

**ԹՎԱՅԻՆ ԻՆՔՆԻԶԻՏԱՆՈՒԹՅԱՆ ՀԻՄՆԱԽՆԴԻՐԸ
ԳԼՈՐԱԼԱՑՎՈՂ ԱՇԽԱՐՀՈՒՄ ***

ՀՏԴ 004

DOI: 10.52063/25792652-2025.1.24-138

ԱՆՆԱ ՍԻՍՈՅԱՆ

Երևանի պետական համալսարանի միջազգային հարաբերությունների
ֆակուլտետի քաղաքագիտության ամբիոնի հայցորդ,
ք. Երևան, Հայաստանի Հանրապետություն

anna.sisoyan@ysu.am

ORCID ID: 0009-0009-6170-5366

**Հոդվածի գլխավոր նպատակը թվային ինքնիշխանության բարձրացման
հնարավոր ուղիների բացահայտումն է՝ հիմնվելով Եվրամիության և Նրա
անդամ պետությունների փորձի վերլուծության վրա:**

Նպատակին հասնելու համար մեր առջև դրել ենք հետևյալ խնդիրները՝
վերլուծել «թվային ինքնիշխանություն» հասկացության բովանդակությունը,
դրա Եությունը և սահմանումները, ուսումնասիրել թվային ինքնիշխանության
հիմնական բաղադրիչները և պարզել դրանց փոխկապակցվածությունը,
հայտնաբերել թվային ինքնիշխանության ձևավորման և ամրապնդման
հիմնական նախապայմանները՝ ներառյալ տեխնոլոգիական անկախության,
տվյալների վերահսկման և իրավակարգավորող մեխանիզմների դերը, վեր
հանել այն խնդիրներն ու մարտահրավերները, որոնք կարող են խոչընդոտ
հանդիսանալ թվային ինքնիշխանության հասնելու ճանապարհին:

Հոդվածում ներկայացված է թվային ինքնիշխանության մակարդակների
և աստիճանների համեմատական վերլուծություն, ինչը հնարավորություն է
տալիս հստակ գնահատելու տարբեր երկրների դիրքերը և Նրանց կիրառած
ռազմավարությունները: Վերլուծության միջոցով առանձնացվում են ոլորտի
հիմնական խնդիրները, ինչպես նաև առաջարկվում են մեխանիզմներ և
գործնական լուծումներ, որոնք կարող են նպաստել թվային ինքնիշխանության
բարձրացմանը:

Հետազոտության ընթացքում կատարված եզրակացությունը ցույց է
տալիս, որ Նույնիսկ տեխնոլոգիապես զարգացած երկրները բախվում են
մարտահրավերների՝ թվային ինքնիշխանության ապահովման ճանապարհին:
Եզրակացության մեջ ընդգծվում է նաև, որ տեղեկատվական
տեխնոլոգիաների արագ զարգացման պայմաններում թվային
ինքնիշխանությունը դառնում է պետական ինքնիշխանության անբաժանելի
մաս: Այս առումով, թվային տիրույթի պաշտպանությանն ուղղված
քաղաքականությունն ու միջոցառումները կարևոր նշանակություն ունեն,
քանի որ գլոբալ փոխկապակցվածությունը նաև ինքնիշխանության կորստի
ռիսկեր է պարունակում:

Հիմնաբառեր՝ թվային ինքնիշխանություն, թվային տիրույթ, տվյալների
ինքնիշխանություն, ինքնիշխան ամս, ամսային պահեստ, համացանց, տվյալների
ռեզիդենտություն:

* Հոդվածը ներկայացվել է 10.02.2025թ., գրախոսվել՝ 08.04.2025թ., տպագրության ընդունվել՝
30.04.2025թ.:

Ներածություն

Արդի գլոբալացվող աշխարհում տեղեկատվական տեխնոլոգիաների, ցանցերի ու տվյալների բազաների աճին զուգընթաց մեծացել է քաղաքականության բոլոր մակարդակներում գործող սուբյեկտների միջև փոխկախվածությունը: Խոսքը հատկապես վերաբերում է համաշխարհային քաղաքականության ու միջազգային հարաբերությունների համակարգում նկատվող փոխազդեցություններին:

Այս ամենը իր հետ բերում է լուրջ անվտանգային խնդիրներ՝ տեղեկատվությանը տիրապետելու համատեքստում, քանի որ օղակներից մեկի կողմից տեղեկատվության շահարկումը կամ տվյալների արտահոսքը կարող է լուրջ վնաս հասցնել մյուս շահառու կողմին: Բնական է, որ տեխնոլոգիական աճն ու տնտեսության մեջ դրանց կիրառումը անդառնալի գործընթացներ են, և դրանցից հրաժարվել այլևս անհնար է: Ուստի՝ առաջ է գալիս այս գործընթացները վերահսկելու, կառավարելի դարձնելու անհրաժեշտություն:

Աճող տվյալափեղք տնտեսություններում, որտեղ կազմակերպությունները տեղափոխում են իրենց ողջ գործունեությունը ամպային պահեստներ¹ և օգտագործում են տվյալների ողջ ներուժը, առաջ է գալիս մի պարզ դիմեմա. ինչպե՞ս է հնարավոր համագործակցել, զարգանալ և նորարարություններ մտցնել գլոբալ թվային շուկայում, միևնույն ժամանակ համապատասխանել նոր և անընդհատ փոփոխվող կարգավորումներին: Նման գործընթացների ֆոնին թվային ինքնիշխանությունը ձեռք է բերում մեծ կարևորություն: Փաստացի թվային ինքնիշխանության գաղափարը, դրան առնչվող տվյալների ինքնիշխանության գաղափարը և ինքնիշխան ամպի հասկացությունը բավական ժամանակ է, ինչ գոյություն ունեն: Այնուամենայնիվ նրանց ուսումնասիրման անհրաժեշտությունն աճել է այն բանի պատճառով, որ մեծացել է կիբերմիջավայրի անվտանգությանն ու գլոբալ քաղաքական իրադարձություններին մարտահրավեր նետող տվյալների բազան, ինչն էլ իր հերթին հանգեցրել է միջազգային կարգավորումների փոփոխման (Karlstad 3):

Թվային ինքնիշխանությունը յուրօրինակ ցուցիչ է, որը ցույց է տալիս թե պետությունը, կազմակերպությունը կամ անհատը որքանով է ունակ կառավարելու սեփական թվային տվյալները, ինչպես նաև վեր է հանում երրորդ կողմից կամ այլ պետությունից ունեցած տեղեկատվական-տեխնոլոգիական կախման աստիճանը:

Թվային ինքնիշխանությունը, որպես այդպիսին, համեմատաբար նոր եզրույթ է և ուսումնասիրության առարկա է դարձել վերջին տարիներին միայն: Այն հիմնականում ուսումնասիրվում է արևմտյան փորձագետների կողմից: Թվային ինքնիշխանության սահմանման հետ կապված մասնագիտական շրջանակներում տիրապետող է ընդհանուր մոտեցում, ըստ որի այն սահմանվում է որպես կարողություն՝ կառավարելու սեփական թվային դաշտը՝ տվյալները, ստեղծված և օգտագործվող ծրագրային ու տեխնիկական ապահովումները (Fleming 2025):

Վերջին տարիներին թվային տեխնոլոգիաների ընձեռած հնարավորությունների աճին զուգընթաց քաղաքական շրջանակներում աճել են թվային ինքնիշխանության հետ կապված մտահոգությունները: Մասնավորապես Եվրոպական Միությունը մեծ ուշադրություն է հատկացնում խնդրին և փորձում է գտնել օրենսդրական կարգավորումներ:

Եվրախորհրդարանի՝ 2020 թվականի «Դեպի առավել կայուն Եվրամիություն» զեկույցում նշվում է. «Կա աճող մտահոգություն, որ Եվրամիության քաղաքացիները, գործարար շրջանակները և անդամ պետություններն աստիճանաբար կորցնում են

¹ Ամպային պահեստը (Cloud Storage) տվյալների պահպանման ռեժիմ է, որում թվային տվյալները պահվում են սերվերների վրա, որոնք գտնվում են տվյալ վայրից դուրս: Սերվերները տրամադրվում են երրորդ կողմ հանդիսացող մատակարարի կողմից, որը պատասխանատու է իր ենթակառուցվածքում տվյալների ընդունման, կառավարման և անվտանգության համար: Մատակարարն ապահովում է սերվերների տվյալների մշտական հասանելիությունը հանրային կամ մասնավոր համացանցային կապի միջոցով, <https://cloud.google.com/learn/what-is-cloud-storage>: Մուկը՝ 25.09.2024:

վերահսկողությունն իրենց տվյալների, նորարարական գաղափարներ իրականացնելու ներուժի և թվային միջավայրում օրենսդրության ձևավորման և կիրարկման կարողության վրա: Այս ֆոնին ավելանում է նոր քաղաքականություն ստեղծելուն ուղղված աջակցությունը, որը պետք է նպաստի թվային դաշտում Եվրոպայի ռազմավարական ինքնավարության աճին: Դա Եվրամիությունից կպահանջի թարմացնել և ձևափոխել մի շարք գործող իրականական, կարգավորող և ֆինանսական գործիքակազմեր և ակտիվորեն խթանել եվրոպական արժեքներն ու սկզբունքները այնպիսի ոլորտներում, ինչպիսիք են տվյալների պաշտպանությունը, կիբեռանվտանգությունը և էթիկապես մշակված արհեստական բանականությունը» (Madigea 1):

Թվային ինքնիշխանության մակարդակները

Թվային ինքնիշխանությանը հետամուտ լինող սուբյեկտ կարող են հանդիսանալ **պետությունները, կազմակերպությունները, անհատները**: Սակայն ինչպես տեսնում ենք վերը նշված օրինակում, Եվրոպական միությունը՝ որպես միջազգային կազմակերպություն, ևս մտահոգված է հենց Եվրոպական միության՝ որպես մի ամբողջի տեղեկատվական անվտանգության հարցերով: Չնայած ԵՄ անդամ մի շարք պետություններ, ինչպես օրինակ՝ Գերմանիան, Ֆրանսիան, անհատապես ջանքեր են գործադրում թվային ինքնիշխանության ամրապնդման ուղղությամբ, այնպես էլ ԵՄ-ն՝ որպես միջազգային վերաբերական կառույց, իր հերթին շահագրգռված է միասնական եվրոպական տարածքի թվային դաշտի անվտանգության ապահովմամբ: Այսպիսով՝ կարող ենք ավելացնել ևս մեկ մակարդակ թվային ինքնիշխանության շահառուների աղյուսակում:

Իհարկե, այս մակարդակները հաստատուն չեն և կարող են ավելանալ ենթամակարդակներ կամ նորերը, ինչպես օրինակ՝ տարածաշրջանային կամ դաշնայինը: Հոդվածը հիմնականում քննության է առնում թվային ինքնիշխանության պետական մակարդակը՝ վեր հանելով պետությունների առջև ծառացած մարտահրավերներն այս ոլորտում:

Անհատների մակարդակ

Անհատների մակարդակում թվային ինքնիշխանությունը մեծապես վերաբերում է տվյալների պաշտպանվածությանը և գաղտնիության քաղաքականությանը: Սոցիալական ցանցերի, թվային բազմապիսի հարթակների, այդ թվում՝ առևտրային, վճարային, ժամանցային և այլն, մեծ տարածում ձեռք բերելուն զուգընթաց անհատները մեծաքանակ տվյալներ են «ի պահ տալիս» տարբեր սերվերներում: Ճառայություն մատուցող կազմակերպությունները օգտատերերին պարտադիր տրամադրում են իրենց գաղտնիության քաղաքականությունը, որի՝ օգտատիրոջ կողմից հաստատման դեպքում միայն կազմակերպությունը հասանելիություն է ձեռք բերում տվյալներին և արտոնվում տնօրինել ըստ անհրաժեշտության, կարգավորումներում սահմանված կարգով: Ինքնին հասկանալի է, որ առանց իրավական կարգավորումների տվյալների պաշտպանության հարցը կմնար հայեցողական մակարդակի վրա և կհանգեցներ չարաշահումների: Այս առումով անհատների տվյալների պաշտպանությունը հսկայական կարևորություն է ձեռք բերում, որի շուրջ մշակվել ու մշակվում են մի շարք օրենսդրական ակտեր, ներդրվում են կարգավորումներ ինչպես կազմակերպությունների կողմից օրինական կերպով ձեռք բերված տվյալների պաշտպանության, այնպես էլ ցանցահեռություններից և ապօրինություններից պաշտպանության համար:

Այդպիսի կարգավորման վառ օրինակ է Եվրամիության «Տվյալների պաշտպանության ընդհանուր կանոնակարգը», առավել հայտնի՝ GDPR-ը, որը ցույց է տալիս, թե ինչպես է թվային ինքնիշխանությունը դրսևորվում առօրյա կյանքում: Այս ձգտում է միավորելու առցանց հարթակներում անձնական տվյալների պահպանման

առնչվող կանոններն ու կանոնակարգերը և խախտումների արձանագրման դեպքում կիրառվելիք պատժամիջոցները: Համաձայն GDPR-ի պայմանների՝ ցանկացած կազմակերպություն, անկախ նրանից, թե որտեղ է գտնվում, պարտավոր է պահպանել տվյալների կառավարման մի շարք կանոններ, եթե ցանկանում է գործ ունենալ ԵՄ անդամ հանդիսացող երկրների հաճախորդների հետ: Այս կարգավորումները անհատ քաղաքացիներին հնարավորություն են տալիս ավելի շատ վերահսկելու իրենց տվյալների օգտագործումը: Այն նախատեսում է մոտ 25 մլն եվրոյի հնարավոր տուգանք իրավախախտումների դեպքում (Fleming 2025):

Կազմակերպությունների մակարդակ

Կազմակերպությունների մակարդակում թերևս թվային ինքնիշխանությունը փոքր-ինչ այլ բան է ենթադրում: Այս դեպքում թվային ինքնիշխանությունը ներառում է հավաքագրված և մշակված տվյալների ամբողջական վերահսկողությունը, ինչպես նաև որոշումներ իրականացնելու անկախությունը այն հարցում, թե ով կարող է հասանելիություն ունենալ այդ տվյալներին: Այն նաև ընդգրկում է տեխնոլոգիական բաղադրիչները անկախ կերպով ստեղծելու, փոփոխելու, ղեկավարելու և ավելացնելու ընկերությունների հնարավորությունները:

Կազմակերպությունների համար թվային ինքնիշխանության պահպանումն ավելին է, քան պարզապես տվյալների թափանցիկության և անվտանգության ապահովումը: Այն վերաբերում է նաև ռիսկերի նվազեցմանը, հնարավոր խախտումների դեպքում կանոնակարգերին համապատասխան գործելուն և, որ ամենակարևորն է, հաճախորդների վստահության ձևավորմանը:

Արհեստական բանականության վրա հիմնված աշխարհում, որտեղ տվյալները գտնվում են ինտենսիվ հսկողության ներքո, թվային ինքնիշխանությունն այն է, ինչը դնում է կազմակերպություններին հաճախորդների վստահության պահպանի դերում (Pascucci, Parin 2024):

Պետական մակարդակ

Թվային ինքնիշխանության **պետական մակարդակը** ենթադրում է պետությունների կախվածության նվազեցում այլ պետություններից՝ սեփական տեղեկատվական տարածքը պաշտպանելու համատեքստում:

Պետության թվային ինքնիշխանության հայեցակարգը, որը ներառում է ներքին և արտաքին քաղաքականության մեջ թվային ոլորտում անկախություն, գլոբալ թվային փոխակերպումների դարաշրջանում դարձել է պետականության կարևորագույն ասպեկտ: Այն ցույց է տալիս թե երկրի ղեկավարությունը որքանով է իրավասու և ունակ իրականացնելու ազատ որոշումներ թվային տիրույթում, որոնք ազդում են քաղաքացիների և գործարար շրջանակների վրա: Թվային ինքնիշխանությունը հաճախ պետության ինքնիշխանության, անվտանգության և տնտեսական ներուժի չափման ցուցիչ է: Թվային ինքնիշխանության հայեցակարգը առավել կարևորվում է տվյալների արագ աճող քանակի, կիբեռանվտանգությանն առնչվող մարտահրավերների, գլոբալ քաղաքական ցնցումների և միջազգային կանոնակարգերի փոփոխությունների պայմաններում: Այն սերտորեն կապված է տվյալների ինքնիշխանության և ինքնիշխան ամպային տարածքի հետ: Այս համատեքստում կարևորվում են կանոնակարգերն ու այն դերակատարները, որոնք ի գործ են օգնելու պաշտպանելու տվյալները և ապահովելու պետական վերահսկողություն օգտագործվող տեխնոլոգիաների և ծառայությունների նկատմամբ (Saaida 1):

Վերը նշվածը ամենից առաջ ենթադրում է սեփական թվային տարածքը վերահսկելու պետությունների տեխնիկական կարողությունները: Որոշ պետություններ ունեն առավելություն այլ երկրների նկատմամբ թվային առումով, քանի որ վերահսկում են ինտերնետ-պրովայդերների, սերվերների, տվյալների փոխանցման միջոցներ: Մասնավորապես ԱՄՆ-ն հանդիսանում է ոչ միայն

համացանցի սպառող, այլև մատակարար ամբողջ աշխարհին, ուստի արդարացիորեն իրավունքն ունի կոչվելու հեգեմոն այդ առումով: Այս ամենը հաշվի առնելով՝ դժվար է պատկերացնել մի պետություն, որն ամբողջությամբ անկախ է թվային հարցերում:

Այլ երկրներից կախման աստիճանը հաշվի առնելով տեսաբաններն առանձնացնում են թվային ինքնիշխանության երեք մակարդակ¹

1. Կախման բարձր մակարդակ

- Ընտրության հնարավորության բացակայություն
- Ներկրման երկրներից կամ կորպորացիաների կողմից տվյալների վերահսկում
- Տվյալների անվտանգության հարցերում թափանցիկության պակաս

2. Կախման միջին մակարդակ

- Համագործակցություն գործընկերների հետ
- Երկկողմ կամ բազմակողմ մուտքի թույլտվություն տվյալներին
- Ստանդարտների կիրառում կողմերի համար
- Հոսսայի պայմանագրեր

3. Թվային ինքնիշխանություն

- Տվյալների ամբողջական վերահսկողություն
- Տվյալների ինքնուրույն տնօրինում
- Բաց, փաստաթղթավորված ստանդարտների կիրառում

Թվային ինքնիշխանության առկայությունից խոսելու համար անհրաժեշտ է հաշվի առնել մի շարք գործոններ, այդ թվում՝

- Տվյալների տեղակայման վայրը (այն սերվերները, որտեղ տվյալները պահուստավորվում և մշակվում են, արդյո՞ք ֆիզիկապես գտնվում են տվյալ երկրում):
- Տվյալների ինքնիշխանությունը (արդյո՞ք տվյալները համապատասխանում են տվյալ երկրի գաղտնիության և ամբողջականության օրենքներին ու նորմերին):
- Իրավական վերահսկողությունը (արդյո՞ք տվյալները այդ պետության վերահսկողության տակ են և չեն վերահսկվում այլ երկրի կողմից) (Karsted 9):

Այլ կերպ ասած՝ թվային ինքնիշխանությունը իրենից ենթադրում է պետությունների կողմից տեխնոլոգիաների և դրանց ընձեռած ծառայությունների վրա պետության վերահսկողություն՝ նպատակ ունենալով պաշտպանելու խոցելի տվյալները և հնարավորություն ընձեռելու գործարար շրջանակներին, ընկերություններին և անհատներին՝ օգտվելու իրենց թվային ակտիվների և տվյալների վրա ունեցած ինքնավարությունից: Պարզ ասած, այն վերահսկողությունն է, թե որտեղ են տվյալները պահուստավորվում, որտեղ են հոսում, և ով կարող է տնօրինել դրանք (Karsted 3):

Իսկ «ինչպե՞ս է հնարավոր հասնել թվային ինքնիշխանության» հարցի հիմնական պատասխանը **ինքնիշխան ամպային տարածքն** է (Sovereign Cloud):

«Ինքնիշխան ամպ» հասկացությունը

Ինքնիշխան ամպը թվային ինքնիշխանության գլխավոր երաշխավորն է: Այն իրենից ենթադրում է նոր և դինամիկ կերպով համակցվող ու բազմակողմ ամպային լուծումներ, որոնք նախագծված են ի պատասխան այն նոր կանոնակարգերին, որոնք մեծացնում են ինքնիշխանությունը՝ ապահովելով գործընթացներին

¹ Այս դասակարգումը կիրառելի է նաև թվային ինքնիշխանության մյուս մակարդակների դեպքում:

համապատասխանությունը և համատեղելով պատկերացումները, նորարարությունը, անը և անվտանգությունը (Karsted 10):

Ինքնիշխան ամպը մի միջավայր է, որը օգնում է կազմակերպություններին հոգալ իրենց թվային պահանջները: Օգտագործելով ինքնիշխանություն ունենալու միջոցները՝ կազմակերպությունները (ինչպես նաև պետությունները) ձգտում են պաշտպանելու անհատների մասին տեղեկատվությունը (այդ շրջանակը ավելի լայն է. այն ներառում է մտավոր սեփականությունը, ծրագրային ապահովումները, գործարարության մեթոդները, ֆինանսական տվյալները, տեղեկատվական տեխնոլոգիաների ենթակառուցվածքի մասին տեղեկություններ և անգամ մետադատան¹) (Karsted 10):

Ինքնիշխան ամպը կարող է նաև կազմաձևվել որպես ամպանման ծրագրային հավելված մեծ կազմակերպությունների տեղեկատվական կենտրոնում. հավելվածը գործում է ամպային միջավայրի նման և պահպանվում է ամպային ծառայության մատակարարի կողմից, սակայն այն ֆիզիկապես մեկուսացված է արտաքին աշխարհից:

Ամպային միջավայրի մասին խոսելիս պետք է հաշվի առնել հետևյալ գործոնները՝

1. Ամպային ինքնիշխանության համար կարող է մարտահրավեր հանդիսանալ բոլոր կանոնակարգերին տիրապետող մատակարար գտնելը, որը կարող է օգնել պաշտպանության անհրաժեշտ մակարդակը գտնելու հարցում և ունի համապատասխան հավաստագրերն ու պահանջներին համապատասխան իրավաբանական անձեր:

2. Ինքնիշխան ամպերը հիմնականում միացած են համացանցին և մուտք են գործվում անվտանգ, գաղտնագրված հղումներով և ընթացակարգերով: Որոշ դեպքերում կարող է պահանջվել բաց օդային համացանց:

Ամփոփելով նշենք, որ ստուգելու համար՝ արդյո՞ք ամպային միջավայրը անվտանգ է, պետք է տալ հետևյալ հարցերը.

- Ո՞վ է տնօրինում ողջ ծրագրային ապահովումը:
- Ի՞նչ է տեղի ունենում ընկերության կամ պետության տվյալների հետ:
- Որտե՞ղ են ամբարված տվյալները (տվյալների ռեզիդենտությունը):
- Ո՞վ է մշակում այդ տվյալները:
- Ինչպե՞ս է տեղի ունենում համագործակցությունը:
- Կա՞մ բոլոր անհրաժեշտ կանոնակարգերին ու օրենքներին համապատասխանեցում:

Ենթադրվում է, որ կմեծանան թվային ինքնիշխանությանն առնչվող օրենքների ու կարգավորումների քանակն ու բարդությունը, ինչպես նաև կիստանան ֆինանսական և քրեական տույժերը՝ ընթացակարգերին համապատասխանության ստուգումները (աուդիտ) ձախողելու կամ տվյալների արտահոսքի դեպքում (Zeichick 2023):

Թվային ինքնիշխանության գլոբալ մոտեցումները

Ոչ եվրոպական տարածքում թվային ինքնիշխանության պահանջները այլ կերպ են արձագանք գտնում: Օրինակ՝ ԱՄՆ-ը անհանգստացած է այլ երկրների, այդ թվում եվրոպական երկրների, ոլորտը կարգավորելու վերաբերյալ ինչեցրած պահանջներով: ԱՄՆ-ը (բացառությամբ Թրամփի վարչակարգի պաշտոնավարման շրջանի) միշտ ունեցել է նվազագույն պետական միջամտություն, բաց ստանդարտներ, միջազգային

¹ Հիմնական տեղեկատվությունը պահվող տվյալների մասին, որը կարող է հեշտացնել անհրաժեշտ տվյալների որոնումը: Այլ կերպ ասած՝ մետադատան պարունակում է որոնվող տվյալների բնութագրիչներ (ստեղծման ամսաթիվ, չափը, փոփոխման տարեթիվը և այլն), որոնք հեշտացնում են որոնվող տվյալների նույնականացումը, <https://www.techtarget.com/whatis/definition/metadata>: Մուտք՝ 13.09.2024:

փոխգործակցություն և հնարավորինս մեծ տնտեսական ազատություն: Ըստ ԱՄՆ տեսակետի՝ թվային ինքնիշխանությանն ուղղված պահանջները հանդիսանում են որպես հարձակում՝ ամերիկյան խոշոր կորպորացիաների շուկայական հզորության վրա, ինչպիսիք Meta-ն ու Alphabet-ն են:

Այլ՝ ոչ եվրոպական երկրների համար թվային ինքնիշխանությունը սովորաբար նշանակում է թվային, տնտեսական և առաջին հերթին անխորհրդատ անվտանգային քաղաքականություն իրականացնելու հնարավորություն՝ հիմնականում ուղղված ինքնիշխանությանը: Պետականակենտրոն «Համացանցային ինքնիշխանության» հասկացությունը առաջացել է Չինաստանում, որը, օրինակ, ներառում է պետության կողմից համացանցին առնչվող կարգավորումների վերահսկողությունը, ինչպես նաև վերահսկողությունը իր քաղաքացիների տվյալների նկատմամբ:

Չնայած Չինաստանի ջանքերը՝ տարածելու թվային ինքնիշխանության վերաբերյալ իր ընկալումները, միջազգային մակարդակում ընդունելի չեն, բայց տեղական տվյալների պահուստավորման (local data storage) մասին կոնցեպտը հարուցել է միջազգային հանրության հետաքրքրությունը: Այն խրախուսում է տվյալների պահուստավորումը այն երկրում, որտեղ դրանք ստեղծվել են:

Շատ աֆրիկյան երկրներ ավելի ու ավելի են դիրքավորվում թվային ինքնիշխանության պետականակենտրոն ընկալման օգտին: Տեղական պահեստավորման չինական գաղափարը ողջունվում է նաև աֆրիկյան շատ երկրներում: Պետության ղեկավարներին, ի թիվս այլ բաների, օգտակար է թվում պետականաշինությունը առաջ տանելը և, իհարկե, առաջին հայացքից այն թվում է հակազդողության մոդել (Schibler 2023):

Թվային ինքնիշխանության հասնելու հնարավորությունները

Հնարավոր է արդյոք ունենալ լիակատար թվային ինքնիշխանություն: Ինչպես արդեն նշվեց, թվային ինքնիշխանության հիմնական երաշխավորը ինքնիշխան ամպն է: Սակայն որքանով է ինքնիշխան ամպը «ինքնիշխան»: Մի շարք երկրներ, այդ թվում Գերմանիան, Միացյալ Թագավորությունը, Ճապոնիան քայլեր են ձեռնարկում սեփական սուվերեն ամպը ունենալու ուղղությամբ: Մասնավորապես՝ Գերմանիան արդեն ստեղծել է իր ամպային տարածքը, որի սերվերները և տվյալների կենտրոնը, որոնք «հյուրընկալում» են սուվերեն ամպը, տեղակայված են Գերմանիայում: Այս ամենը պետք է գործեն Գերմանիայի օրենսդրության շրջանակներում՝ ապահովելով այնտեղ պահուստավորված տվյալների ենթակայությունը գերմանական օրենսդրությանն ու իրավունքին՝ խստիվ արգելելով դրանց արտահոսքը առանց հատուկ թույլտվության կամ դեպի տվյալները չարտոնված մուտքը: Սակայն, երբ դիտարկում ենք այն կորպորացիաները, որոնց սերվերները ծառայում են նշված տեղական ինքնիշխան ամպերի բազային, նկատում ենք, որ բոլորը պատկանում են բացառապես ամերիկյան վերազգային կորպորացիաների¹: Թեև բոլոր ամպային սերվերները տեղակայված են համապատասխան երկրներում, բայց բոլորը պատկանում են այնպիսի ընկերությունների, որոնց իրավաբանական հասցեն գտնվում է ԱՄՆ-ում: Այս ամենը սուվերեն ամպի հասկացությունը դարձնում է հարաբերական, քանի որ, չնայած տեղակայման վայրին և օրենսդրական մի շարք կազմավորումների, սերվերների սեփականատերը հանդիսանում է մեկ այլ երկիր: Սա առաջ է բերում մի շարք մարտահրավերներ, այդ թվում իրավաբանական (օրինակ՝ CLOUD Act-ը (որը թույլ է տալիս ԱՄՆ կառավարությանը հասանելիություն ունենալ ԱՄՆ ընկերությունների կողմից պահուստավորված տեղեկատվությանը՝ անգամ

¹ Օրինակ՝ Գերմանիան օգտագործում է հետևյալ ամպերը՝ Microsoft Azure, Amazon Web Services (AWS), Google Cloud ամպային սերվերները: Նույնը գլոբալ սերվերներից են օգտվում Մեծ Բրիտանիան, Ավստրալիան, Ճապոնիան, Հնդկաստանը և բազմաթիվ մեծ ու փոքր երկրներ: <https://www.eccouncil.org/cybersecurity-exchange/cloud-security/biggest-cloud-service-providers/>: Մուտք՝ 14.11.2024:

արտերկրում), կառավարչական (անգամ արտերկրում տեղակայված լինելու դեպքում որոշ ծրագրային, տեխնիկական ապահովումներ կառավարվում են մատակարարի կողմից), արտատարածքային ազդեցության (երբ մատակարար երկրի օրենսդրությունը հակասության մեջ է մտնում տեղակայման երկրի օրենսդրության հետ) և այլն:

Այնուամենայնիվ, կան մի շարք միջոցառումներ, որոնց իրականացումը թույլ կտա ունենալ թվային ինքնիշխանության աճ և ԱՄՆ հնարավոր ազդեցության նվազում: Որոշ երկրներ, օրինակ՝ Ֆրանսիան, քայլեր են ձեռնարկում ստեղծելու սեփական ամպային մատակարարներին: Նշվածի դրսևորումներից է կառավարությանը պատկանող ամպի ստեղծումը, որը կղեկավարվի ուղղակիորեն տվյալ երկրի կառավարության կողմից՝ երաշխավորելով ինքնիշխան պետության կողմից տվյալների ամբողջական տիրապետումը:

Ներկայումս առավել գործուն է հիբրիդային ինքնիշխան ամպի մոդելը, երբ տեղի է ունենում գլոբալ և տեղային համագործակցություն, և որտեղ տեղային գործընկերը («հյուրընկալող» երկիրը) մեծ վերահսկողություն է ունենում ենթակառուցվածքի և տվյալների վրա: Նաև կիրառելի է ապակենտրոն և բաց ամպային լուծումը, երբ տվյալները չեն կենտրոնացվում մի կորպորացիայի կամ մատակարարի առաջարկած ամպային սերվերներում և օգտագործվում են նաև պահուստավորման այլ բաց աղբյուրներ, ինչպես օրինակ՝ OpenStack-ը, CloudStack-ը, Eucalyptus-ը, Nextcloud-ը, SovereignCloudStack-ը և այլք:

Դե, իսկ կարևորագույն գործոններից մեկը թվային ինքնիշխանության հարցում մնում է օրենսդրական և պայմանագրային կարգավորումը: Պետությունները համապատասխան պայմանագրային բազա ունենալու դեպքում կարող են պատշաճ կերպով պաշտպանել սեփական ամպային տարածքը: Դրան է միտված ԵՄ երկրների կողմից ստեղծված GAIA-X նախաձեռնությունը¹, որի նպատակն է ստեղծել անվտանգ տվյալային ենթակառուցվածք Եվրոպայում, զարգացնել վստահելի հարթակ ամպային մատակարարների համար՝ որպես այլընտրանք ամերիկյան պրովայդերներին: Այս համատեքստում այնպիսի արժեքները, ինչպիսիք են գաղտնիությունը, տվյալների պաշտպանությունը, վստահելիությունը և թափանցիկությունը, գտնվում են առաջին շարքում (Schibler 2023):

Ինչ վերաբերում է Հայաստանին, ապա թվային ինքնիշխանությունը որպես երևույթ դեռևս ճանաչում չի գտել: Թվային դաշտում Հայաստանի Հանրապետության առաջ դրված խնդիրները հիմնականում վերաբերում են տեղեկատվական դիմակայությանն ու կիբերանվտանգությանը, և որոշակի ջանքեր արվում են այս ոլորտներում երկրի կայունությունն ապահովելու համար: Թվային սուվերենության առումով Հայաստանը և տարածաշրջանը լուրջ մարտահրավերների առաջ են կանգնած: Մի կողմ դնելով սեփական սերվերների և ամպերի բացակայությունը՝ լուրջ հարց է ինտերնետի մատակարարման հարցը: Հայաստանի ինտերնետային մատակարարները ինտերնետ ստանում են Վրաստանից, մեկ կապուղու միջոցով, որի խաթարումը կարող է ողջ պետությանը գրեթե ամբողջապես զրկել համացանցից: Նմանատիպ դեպք գրանցվեց 2024 թվականի փետրվարին, երբ, այդ համացանցային «թունելի» աշխատանքների խաթարումով պայմանավորված, խաթարվեց համացանցի աշխատանքը ողջ Հայաստանում, և տեղական ինտերնետ-մատակարարները ի գործ չէին պատշաճ կապով ապահովելու թե՛ կորպորատիվ, թե՛ անհատ սպառողներին: Նման դեպքերից խուսափելու համար անհրաժեշտ է քայլեր ձեռնարկել համացանցային մատակարարների, ինչպես նաև աղբյուրների

¹ Gaia-X ծրագիրը միտված է բիզնեսի, գիտության, քաղաքականության ներկայացուցիչների միջոցով միջազգային մակարդակում Եվրոպայում տվյալային ենթակառուցվածքի զարգացմանն ուղղված կայուն ներդրումների զարգացմանը, <https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html>: Մուտք՝ 23.07.2024:

դիվերսիֆիկացման ուղղությամբ: Որպես կաբելային համացանցի այլընտրանք կարելի է դիտարկել արբանյակային համացանցը:

Եզրահանգումներ

Ամփոփելով հոդվածը՝ կարող ենք ներկայացնել հետևյալ հիմնական եզրահանգումները.

- Թվային ինքնիշխանությունը աստիճանաբար դառնում է պետական ինքնիշխանության կարևորագույն ատրիբուտներից մեկը:

- Պետությունները հսկայական ջանքեր են գործադրում՝ ուղղված թվային ինքնիշխանության մակարդակի մեծացմանն ու ամրապնդմանը:

- Թեև կան մի շարք մեխանիզմներ, որոնք ուղղված են թվային ինքնիշխանությունն ամրապնդելուն, այնուամենայնիվ այդ ուղին զերծ չէ մարտահրավերներից ու խոչընդոտներից: Այդ մարտահրավերներից հիմնականը մեկ երկրի կորպորացիաների արտադրանքից կախում ունենալն է: Ներկայումս շատ պետություններ մշակում են թվային ինքնիշխանության հասնելու իրենց ուղին: Այդ ճանապարհին շատ կարևոր է իրավապայմանագրային պատշաճ բազայի ստեղծումը, դիվերսիֆիկացված ամպային տարածքից օգտվելը, ենթակառուցվածքի պատշաճ տեխնիկական ապահովումը:

- Հայաստանի Հանրապետության դեպքում թվային ինքնիշխանության հասնելու ուղղությամբ ջանքերը դեռևս գտնվում են սաղմնային փուլում, և պահանջվում է լուրջ աշխատանք նախ՝ համացանցային կապուղիների ամրապնդման, այնուհետև՝ այլ երկրներից թվային կախումը նվազեցնելու ուղղությամբ:

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. Clancy, Ryan. *AWS, GCP and Azure: The 3 Biggest Cloud Service Providers in 2025*. <https://www.eccouncil.org/cybersecurity-exchange/cloud-security/biggest-cloud-service-providers/>. Accessed: 14.11.2024.

2. Fleming, Sean. *What is Digital Sovereignty and why is Europe so Interested in it?*. Weforum, <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>. Accessed: 13.05.2024.

3. Karlstad, Wenche. *Digital Sovereignty. Adapting to Challenging Digital Landscape*. 2023, tech-services-digital-sovereignty-whitepaper-v1-2023.pdf. Accessed: 07.02.2025.

4. Kranz, Garry. *Metadata*. 2021, <https://www.techtarget.com/whatis/definition/metadata>. Accessed: 13.09.2024.

5. Madigea, Tambiama. *Digital Sovereignty for Europe, EPRS Ideas Paper, Towards a more resilient EU*. Page 1. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf). Accessed: 07.02.2025.

6. Pascucci, Marg; Parin, Matthew. *Customer Trust Is Everything — Here's How to Protect It with Digital Sovereignty*. 2024, <https://www.salesforce.com/blog/digital-sovereignty/>. Accessed: 17.07.2024.

7. Saaida, Mohammed. *Digital Sovereignty*. Page 1, 2024, https://www.researchgate.net/publication/377019471_Digital_Sovereignty. Accessed: 21.08.2024.

8. Schibler, Antoine. *Digital Sovereignty – An International and Individual Policy Challenge*. 2023, <https://www.bmz-digital.global/en/digital-sovereignty-an-international-and-individual-policy-challenge/>. Accessed: 13.09.2024.
9. “What is Cloud Storage?”. Cloud.google.com, <https://cloud.google.com/learn/what-is-cloud-storage>. Accessed: 25.09.2024.
10. Zeichick, Alan. *What Is a Sovereign Cloud? Why Is It Important?* Oracle, <https://www.oracle.com/cloud/sovereign-cloud/what-is-sovereign-cloud/>. Accessed: 13.09.2024.
11. “Das Gaia-X Ökosystem - Souveräne Dateninfrastruktur für Europa”. Bmwk, <https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html>. Accessed: 23.07.2024.

THE ISSUE OF DIGITAL SOVEREIGNTY IN A GLOBALIZING WORLD

ANNA SISOYAN

*Yerevan State University,
Department of International Relations,
Chair of Political Science, Ph.D. Student,
Yerevan, the Republic of Armenia*

The main goal of the article is to identify possible ways to increase digital sovereignty, based on an analysis of the experience of the European Union and its member states.

To achieve this goal, we have set the following tasks: to analyze the content of the concept of “digital sovereignty”, its essence and definitions, to study the main components of digital sovereignty and clarify their interrelationships, to identify the main prerequisites for the formation and strengthening of digital sovereignty, including the role of technological independence, data control and legal regulatory mechanisms, to highlight the problems and challenges that may hinder the path to achieving digital sovereignty.

The article presents a comparative analysis of the levels and degrees of digital sovereignty, which allows us to clearly assess the positions of different countries and the strategies they use. The analysis identifies the main problems in the field, as well as proposes mechanisms and practical solutions that can contribute to increasing digital sovereignty.

The conclusion drawn during the research shows that even technologically advanced countries face challenges on the way to ensuring digital sovereignty. The conclusion also emphasizes that in the conditions of rapid development of information technologies, digital sovereignty is becoming an integral part of state sovereignty. In this regard, policies and measures aimed at protecting the digital domain are of paramount importance, as global interconnectedness also carries risks of loss of sovereignty.

Key words: *digital sovereignty, digital domain, data sovereignty, sovereign cloud, cloud storage, internet, data residency.*

ПРОБЛЕМА ЦИФРОВОГО СУВЕРЕНИТЕТА В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ МИРА

АННА СИСОЯН

*соискатель кафедры политологии
факультета международных отношений
Ереванского государственного университета,
г. Ереван, Республика Армения*

Основная цель статьи — выявить возможные пути повышения цифрового суверенитета, основываясь на анализе опыта Европейского союза и его государств-членов.

Для достижения этой цели нами были поставлены следующие задачи: проанализировать содержание понятия «цифровой суверенитет», его сущность и определения, изучить основные компоненты цифрового суверенитета и выяснить их взаимосвязь, выявить основные предпосылки формирования и укрепления цифрового суверенитета, включая роль технологической независимости, контроля данных и правовых механизмов регулирования, выделить проблемы и вызовы, которые могут препятствовать достижению цифрового суверенитета.

В статье представлен сравнительный анализ уровней и степеней цифрового суверенитета, позволяющий наглядно оценить позиции разных стран и применяемые ими стратегии. Анализ выявляет основные проблемы в секторе, а также предлагает механизмы и практические решения, которые могут способствовать повышению цифрового суверенитета.

Вывод, сделанный в ходе исследования, показывает, что даже технологически развитые страны сталкиваются с трудностями на пути обеспечения цифрового суверенитета. В заключении также подчеркивается, что в условиях стремительного развития информационных технологий цифровой суверенитет становится неотъемлемой частью государственного суверенитета. В этой связи политика и меры, направленные на защиту цифровой сферы, имеют первостепенное значение, поскольку глобальная взаимосвязанность также несет в себе риски потери суверенитета.

Ключевые слова: *цифровой суверенитет, цифровой домен, суверенитет данных, суверенное облако, облачное хранилище, интернет, резидентность данных.*