С. 160.

Ռազմավարությունը նաև ընդգծում է կենսական նշանակության տեղեկատվական ենթակառուցվածքների պաշտպանության ապահովման նպատակով համապատասխան օրենսդրության բացակայությունը, ինչը լուրջ սպառնալիք է ներկայացնում ինչպես պետական, այնպես էլ մասնավոր սեկտորի համար:

Բացի այդ, համարվում է, որ համակարգչային պատահարների արձագանքման կառույցների ինստիտուցիոնալ կարողությունները դեռևս բավարար մակարդակի վրա չեն գտնվում, ինչը խոչընդոտում է արդյունավետ և օպերատիվ արձագանքմանը հնարավոր կիբեռհարձակումներին:

Վերջապես, նշվում է, որ առկա է կիբեռանվտանգության ոլորտը համակարգող կենտրոնացված կառույցի բացակայություն, ինչը խոչընդոտում է արդյունավետ և համատեղ աշխատանքին տվյալ ոլորտում ներգրավված տարբեր պետական մարմինների միջև:

ՀՀ-ն ստանձնել է պատասխանատվություն՝ այս կարևորագույն խնդիրների լուծման ուղղությամբ քայլեր ձեռնարկելու և այդ մարտահրավերների հաղթահարմանն ուղղված քաղաքականության մշակման ու կիրառման գործում[1]:

Պետական մարմինները պատասխանատու են այս ոլորտում արդյունավետ քաղաքականության ձևավորման և իրականացման, կարևոր տեղեկատվական ենթակառուցվածքների պաշտպանության, կիբեռ միջադեպերին արագ արձագանքելու և միջազգային համագործակցության համար: Մշտապես փոփոխվող սպառնալիքների և տեխնոլոգիական առաջընթացի միջավայրում պետությունները պետք է պատրաստ լինեն ձևափոխել իրենց մոտեցումները և կիրառել նորարարական լուծումներ՝ ապահովելու տեղեկատվական տարածքի հուսալի պաշտպանությունը:

[1] ՀՀ ազգային անվտանգության ռազմավարություն,
https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf

2. ՀՀ պետական մարմինների դերը և խնդիրները տեղեկատվական անվտանգության ապահովման գործընթացում

ՀՀ-ն տարածաշրջանային և համաշխարհային գործընթացներում ներգրավված երկիր է և լիիրավ մասնակից բազմաթիվ քաղաքական, սոցիալական և տնտեսական իրադարձությունների՝ ինչպես տարածաշրջանային, այնպես էլ միջազգային մակարդակներում: Այս առումով ՀՀ շահերը միջազգային անվտանգության հարցերում օբյեկտիվորեն հատվում են այլ պետությունների շահերի հետ, ներառյալ՝ թմրամիջոցների ապօրինի շրջանառության դեմ պայքարը, միջազգային ահաբեկչության դեմ պայքարը, տարածաշրջանային հակամարտությունների կարգավորումը, սուր բնապահպանական խնդիրների լուծումը և միջազգային համագործակցության այլ ոլորտներ: Մեր երկրի ազգային շահերը վերոնշյալ ոլորտներում, ինչպես նաև տեղեկատվական անվտանգության ոլորտում, որը ներառում է հասարակական և պետական գործունեության բոլոր ոլորտների և մակարդակների տեղեկատվական բաղադրիչները, սահմանում են նրա տեղեկատվական անվտանգության էությունը: Հայաստանը, գտնվելով բարդ աշխարհաքաղաքական տարածաշրջանում, ներգրավված է ակտիվ տեղեկատվական գործընթացներում: Որպեսզի ոչ միայն նվազեցվի տեղեկատվության ոլորտում ազգային շահերին սպառնացող վտանգների բացասական ազդեցությունը, այլև նախաձեռնողականություն դրսևորվի ազգային և պետական նպատակների ապահով և անվտանգ իրականացման գործընթացում, անհրաժեշտ է չափազանց գրագետ և զգույշ ներկայություն ունենալ թե՛ ներքին, թե՛ արտաքին տեղեկատվական դաշտում[1]:

Պետական մարմինները, որպես ազգային անվտանգության երաշխավորներ, կենտրոնական դեր են խաղում ներքին ու արտաքին սպառնալիքներից տեղեկատվության պաշտպանության ապահովման գործընթացում:

[1] **Аветисян П. С., Тадевосян М. Р.** Основные приоритеты развития кибербезопасности Армении в контексте медиаобразования // Регион и мир. 2023, № 1, https://geopolitika.am/dir/wp-content/blogs.dir/1/files/2023_1_18_22.pdf

ՀՀ տեղեկատվական անվտանգության ապահովման համակարգի կազմակերպական հիմքերը ներառում են մի շարք պետական ու հասարակական մարմիններ: Այս համակարգի հիմնական բաղադրիչներն են՝ ՀՀ Նախագահը, Ազգային ժողովը, Կառավարությունը, Ազգային անվտանգության խորհուրդը, ինչպես նաև միջգերատեսչական հանձնաժողովները: Դրանց կողքին նաև կարևոր դեր են խաղում տեղական ինքնակառավարման մարմինները, դատական իշխանության մարմինները, հասարակական միավորումները և քաղաքացիները, ովքեր, համապատասխան ՀՀ օրենսդրությանը, մասնակցում են տեղեկատվական անվտանգության ապահովմանը:

Նախագահը, իր սահմանադրական լիազորությունների շրջանակներում, նպաստում է տեղեկատվական անվտանգության ապահովման մարմինների արդյունավետ գործունեությանը: Կառավարությունն ապահովում է գործադիր իշխանության մարմինների գործունեությունը տեղեկատվական անվտանգության ոլորտում և նախատեսում է միջոցներ պետական ծրագրերի իրականացման համար:

Ազգային անվտանգության խորհուրդն իրականացնում է տեղեկատվական անվտանգության սպառնալիքների վերհանում և գնահատում՝ ներկայացնելով համապատասխան առաջարկություններ: Խորհուրդն առաջարկություններ է մշակում տեղեկատվական անվտանգության ապահովման, ինչպես նաև գործող հայեցակարգի ճշգրտման ուղղությամբ:

Գործադիր իշխանության մարմիններն ապահովում են օրենսդրական ակտերի պահանջների կատարումը տեղեկատվական անվտանգության ոլորտում՝ համագործակցելով ոլորտի այլ սուբյեկտների հետ, և Կառավարությանը ներկայացնում են համակարգի կատարելագործման առաջարկություններ:

Տեղական ինքնակառավարման մարմիններն իրենց լիազորությունների շրջանակներում ապահովում են օրենսդրական պահանջների կատարումը և համագործակցում քաղաքացիների ու հասարակական կազմակերպությունների հետ՝ տեղեկատվական անվտանգության ապահովման ուղղությամբ միջոցառումներ իրականացնելիս[1]:

[1] «ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին» ՀՀ Նախագահի կարգադրություն (ՆԿ-97-Ն 26.06.2009 թ.):

2011 թվականից ՀՀ տեղեկատվական անվտանգության տեխնիկական բաղադրիչի համակարգողը Ազգային անվտանգության ծառայությունն է[1]: Բովանդակային հատվածով տեղեկատվական անվտանգության գործառույթները բաշխված են մի շարք կառույցների միջև, բազմաթիվ գործառույթներ իրականացնում են ՀՀ պաշտպանության նախարարությունը, ՀՀ արտաքին գործերի նախարարությունը, ՀՀ ներքին գործերի նախարարությունը և այլն: Համակարգող դեր ունի ՀՀ Նախագահի աշխատակազմի հանրային կապերի և տեղեկատվության կենտրոնը:

Սակայն ՀՀ-ն ունի նաև տեղեկատվական անվտանգության անվերահսկելի հատվածներ: Մի շարք բնագավառներ տեղեկատվական անվտանգության առումով դուրս են մնում ընդհանուր և մասնավոր վերահսկումից: Հայաստանում գոյություն չունի ազգային կիբեռանվտանգության պատասխանատու մարմին: Ազգային անվտանգության ծառայության կողմից վերահսկվում է միայն պետական ցանցը, այն էլ՝ ոչ ամբողջությամբ: Այսպես, Կառավարությանը կից մի շարք մարմինների կայքերը չեն վերահսկվում[2]:

Հայաստանում մի շարք կրիտիկական ենթակառուցվածքներ գտնվում են անվերահսկելի վիճակում, քանի որ դրանք դուրս են պետության անմիջական վերահսկողությունից: Կենսական կարևոր հանգույցներ, լինելով մասնավոր կամ օտարերկրյա կազմակերպությունների վերահսկողության ներքո, չեն ենթարկվում օրենսդրությամբ սահմանված տեղեկատվական անվտանգության հստակ պահանջներին: Օրենքով ամրագրված չեն մեխանիզմներ, որոնք թույլ կտային որևէ պետական կամ անկախ մարմնի իրականացնել աուդիտ և բացահայտել համակարգային խոցելիությունները, որոնք կարող են նպաստել կիբեռհարձակումներին:

[1] Տեղեկատվական անվտանգության ապահովման ոլորտում լիազոր և ազգային համակարգող մարմին նշանակելու մասին ՀՀ կառավարության 2011 թ. մարտի 3-ի N 185-Ա որոշում:

[2] **Մարտիրոսյան Ս.Վ.**, Հայաստանի տեղեկատվական անվտանգությունը և կրիտիկական ենթակառուցվածքները: «21-րդ ԴԱՐ», թիվ 3 (73), 2017թ., http://noravank.am/upload/pdf/Samvel_Martirosyan_21_DAR_03_2017.pdf

Օրինակ, եթե Մեծամորի ատոմակայանը գտնվում է պետական վերահսկողության տակ և այստեղ գործում են տեղեկատվական անվտանգության որոշակի չափանիշներ, ապա մնացած էներգահամակարգը գործնականում ազատ է այս կարգավորումներից: Այդպես, առանց պետական վերահսկողության և տեղեկատվական անվտանգության չափանիշների են մնացել մի շարք կարևոր ենթակառուցվածքներ, այդ թվում՝

- էլեկտրաէներգետիկայի համակարգը,
- գազամատակարարումը,
- ջրամատակարարումն ու կոյուղու համակարգը,
- հեռահաղորդակցությունը[1]:

Կիբեռանվտանգության տեսանկյունից չվերահսկվող հատված-ները կարող են դառնալ ավելի խոցելի տարբեր վտանգների նկատմամբ, մասնավորապես՝ հանդիսանալ թիրախ հաքերների և կիբեռհանցագործների համար:

Նշված իրավիճակում պետությունը պետք է ունենա ավելի հստակ մոտեցումներ տեղեկատվական անվտանգության և կրիտիկական ենթակառուցվածքների պաշտպանության հարցերում:

3. Եզրակացություն

Պետական մարմիններն առանցքային դեր են կատարում տեղեկատվական անվտանգության ապահովման գործընթացի բոլոր մակարդակներում՝ կարգավորող դաշտի մշակումից մինչև միջադեպերին արագ արձագանքելը: Նրանց գործունեությունն ուղղված է անվտանգ տեղեկատվական միջավայրի ստեղծմանը, որը պետության և հասարակության կայուն զարգացման բանալին է: Այս ոլորտում պետական մարմինների արդյունավետությունը մեծապես կախված է նոր մարտահրավերներին դիմակայելու և տեղեկատվական անվտանգության ապահովման գործում ներգրավված տարբեր սուբյեկտների հետ փոխգործակցություն ապահովելու նրանց կարողությունից:

[1] Տես՝ նույն տեղում:

Օգտագործված նորմատիվ իրավական ակտերի և գրականության ցանկ

1. Ազգային անվտանգության մասին ՀՀ օրենք (ընդունվել է 2001 թվականի դեկտեմբերի 28-ին):

2. ՀՀ ազգային անվտանգության ռազմավարություն, https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf

3. ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին» ՀՀ Նախագահի կարգադրություն (ՆԿ-97-Ն 26.06.2009 թ.):

4. **Մարտիրոսյան Ս.Վ.**, Հայաստանի տեղեկատվական անվտանգությունը և կրիտիկական ենթակառուցվածքները: «21-րդ ԴԱՐ», թիվ 3 (73), 2017 թ., http://noravank.am/upload/pdf/Samvel_Martirosyan_21_DAR_03_2017.pdf

5. Տեղեկատվական անվտանգության ապահովման ոլորտում լիազոր և ազգային համակարգող մարմին նշանակելու մասին ՀՀ կառավարության 2011 թ. մարտի 3-ի N 185-Ա որոշում:

6. **Вострецова Е.В.** Основы информационной безопасности // Учебное пособие. – Екатеринбург: Издательство Уральского университета, 2019. - 208 с.

7. **Аветисян П.С., Тадевосян М.Р.** Основные приоритеты развития кибербезопасности Армении в контексте медиаобразования // Регион и мир. 2023, № 1; https://geopolitika.am/dir/wp-content/blogs.dir/1/files/2023_1_18_22.pdf

8. **Чеботарева А.А.** Информационное право // Учебное пособие. - Москва, 2014. - 160 с.

ГОСУДАРСТВЕННЫЕ ОРГАНЫ В ПРОЦЕССЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ АРМЕНИЯ

Аннотация

В современном мире информационная безопасность стала одной из важнейших составляющих национальной безопасности каждого государства. Технологический прогресс, рост киберугроз и повсеместное распространение цифровой информации требуют от стран принятия превентивных мер по защите своих информационных ресурсов. Республика Армения, как и многие другие государства, сталкивается с серьезными вызовами в сфере информационной безопасности. В этом контексте роль государственных органов имеет особое значение, поскольку они несут ответственность за разработку политики, формулирование стратегии и реализацию практических мер по защите информации.

Государственные органы являются не только разработчиками и исполнителями нормативно-правовых актов, но и основными координационными центрами, отвечающими за взаимодействие различных субъектов, от частного сектора до международных партнеров. Они обеспечивают мониторинг и контроль соблюдения требований безопасности, реагируют на инциденты, повышают общую осведомленность и навыки защиты информации.

В данной статье будут представлены основные функции государственных органов в сфере информационной безопасности, их влияние на обеспечение национальной безопасности и их роль в противодействии современным угрозам.

Ключевые слова: информационная безопасность, государственные органы, национальная безопасность, угрозы, вызовы, функции, кибербезопасность.

STATE BODIES IN THE PROCESS OF ENSURING INFORMATION SECURITY OF THE REPUBLIC OF ARMENIA

Annotation

In the modern world, information security has become one of the most important components of the national security of every state. Technological progress, the growth of cyber threats and the widespread distribution of digital information require countries to take proactive measures to protect their information resources. The Republic of Armenia, like many other states, faces serious challenges in the field of information security. In this context, the role of state bodies is of particular importance, as they are responsible for policy development, strategy formulation and implementation of practical information protection measures.

State bodies are not only the developers and implementers of laws and regulations, but also the main coordination centers responsible for the interaction of various entities, from the private sector to international partners. They provide monitoring and control of compliance with security requirements, respond to incidents, and promote general awareness and information protection skills.

This article will present the main functions of state bodies in the field of information security, their impact on ensuring national security and their role in countering modern threats.

Keywords: information security, state bodies, national security, threats, challenges, functions, cyber security.

Հոդվածը հանձնված է խմբագրություն 02.09.2024 թ., տրվել է գրախոսության 02.09.2024 թ., ընդունվել է տպագրության 08.09.2024 թ.: