Հոդվածի հղումը. Ղազարյան Ա., Արտաշյան Ա., Թումանյան Ա., Կեսոյան Ն., Կիրակոսյան Կ. (2025), Տեղեկատվական և կիբեռանվտանգության գլոբալ մարտահրավերները և Հայաստանի դիրքը միջազգային համատեքստում, *Տնտեսություն և հասարակություն, ՀՊՏՀ, Տնտեսագետ*, 2(8), 168-193, DOI: 10.52174/29538114_2025.2-168
Ներկայացվել է խմբագրություն՝16.10.2025 թ.
Ուղարկվել է գրախոսության՝16.10.2025 թ.
Երաշխավորվել է հրապարակման՝ 29.12.2025 թ.

ԱՐՄԵՆ ՂԱԶԱՐՅԱՆ
ՀՊՏՀ տեղեկատվական համակարգերի և տեղեկատվական տեխնոլոգիաների բիզնեսի ամբիոնի վարիչ, տնտեսագիտության թեկնածու
https://orcid.org/0000-0001-6083-5489

ԱՐԳԱՄ ԱՐՏԱՇՅԱՆ
ՀՊՏՀ տեղեկատվական համակարգերի և տեղեկատվական տեխնոլոգիաների բիզնեսի ամբիոնի դոցենտ, տնտեսագիտության թեկնածու
https://orcid.org/0000-0002-4550-3491

ԱՆՈՒՇ ԹՈՒՄԱՆՅԱՆ
ՀՊՏՀ տեղեկատվական համակարգերի և տեղեկատվական տեխնոլոգիաների բիզնեսի ամբիոնի դոցենտ, տնտեսագիտության թեկնածու
https://orcid.org/0000-0001-8626-0310

ՆԱՐԵԿ ԿԵՍՈՅԱՆ
ՀՊՏՀ ակտուարական և ֆինանսական մաթեմատիկայի ամբիոնի դոցենտ, տնտեսագիտության թեկնածու
https://orcid.org/0000-0001-7751-3726

ԿԱՏՅԱ ԿԻՐԱԿՈՍՅԱՆ
ՀՊՏՀ տեղեկատվական համակարգերի և տեղեկատվական տեխնոլոգիաների բիզնեսի ամբիոնի մագիստրանտ
https://orcid.org/0009-0008-5240-1531

ՏԵՂԵԿԱՏՎԱԿԱՆ ԵՎ ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԳԼՈԲԱԼ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ԵՎ ՀԱՅԱՍՏԱՆԻ ԴԻՐՔԸ ՄԻՋԱԶԳԱՅԻՆ ՀԱՄԱՏԵՔՍՏՈՒՄ

Տնտեսության կայուն զարգացման և ազգային անվտանգության ապահովման կարևորագույն նախապայմաններից են տեղեկատվական անվտանգությունն ու կիբեռանվտանգությունը: Աշխարհում ձևավորված թվային իրականությունը, որն աչքի է ընկնում մեծածավալ տվյալների շրջանառությամբ, համացանցի գլոբալ հասանելիությամբ

և նորարարական տեխնոլոգիաների լայն կիրառությամբ, ստեղծում է ինչպես զարգացման նոր հնարավորություններ, այնպես էլ լուրջ սպառնալիքներ: Այս պայմաններում տեղեկատվական անվտանգության ապահովումը Հայաստանի Կառավարության առաջնահերթություններից պետք է լինի, քանի որ այն անմիջականորեն կապված է երկրի տնտեսական կայունության, պետական կառավարման արդյունավետության և քաղաքացիների կյանքի որակի բարելավման հետ:

Տեղեկատվական անվտանգության ներկայիս վիճակի համակողմանի վերլուծությունը ցույց է տալիս, որ Հայաստանը շարունակում է մնալ խոցելի՝ հատկապես կազմակերպչական և ինստիտուցիոնալ կարողությունների առումով: Թեև իրավական դաշտում նկատվում է որոշակի առաջընթաց, սակայն ինքնաբավության մակարդակը դեռևս ցածր է. երկրի թվային ենթակառուցվածքները զգալիորեն կախված են արտաքին գործոններից, իսկ ներմուծումից կախվածությունը մեծացնում է կիբեռռիսկերի հավանականությունը:

Սույն հոդվածի շրջանակում փորձ է արվել ուսումնասիրելու Հայաստանի կիբեռանվտանգության համակարգի կազմակերպական, իրավական և տեխնիկական հիմքերը, վերլուծելու միջազգային համեմատություններում երկրի դիրքը, ինչպես նաև գնահատելու ներմուծումից կախվածության հետևանքները և հնարավոր ռիսկերը: Վերլուծության արդյունքները վկայում են, որ կիբեռանվտանգության հիմնախնդիրների անտեսումը կարող է լրջագույն սպառնալիք դառնալ ինչպես պետական կառավարման համակարգի, այնպես էլ տնտեսության կայունության համար:

Այս առումով առաջնային կարևորություն ունի համապարփակ և կենսունակ քաղաքականության իրագործումը՝ ուղղված ոչ միայն պետական կառույցների, այլև մասնավոր հատվածի և հասարակության կիբեռանվտանգության մակարդակի բարձրացմանը: Նպատակային քաղաքականության իրականացումը պետք է ներառի միջազգային գործընկերների հետ համագործակցության խորացում, տեխնոլոգիական կախվածության նվազեցում և տեղական արտադրական ու կազմակերպական կարողությունների ընդլայնում, ինչը հիմք կստեղծի Հայաստանի թվային զարգացման անվտանգ ու կայուն ընթացքի համար:

Հիմնաբառեր: *կիբեռանվտանգություն, տեղեկատվական անվտանգություն, թվային զարգացում, ռիսկերի կառավարում, ինստիտուցիոնալ կարողություններ, ազգային անվտանգություն*

JEL: L86, O33
DOI: 10.52174/29538114_2025.2-168

Ներածություն: Տեղեկատվական տեխնոլոգիաների արագ զարգացումն ու թվայնացման խորացումը 21-րդ դարում արմատապես փոխել են անվտանգության ընկալումները: Եթե նախկինում ազգային անվտանգությունը դիտարկվում էր հիմնականում ռազմական և քաղաքական հարթության մեջ, ապա այսօր նույնքան կարևոր է նաև կիբեռանվտանգության ապահովումը: Կիբեռտարածքում իրականացվում են լրտեսական գործողություններ, ֆինանսական շահարկումներ, ինչպես նաև պետական ու մասնավոր ենթակառուցվածքների խափանման փորձեր: Վերջին տարիներին արձանագրված տվյալների արտահոսքերի և կիբեռհարձակումների աճը վկայում է, որ թվային միջավայրը դարձել է ոչ միայն զարգացման, այլև խոցելիության աղբյուր:

Հետազոտության նպատակն է բացահայտել տեղեկատվական անվտանգության և կիբեռանվտանգության ոլորտում գլոբալ և տարածաշրջանային միտումները, վերլուծել դրանց ազդեցությունը Հայաստանի վրա և առաջարկել զարգացման ռազմավարական ուղղություններ:

Միջազգային տվյալները ցույց են տալիս, որ կիբեռհարձակումների ֆինանսական հետևանքները շարունակ աճում են. 2024 թվականին տվյալների արտահոսքի միջին արժեքը կազմել է շուրջ 4.88 միլիոն ԱՄՆ դոլար: Առողջապահական և արդյունաբերական ոլորտները հայտնվել են առավել խոցելի դիրքում: Միևնույն ժամանակ, առաջատար երկրները՝ Ֆինլանդիան, Նորվեգիան, Դանիան և Մեծ Բրիտանիան, ապահովում են բարձր մակարդակի պաշտպանություն՝ համատեղելով օրենսդրական, տեխնիկական և կազմակերպչական միջոցառումները[1]:

Հայաստանը ևս կանգնած է համանման մարտահրավերների առաջ: Չնայած օրենսդրական դաշտում որոշակի առաջընթացին, կազմակերպչական թերություններն ու ինստիտուցիոնալ մեխանիզմների բացակայությունը խոչընդոտում են համակարգի կայուն զարգացումը: Գլոբալ կիբեռանվտանգության ինդեքսի տվյալներով Հայաստանը զիջում է տարածաշրջանի առաջատարներին՝ Թուրքիային, Ադրբեջանին և Վրաստանին:

Հետևաբար՝ անհրաժեշտ է վերլուծել Հայաստանի դիրքը միջազգային ինդեքսներում, գնահատել տվյալների արտահոսքերի ֆինանսական և կազմակերպչական հետևանքները, ուսումնասիրել օրենսդրական և ինստիտուցիոնալ համակարգերի արդյունավետությունը, ինչպես նաև հանրային և մասնավոր հատվածների համագործակցության մակարդակը: Այս հետազոտությունը միտված է ոչ միայն առկա խնդիրների բացահայտմանը, այլև դրանց գործնական լուծումների մշակմանը՝ հիմնված միջազգային լավագույն փորձի վրա և համահունչ Հայաստանի ազգային շահերին:

Գրականության ակնարկ: Վերջին տարիներին կիբեռանվտանգությունը դարձել է ոչ միայն տեխնիկական, այլև ռազմավարական և հասարակական կարևոր նշանակության ոլորտ: Այս թեմային անդրադարձել են բազմաթիվ հեղինակավոր հետազոտողներ:

Թոմաս Ջ. Մոուբրեյն իր «Կիբեռանվտանգության համակարգերի կառավարում, թեստավորում և ներխուժումների հետաքննություն» (2013) գրքում ընդգծում է կիբեռհարձակումների աշխարհագրական տարածման խնդիրը և միջազգային համագործակցության անհրաժեշտությունը: Հեղինակի կարծիքով փոքր և զարգացող երկրները հատկապես խոցելի են, քանի որ հաճախ չեն ունենում բավարար ռեսուրսներ կանխարգելիչ և արձագանքման համակարգեր ստեղծելու համար[2]:

Հիմմաթը, Իբրահիմը, Համմամը, Էլդիրդիերին և Ալգազոլին իրենց հոդվածում ընդգծում են կիբեռանվտանգության ընթացիկ միտումների, տեխնիկայի և մարտահրավերների կարևորությունը: Հեղինակների կարծիքով տեղեկատվական համակարգերի արագ զարգացումը ոչ միայն ստեղծում է նոր հնարավորություններ, այլև մեծացնում է անվտանգության խախտումների հավանականությունը, ինչը պահանջում է համալիր մոտեցումներ և ժամանակա-

[1] Տե՛ս IBM (2024), *Cost of a data breach report 2024*. IBM, https://www.ibm.com/reports/data-breach

[2] Տե՛ս **Mowbray T. J.** (2013), *Cybersecurity: Managing systems, conducting testing, and investigating intrusions* (1st ed.). Wiley, https://www.wiley.com/en-us/Cybersecurity%3A+Managing+Systems%2C+Conducting+Testing%2C+and+Investigating+Intrusions-p-9781118695066

կից լուծումներ[3]:

«Ռոբոտաշինություն և արհեստական բանականություն խելացի քաղաքներում կիբերանվտանգության և կարևորագույն ենթակառուցվածքների համար» գրքում ընդգծվում է, որ խելացի քաղաքների կայունությունն ու անվտանգությունը մեծապես կախված են արհեստական բանականության և կիբեռանվտանգության ու կարևոր ենթակառուցվածքների պաշտպանության ոլորտում ռոբոտատեխնիկայի կիրառությունից: Հեղինակների կարծիքով նորագույն տեխնոլոգիաների ինտեգրումը ոչ միայն ուժեղացնում է պաշտպանական մեխանիզմները, այլև հնարավորություն է տալիս կանխատեսելու ու նվազեցնելու զարգացող սպառնալիքների ազդեցությունը[4]:

Կադենան և Գուպին իրենց հոդվածում ընդգծում են մարդկային գործոնի կարևոր դերը կիբեռանվտանգությունում և դրա ազդեցությունը կազմակերպությունների անվտանգության մակարդակում: Հեղինակների կարծիքով աշխատակիցների թվային գրագիտության պակասը և մարդկային սխալները հաճախ դառնում են ամենաթույլ օղակը, ինչը սոցիալական ինժեներիայի միջոցով իրականացվող հարձակումների հնարավորություն է ստեղծում [5]:

Վերջապես, Սաիդը, Գուլը, Ալդոսսարին, Ալթամիմին, Ալշահրանին, Սաքիբը և Ալմուհաիդեբը իրենց հոդվածում ընդգծում են էներգետիկ ոլորտի թվայնափոխության ընթացքում առաջացող կիբեռանվտանգության մարտահրավերների և հետևանքների կարևորությունը: Հեղինակների կարծիքով նոր տեխնոլոգիաների ինտեգրումը չպատրաստված պաշտպանական համակարգերի հետ, կարող է բարձրացնել սառը և նպատակային հարձակումների ռիսկերը, ինչը պահանջում է համալիր ռազմավարական մոտեցումներ և ժամանակակից լուծումներ[6]:

Կիբեռանվտանգության ոլորտում Հայաստանի համատեքստի ուսումնասիրությունը հնարավոր չէ առանց տեղական մասնագետների կատարած գիտական և փորձագիտական վերլուծությունների: Վերջին տարիներին մի շարք հայ հետազոտողներ և կազմակերպություններ անդրադարձել են ազգային կիբեռանվտանգության համակարգում առկա բացերին, ինստիտուցիոնալ թերություններին և թվային ենթակառուցվածքների խոցելիությանը:

Հայաստանում կիբեռանվտանգության կառավարման ինստիտուցիոնալ խնդիրներին անդրադառնում է նաև DCAF-ի «Armenia Cybersecurity Governance Assessment» գնահատումը: Զեկույցում նշվում է, որ պետական կառավարման համակարգում գործող ինստիտուտները հաճախ ունենում են դերերի և պատասխանատվությունների ոչ հստակ բաժանում, ինչի հետևանքով առաջանում են կոորդինացիոն բացեր: Արձանագրվում է, որ տեղեկատվական և կիբեռանվտանգության ոլորտների քաղաքականությունը մի շարք

---

[3] Տե՛ս **Himmat M., Ibrahim M. A., Hammam N., Eldirdiery H. F., Algazoli G.** (2023), The current trends, techniques, and challenges of cybersecurity. *European Journal of Information Technologies and Computer Science, 3*(4), էջ 1–5, https://doi.org/10.24018/compute.2023.3.4.93

[4] Տե՛ս **Nedjah N., Abd El-Latif A. A., Gupta B. B., & Mourelle L. M. (Eds.)**, (2022), *Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities* (Vol. 1030). Springer Nature.

[5] Տե՛ս **Kadena E., Gupi M.** (2021), Human factors in cybersecurity: Risks and impacts. *Security science journal*, *2*(2), էջ 51-64, **DOI:** 10.1109/CIC48465.2019.00047

[6] Տե՛ս **Saeed S., Gull H., Aldossary M. M., Altamimi A. F., Alshahrani M. S., Saqib M., Zafar Iqbal S., Almuhaideb A. M.** (2024), Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications. *Information*, *15(12),* էջ 764, https://doi.org/10.3390/info15120764

դեպքերում չունի միասնական մոտեցում և ամբողջական կառավարման մեխանիզմ, ինչը սահմանափակում է պետական մարմինների արդյունավետ համագործակցությունն ու անվտանգության գործընթացների համակարգված իրականացումը[7]:

Հայաստանում e-governance-ի զարգացումը առաջ է բերում նոր մարտահրավերներ կիբեռանվտանգության ոլորտում՝ ինչպես տեխնիկական, այնպես էլ քաղաքական բնույթի: Հոդվածում ընդգծվում է, որ, առանց միասնական և հստակ մշակված պետական քաղաքականության, կիբեռանվտանգության կառավարման համակարգը կարող է լինել խոցելի և անարդյունավետ: Այս պնդումները կարևոր հենք են հետագա ուսումնասիրությունների և քաղաքական առաջարկությունների համար՝ նպատակ ունենալով բարելավելու տեղեկատվական անվտանգության ինստիտուցիոնալ կառավարման մեխանիզմները[8]:

2017 թ. «Ինտերնետի ազատությունը Հայաստանում և մարդու հիմնարար իրավունքների իրականացումը» զեկույցն անդրադառնում է Հայաստանում տեղեկատվական ազատությունների և անձնական տվյալների պաշտպանության իրավիճակին: Զեկույցում քննվում է, թե ինչպես տեղեկատվական ազատությունները (օրինակ՝ ինտերնետային բրաուզինգը և հաղորդակցությունը) համադրվում են ազգային և պետական անվտանգության պահանջների հետ, և ընդգծվում է՝ անհրաժեշտ է հավասարակշռել քաղաքացիների իրավունքները և պետության անվտանգության գործոնները: Այս ուսումնասիրությունը կարևոր հիմք է հետագա հետազոտությունների համար՝ երկրի թվային քաղաքականության և կիբեռանվտանգության կառավարման համատեքստում[9]:

Ներկայացված վերլուծությունը ընդգծում է, որ ինչպես միջազգային փորձը, այնպես էլ տեղական հետազոտությունները կարևոր ուղեցույց են Հայաստանի կիբեռանվտանգության զարգացման համար: Կադենայի և Գուպիի (2021) աշխատանքները ցույց են տալիս, որ մարդկային գործոնը, տեխնոլոգիական թուլությունները և նոր տեխնոլոգիաների ինտեգրման սխալ ռազմավարությունները կարող են բարձրացնել կազմակերպությունների և ոլորտների խոցելիության աստիճանը: Միաժամանակ, տեղական ուսումնասիրություններն ու զեկույցները, ներառյալ CyberHUB-AM (2023), DCAF (2020) և Սիսոյան (2020), փաստում են, որ Հայաստանի կիբեռանվտանգության կառավարման համակարգում առկա են ինստիտուցիոնալ բացեր, համակարգային թուլություններ և միասնական քաղաքականության բացակայություն:

Համադրված միջազգային և տեղական փորձը ցույց է տալիս, որ Հայաստանում անհրաժեշտ է համալիր ռազմավարություն՝ ներառելով տեխնիկական, քաղաքական և կրթական միջոցառումներ, բարձրացնելով աշխատակիցների թվային գրագիտությունը և ապահովելով կայուն ու անվտանգ թվա-

---

[7] Տե՛ս ***Spînu N.*** *(2020), Armenia cybersecurity governance assessment. Geneva Centre for Security Sector Governance (DCAF),* https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf

[8] Տե՛ս ***Sisoyan A.*** *(2020), New cybersecurity challenges: Digital transformation and the political implications of their implementation. Yerevan State University Journals*, https://journals.ysu.am/index.php/j-pol-sci/article/view/12695

[9] Media Initiatives. (2017), *Internet freedom in Armenia and execution of basic human rights*, https://mediainitiatives.am/wp-content/uploads/2018/03/Internet-Freedom-Research-Report-2017-in-English.pdf

յին միջավայր, հավասարակշռելով քաղաքացիների իրավունքները և պետական անվտանգության պահանջները:

Հետազոտության մեթոդաբանություն: Հետազոտության տեսական հիմքը կազմել են տեղեկատվական անվտանգության և կիբեռանվտանգության ոլորտում հայկական և արտասահմանյան հեղինակավոր մասնագետների մոտեցումները: Ուսումնասիրվել են նաև անվտանգության կառավարման, ռիսկերի նվազեցման և կիբեռհանցագործությունների կանխարգելման վերաբերյալ ժամանակակից դիտարկումները:

Հետազոտությունն իրականացվել է համակցված մեթոդաբանությամբ՝ ներառելով ինչպես քանակական, այնպես էլ որակական գործիքներ: Քանակական մոտեցմամբ ուսումնասիրվել են վիճակագրական տվյալներ՝ տվյալների արտահոսքի միջին արժեքներ, համաշխարհային ծախսեր տեղեկատվական անվտանգության ապահովման նպատակով, կիբեռանվտանգության գլոբալ և ազգային ինդեքսներ (GCI, NCSI): Որակական վերլուծության շրջանակում ուսումնասիրվել են միջազգային ստանդարտներ (ISO/IEC 27001, NIST CSF, ISA/IEC 62443, CIS Controls), ազգային քաղաքականություններ և փորձագիտական գնահատականներ: Այս համադրությունը թույլ է տվել ապահովել վերլուծության բազմակողմանիություն և նվազեցնել տվյալների հնարավոր թերությունները:

Տվյալների աղբյուրներն ընդգրկում են միջազգային կազմակերպությունների հաշվետվություններ (ITU, e-Governance Academy, IBM, Gartner), ազգային ռազմավարություններ և օրենսդրական փաստաթղթեր, ինչպես նաև մասնագիտական գրականություն և հետազոտական հոդվածներ: Վիճակագրական տվյալները հավաքագրվել են 2020–2025 թթ. ժամանակահատվածում՝ ապահովելով համեմատական և դինամիկ դիտարկում:

Վերլուծական մեթոդներից կիրառվել են. համեմատական վերլուծություն՝ երկրների և տարածաշրջանների կիբեռանվտանգության ցուցանիշների համադրությամբ, տնտեսական վերլուծություն՝ արտահոսքերի ֆինանսական հետևանքների հաշվարկով, ինչպես նաև ինդեքսային մեթոդաբանություն՝ GCI, NCSI և DDL ցուցանիշների համադրությամբ: Բացի դրանից, կատարվել է սցենարային վերլուծություն՝ Հայաստանի համար հնարավոր զարգացումների և քաղաքական ընտրությունների գնահատման նպատակով:

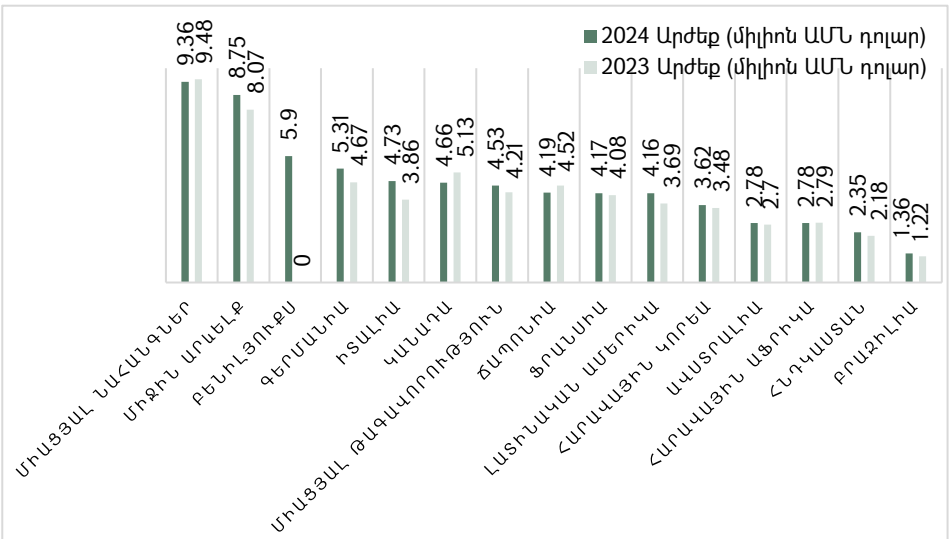
Հետազոտության հիմնական քայլերն են. տվյալների հավաքագրում և համակարգում, ցուցանիշների մշակում և գծապատկերների կազմում, Հայաստանի դիրքի գնահատում հարևան երկրների համատեքստում, օրենսդրական և կազմակերպչական միջավայրի վերլուծություն, ինչպես նաև գործնական առաջարկությունների մշակում:

Մեթոդաբանության սահմանափակումներն են տվյալների հասանելիության սահմանափակումները և որոշ ցուցանիշների հաշվարկման մեթոդաբանական տարբերությունները: Չնայած դրան՝ բազմաբնույթ աղբյուրների համադրումը ապահովում է բարձր վստահելիություն:

Ակնկալվում է, որ արդյունքները կօգնեն բացահայտել Հայաստանի ուժեղ և թույլ կողմերը, մատնանշել առաջնահերթ բարեփոխումները և ձևավորել ռազմավարական լուծումներ՝ համահունչ միջազգային լավագույն փորձին: Այս

մոտեցումը կարող է ծառայել որպես տեսական ու գործնական հիմք՝ պետական կառույցների, մասնավոր հատվածի և ակադեմիական համայնքի համագործակցության ամրապնդման համար:

Վերլուծություն: Տեղեկատվական անվտանգությունն ու կիբեռանվտանգությունը 21-րդ դարում դարձել են ազգային անվտանգության, տնտեսական կայունության և հասարակական վստահության հիմնական հենասյուները: Տեղեկատվական տեխնոլոգիաների արագ զարգացումն ու թվայնացման գործընթացների խորացումը, ինչպես նաև պետական և մասնավոր հատվածների թվային փոխազդեցության ակտիվացումը ստեղծել են նոր հնարավորություններ, բայց, միևնույն ժամանակ, բարձրացրել են ռիսկերի և սպառնալիքների մակարդակը: COVID-19 համավարակի սկզբից ի վեր կիբեռսպառնալիքների թիվը, տեղեկատվական անվտանգության գծով տնօրենների (CISO) գնահատմամբ, աճել է 72%-ով[10]: SS ոլորտի մասնագետների 61%-ը նույնպես նշում է, որ հեռավար աշխատանքը զգալիորեն մեծացնում է կիբեռանվտանգության խախտումների հավանականությունը: Կիբեռհանցագործությունների ֆինանսական հետևանքներից ամենամեծը տվյալների արտահոսքի ծախսերն են:



Գծապատկեր 1. ***Տվյալների արտահոսքի միջին ծախսերն ըստ երկրների/տարածաշրջանների, 2023–2024 թթ.***[11]

Արդյունաբերության ոլորտում արձանագրվել է ծախսերի ամենամեծ աճը՝ 830,000 ԱՄՆ դոլար: Այդպիսով՝ մեկ արտահոսքի միջին արժեքը հասել է 5.56 միլիոն ԱՄՆ դոլարի, ինչը 13%-ով գերազանցում է համաշխարհային միջին ցուցանիշը: Սա վկայում է թիրախային հարձակումների աճի և/կամ համակարգային խոցելիությունների առկայության մասին[12]:

---

[10] Տե՛ս Jobera. "Remote Work Cybersecurity Statistics." *Jobera.com*, https://jobera.com/remote-work-cybersecurity-statistics/

[11] Statista Market Insights (2024). Average cost of a data breach worldwide from March 2023 to February 2024, by country or region, https://www.statista.com/statistics/463714/cost-data-breach-by-country-or-region/

[12] Տե՛ս IBM Security // Cost of a Data Breach Report 2024 // IBM, 2024, https://www.ibm.com/reports/data-breach

Տվյալների արտահոսքի հետևանքների համակողմանի գնահատման համար անհրաժեշտ է հաշվի առնել նաև տարածաշրջանային առանձնահատկությունները: Տարբեր երկրներում կիբեռսպառնալիքների մակարդակը պայմանավորված է ոչ միայն տեղական օրենսդրությամբ, այլև տնտեսության կառուցվածքով և կիբեռհանցագործությունների զարգացման միտումներով:

Դիտարկվող ժամանակահատվածում Միացյալ Նահանգները եղել է առաջինը՝ ըստ տվյալների արտահոսքի ամենաբարձր միջին արժեքների: 2024 թվականին դրանք կազմել են մոտ 9.36 միլիոն ԱՄՆ դոլար, ինչը համեմատելի է 2023 թվականի 9.48 միլիոն ԱՄՆ դոլարի հետ: Այսպիսի կայուն բարձր ցուցանիշը կարող է բացատրվել ԱՄՆ-ի խիստ կարգավորող օրենսդրությամբ, ինչպես նաև անվտանգության միջադեպերի արձագանքման և դատական գործընթացների բարձր ծախսերով: Ուշագրավ է Միջին Արևելքի դիրքը, որտեղ տվյալների արտահոսքի միջին արժեքը 2023-ի 8.07 միլիոն ԱՄՆ դոլարից աճել է՝ հասնելով 8.75 միլիոն ԱՄՆ դոլարի՝ 2024 թվականին: Սա վկայում է տարածաշրջանում տեղի ունեցող նշանակալի փոփոխությունների մասին, որոնք պայմանավորված են թվային փոխակերպման արագացմամբ և կիբեռռիսկերի բարդությամբ:

Ցուցակում ընդգրկված եվրոպական երկրները ցույց են տալիս տարբեր միտումներ: Մինչ Գերմանիան (5.31 մլն ԱՄՆ դոլար) և Իտալիան (4.73 մլն ԱՄՆ դոլար) 2024 թվականին, 2023 թվականի համեմատությամբ, արձանագրել են աճ, Կանադան (4.66 մլն ԱՄՆ դոլար) և Ճապոնիան (4.19 մլն ԱՄՆ դոլար) գրանցել են որոշակի նվազում: Սա ցույց է տալիս, որ նույնիսկ զարգացած տնտեսություններում կիբեռանվտանգության մարտահրավերների կառավարումը բարդ և դինամիկ գործընթաց է, որի արդյունքները կարող են տարբերվել՝ կախված ազգային քաղաքականությունից և պաշտպանության մեխանիզմներից:

Հնդկաստանը և Բրազիլիան ունեն ամենացածր ցուցանիշները, համապատասխանաբար՝ 2.35 մլն և 1.36 մլն ԱՄՆ դոլար 2024 թվականին: Սակայն նրանց ցուցանիշները նույնպես աճել են 2023 թվականի համեմատությամբ: Սա վկայում է, որ կիբեռհանցագործությունների ազդեցությունը համաշխարհային բնույթ ունի և աստիճանաբար մեծանում է նաև զարգացող տնտեսություններում:

Ըստ 2024 թվականի «Կիբեռանվտանգության վերջնական գնահատական» զեկույցի՝ Ֆինլանդիան, Նորվեգիան, Դանիան, Ավստրալիան, Մեծ Բրիտանիան, Շվեդիան, Ավստրիան, Ճապոնիան, ԱՄՆ-ն և Կանադան կիբեռռիսկի ամենացածր մակարդակ ունեցող 10 երկրներն են (աղյուսակ 1)[13]:

[13] Տե՛ս Global Cybercrime Report 2024: Which Countries Face the Highest Risk? - MixMode AI, https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk/

Աղյուսակ 1

Կիբեռանվտանգության առաջատար երկրների վարկանիշը (2024 թ.)[14]

Դիրք	Երկիր	Կիբեռանվտանգության ազգային ինդեքս	Կիբեռանվտանգության խոցելիության ինդեքս	Կիբեռանվտանգության գլոբալ ինդեքս	Կիբեռդիմազկունության ինդեքս	Կիբեռանվտանգության վերջնական գնահատական
1	Ֆինլանդիա	86	89	96	94	93
2	Նորվեգիա	68	87	97	94	93
3	Դանիա	84	88	93	96	92
4	Ավստրալիա	66	87	97	86	90
5	Միացյալ Թագավորություն	90	79	100	90	90
6	Շվեդիա	84	79	95	95	90
7	Ավստրիա	86	84	94	91	90
8	Ճապոնիա	64	86	98	82	89
9	Միացյալ Նահանգներ	65	86	100	80	89
10	Կանադա	70	79	98	88	88

Ֆինլանդիա: Թեպետ Ֆինլանդիան ըստ կիբեռանվտանգության ազգային ինդեքսի (NCSI) գտնվում է 4-րդ հորիզոնականում, մյուս ցուցանիշներում, բարձր արդյունքների շնորհիվ, զբաղեցնում է առաջին տեղը համակցված՝ վերջնական գնահատականով (Cyber Safety Score)[15]: Այս դիրքը վկայում է երկրի համապարփակ և համակարգված մոտեցման մասին, որը ներառում է ռազմավարական պլանավորում, նորարարական ներդրումներ, ինչպես նաև ազգային և միջազգային մակարդակներում համագործակցության ամրապնդում:

Նորվեգիա: Նորվեգիան համարվում է Եվրոպայի և նույնիսկ աշխարհի առաջատարներից մեկը թվայնացման և կիբեռանվտանգության ոլորտներում: Տնտեսության թվային վերափոխման շրջանակում կիբեռանվտանգության շուկան ձևավորում է կարևոր ենթակառուցվածք՝ ապահովելով թվային միջավայրի պաշտպանությունը ինչպես պետական, այնպես էլ մասնավոր հատվածներում: Նորվեգիայի փորձն ապացուցում է, որ կիբեռանվտանգությունը պետք է դիտարկել ոչ միայն որպես տեխնոլոգիական, այլև ռազմավարական, սոցիալ-տնտեսական և կրթական հարթակ:

Չնայած երկրի կողմից ներդրված կառույցների կայունությանը և ռազմավարությունների շարունակական կատարելագործմանը՝ կիբեռհանցավորության ֆինանսական հետևանքները և աճող սպառնալիքները վկայում են, որ միայն պաշտպանական տեխնոլոգիաների զարգացումը բավարար չէ:

Դանիա: Վերջին տարիներին Դանիան զգալի առաջընթաց է գրանցել թվային ոլորտում, սակայն թվայնացման աճին զուգահեռ աճել են նաև կիբեռսպառնալիքները: Դանիայի կիբեռանվտանգության և տեղեկատվական անվտանգության կենտրոնի (Center for Cyber Security, CFCS) գնահատականնե-

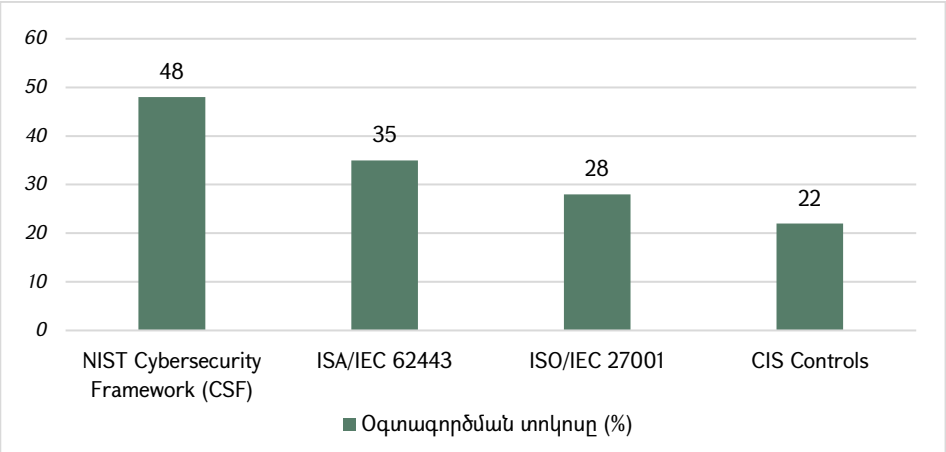
[14] MixMode (2024, June 12). *Global cybercrime report 2024: Which countries face the highest risk?* MixMode, https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk

[15] Տե՛ս NCSI. (2023). Finland – National Cyber Security Index, https://ncsi.ega.ee/country/fi/

րով՝ կիբեռսպառնալիքները ներկայումս դասակարգվում են հինգ հիմնական կատեգորիաների՝ կիբեռլրտեսություն, կիբեռհանցագործություն, կիբեռակտիվիզմ, վնասաբեր կիբեռհարձակումներ և կիբեռահաբեկչություն: Այս դասակարգման շրջանակում կիբեռլրտեսությունն ու կիբեռհանցագործությունը գնահատվում են որպես «շատ բարձր» մակարդակի սպառնալիքներ, ինչը մատնանշում է պետական կառույցների և կազմակերպված հանցախմբերի աճող ներգրավվածությունը Դանիայի կենսական ենթակառուցվածքների ու կազմակերպությունների վրա իրականացվող գործողություններում:

Այս երկրները ներկայացնում են տարբեր աշխարհաքաղաքական միջավայրեր և կիրառում են կիբեռանվտանգության տարբեր մոտեցումներ, այնուամենայնիվ, դրանց միավորում է մեկ ընդհանուր գիծ՝ թվային պաշտպանության հուսալի համակարգերի ձևավորման հանձնառությունը: Այս փորձը կարևոր դասեր է տալիս գլոբալ լավագույն փորձից:

Նման պայմաններում կիբեռանվտանգության ստանդարտացված շրջանակները դառնում են առանցքային գործիքներ՝ ամուր պաշտպանական համակարգեր կառուցելու, ռիսկերը կառավարելու և պետությունների ու կազմակերպությունների միջև փոխվստահություն հաստատելու համար: Դրանք համախմբում են լավագույն փորձը և առաջարկում միասնական մոտեցումներ, որոնք հնարավորություն են տալիս պաշտպանելու զգայուն տվյալները և նվազեցնելու կիբեռհարձակումների հետևանքները:



Գծապատկեր 2. ***Կիբեռանվտանգության առավել օգտագործվող ստանդարտների տոկոսային բաշխումը (2021)[16]***

Ըստ 2021 թվականի տվյալների[17]՝ առավել լայնորեն կիրառվող չորս ստանդարտներն են՝

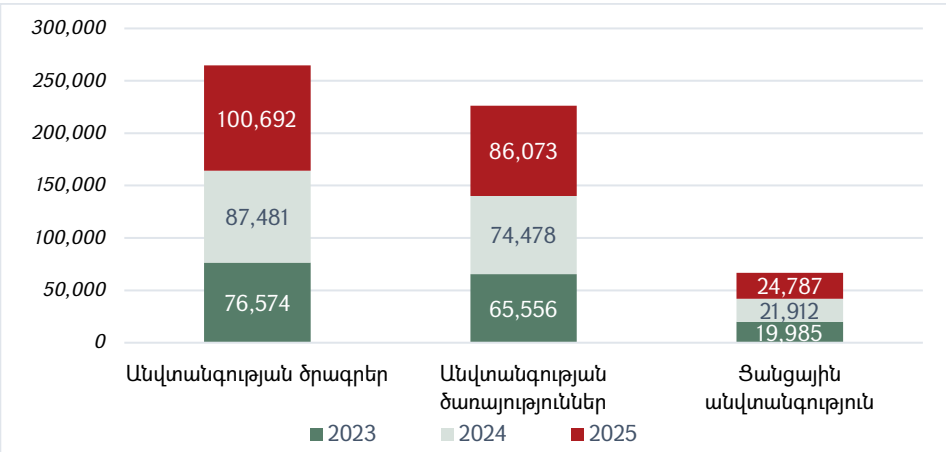
- NIST Cybersecurity Framework-ը (CSF) մշակվել է ԱՄՆ-ի տեխնոլոգիաների և ստանդարտների նյութերի ինստիտուտի (NIST) կողմից և նա-

[16] Tarala J. (2021), *Cybersecurity standards scorecard: 2021 SANS edition*. Cyber Risk and Assurance, https://crfsecure.org/cybersecurity-standards-scorecard-2021-sans-editio

[17] Տե՛ս Statista, Cybersecurity standards usage for control systems in organizations worldwide in 2021, https://www.statista.com/statistics/1273188/cybersecurity-standards-usage-control-systems/

խատեսված է օգնելու կազմակերպություններին կառավարել և նվազեցնել կիբեռանվտանգության ռիսկերը: Սա կամավոր է և նախատեսված է բոլոր տեսակի կազմակերպությունների համար:

- ISA/IEC 62443-ը ստանդարտների շարք է, որը կենտրոնանում է արդյունաբերական ավտոմատացման և կառավարման համակարգերի (IACS) անվտանգության վրա: Դա մշակվել է Միջազգային ավտոմատացման հասարակության (ISA) և Միջազգային էլեկտրատեխնիկական կոմիսիայի (IEC) կողմից և նախատեսված է պաշտպանելու կրիտիկական ենթակառուցվածքները, ինչպիսիք են էներգիայի, տրանսպորտի և քիմիական արդյունաբերության ոլորտները:
- ISO/IEC 27001-ը լայնորեն օգտագործվում է տեղեկատվական անվտանգության կառավարման համակարգերում: Դա միջազգային չափանիշ է, որը սահմանում է տեղեկատվական անվտանգության կառավարման համակարգի (ISMS) ստեղծման, իրականացման, պահպանման և շարունակական բարելավման պահանջները:
- CIS Controls-ը համարվում է գործնական և պարզեցված մոտեցում կիբեռանվտանգության ամրապնդման համար, որը կարող է կիրառվել կառավարման համակարգերում:



Գծապատկեր 3. ***Համաշխարհային ծախսերը տեղեկատվական անվտանգության ապահովման նպատակով 2023–2025 թթ. (միլիոն ԱՄՆ դոլար)[18]***

Համաշխարհային տեղեկատվական անվտանգության ծախսերը կայուն աճ են արձանագրում: 2023 թվականին ընդհանուր ծախսերը կազմել են 162.1 միլիարդ ԱՄՆ դոլար, 2024 թվականին՝ 183.9 միլիարդ ԱՄՆ դոլար, իսկ 2025 թվականին կանխատեսվում է 212 միլիարդ ԱՄՆ դոլար[19]: Այս աճը արտացոլում է կազմակերպությունների կողմից կիբեռանվտանգության ռիսկերի կառավարման ռազմավարությունների ամրապնդման պահանջը: Աճը պայմանավորված է մի քանի հիմնական գործոններով՝

[18] Statista (2023), *Global cybersecurity spending report 2023–2025*, https://www.statista.com/statistics/1104773/global-cybersecurity-spending/

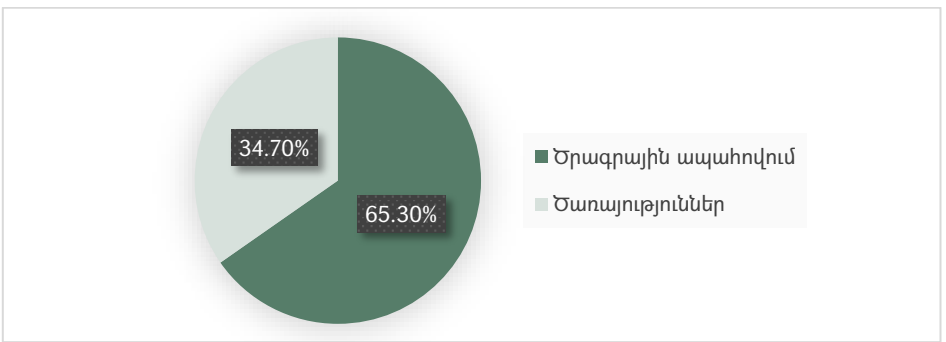
[19] Տե՛ս Gartner (2024, օգոստոսի 28), Gartner Forecasts Global Information Security Spending to Grow 15% in 2025, https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

- **Բարձր սպառնալիքների միջավայր**. կիբեռհարձակումների բարդության և հաճախականության աճը, ներառյալ գեներատիվ ԱԲ-ի օգտագործումը սոցիալական ինժեներիայի հարձակումներում:
- **Ամպային տեխնոլոգիաների ընդունում**. կազմակերպությունների անցումը ամպային լուծումներին մեծացնում է ամպային անվտանգության լուծումների պահանջարկը:
- **Հմտությունների պակաս**. կիբեռանվտանգության մասնագետների համաշխարհային պակասը խթանում է ներդրումներն անվտանգության ծառայություններում, ինչպիսիք են խորհրդատվությունը և կառավարվող ծառայությունները:

Ակնհայտ է, որ տեղեկատվական անվտանգության հետ կապված ներդրումների աճը ոչ միայն օրինաչափ, այլև պարտադիր է դարձել: Այս անհրաժեշտությունից ելնելով՝ վերջին տարիներին էականորեն աճել է SOAR (Security Orchestration, Automation, and Response) համակարգերի դերը կիբեռանվտանգության կառավարման մեջ: Այս համակարգերը ներկայացնում են կազմակերպվածության, ավտոմատացման և պատասխանելու համակցված լուծում, որը միավորում է բազմաթիվ անվտանգության գործիքներ և տվյալներ մեկ միասնական հարթակում:

SOAR համակարգերի կիրառումը հատկապես կարևոր է այն կազմակերպությունների համար, որոնք բախվում են միաժամանակյա խնդիրների, ներառյալ՝ ռեսուրսների սահմանափակում, կիբեռհարձակումների ծավալի աճ և մասնագետների պակաս: Այս համակարգերն ապահովում են ոչ միայն արձագանքման արագացում, այլև աշխատուժի բեռնաթափում՝ ավտոմատացնելով կրկնվող գործընթացները և ազատելով կիբեռանվտանգության մասնագետներին ավելի բարդ վերլուծական խնդիրների լուծման համար:

Ըստ վերջին գնահատականների՝ SOAR շուկայի չափսը 2025 թվականին կանխատեսվում է հասցնել 4.1 միլիարդ ԱՄՆ դոլարի, ինչը վկայում է այս տեխնոլոգիայի նկատմամբ կազմակերպությունների վստահության և հետաքրքրության շարունակական աճի մասին[20]:



Գծապատկեր 4. ***2024 թվականին SOAR շուկայի բաժինների բաշխումը***[21]

[20] Տե՛ս Mordor Intelligence. (2025). Security Orchestration Market Size and Share Analysis - Growth Trends and Forecasts (2025-2030). https://www.mordorintelligence.com/industry-reports /security-orchestration-market

[21] QKS Group (2025, March 26), *Market share: Security orchestration and automation (SOAR), 2024, worldwide*, https://qksgroup.com/market-research/market-share-security-orchestration-and-automation-soar-2024-worldwide-2773Market Growth Reports+3

Ծրագրային ապահովման բաժինը կազմել է 65.3%, ինչը ցույց է տալիս կազմակերպությունների կողմնորոշումը դեպի ավտոմատացման լուծումներ: Միաժամանակ, ծառայությունների բաժինը կազմել է 34.7%, ինչը նույնպես նշանակալի է հատկապես այնպիսի կազմակերպությունների համար, որոնք պահանջում են անհատականացված ռազմավարություններ և մշտադիտարկման մասնագիտական աջակցություն:

SOAR համակարգերը, լինելով նոր սերնդի անվտանգության կառավարման գործիքներ, հնարավորություն են տալիս կազմակերպություններին ոչ միայն դիմագրավելու ներկա սպառնալիքներին, այլև կանխատեսելու վտանգները՝ ձևավորելով ավելի կայուն և ինքնուրույն գործող կիբեռանվտանգության էկոհամակարգեր: Նման մոտեցումը համահունչ է միջազգային փորձին, օրինակ՝ գլոբալ կիբեռանվտանգության ինդեքսի (Global Cybersecurity Index, GCI) մշակման նպատակներին: GCI-ն կիբեռանվտանգության գնահատման միջազգային ինդեքս է, որը մշակվում և հրապարակվում է ՄԱԿ-ի համակարգում գործող Հաղորդակցության միջազգային միության (International Telecommunication Union, ITU) կողմից՝ նպատակ ունենալով գնահատելու և համեմատելու աշխարհի տարբեր պետությունների կիբեռանվտանգության մակարդակը՝ ըստ հստակ սահմանված չափանիշների: Այս ցուցանիշը արտացոլում է յուրաքանչյուր երկրի պատրաստվածության և պաշտպանվածության աստիճանը կիբեռանվտանգության ոլորտում, ինչպես նաև դրանց ռազմավարական մոտեցումները տվյալների պաշտպանության և սպառնալիքների արձագանքման ուղղությամբ: Նշված ինդեքսը հաշվարկվում է հինգ առանցքային ցուցանիշների հիման վրա, որոնք ներկայացնում են կիբեռանվտանգության համապարփակ քաղաքականության հիմնական բաղադրիչները:

1. **Իրավական միջոցառումներ (Legal Measures)**. գնահատվում են կիբեռհանցագործությունների դեմ պայքարի ազգային օրենսդրական դրույթները և դրանց կիրառման մեխանիզմները:
2. **Տեխնիկական միջոցառումներ (Technical Measures)**. ընդգրկում են պետական մակարդակով ներդրված տեխնոլոգիական և ինստիտուցիոնալ հարթակները, որոնք ապահովում են սպառնալիքների մշտադիտարկում, արձագանք և վերականգնում:
3. **Կազմակերպական միջոցառումներ (Organizational Measures)**. վերաբերում են ազգային ռազմավարությունների, քաղաքականությունների, կառույցների և համագործակցության հարթակների առկայությանը:
4. **Կարողությունների զարգացում (Capacity Building)**. ներառում է մասնագիտական կրթության, վերապատրաստման, հանրային իրազեկման և հետազոտական հզորությունների խթանումը:
5. **Միջազգային համագործակցություն (Cooperation)**. գնահատվում է երկրի ներգրավվածությունը միջազգային կիբեռանվտանգության նախաձեռնություններում, երկկողմ և բազմակողմ ծրագրերում:

GCI-ի մեթոդաբանությունը հիմնված է *համապարփակ, կառուցվածքային հարցաթերթիկի վրա*, որը ներառում է մոտ *80 ցուցիչ* (indicators)՝ բաժանված *5 հիմնական չափորոշիչների (pillars)*: Յուրաքանչյուր երկիր լրացնում է հարցաթերթիկը՝ փաստաթղթային ապացույցներով, որոնք հետագայում անցնում

են վավերացման և գնահատման փուլեր: Յուրաքանչյուր ցուցիչ գնահատվում է առավելագույնը 20 միավոր՝ գումարային 100 միավոր:

Փորձագետների ուսումնասիրություններից հետո կատարվում է միավորների հաշվարկ: Յուրաքանչյուր ենթախմբի համար նախապես սահմանվում է միավորների սանդղակ (օրինակ՝ 0, 0.25, 0.5, 0.75, 1.0), որը բազմապատկվում է համապատասխան կշռով: Բոլոր միավորները գումարվում են՝ ձևավորելով ընդհանուր GCI միավորը (0-100 սանդղակով): Այս ամենից հետո երկրները դասակարգվում են ըստ «Tier» մակարդակների՝ իրենց միավորների հիման վրա՝ Tier 1՝ (95-100 միավոր) – Role Modeling, Tier 2՝ (85–95 միավոր) – Advancing, Tier 3՝ (55–85 միավոր) – Establishing, Tier 4՝ (20–55 միավոր)– Evolving, Tier 5(0-20 միավոր) – Building:

Ըստ ITU-I կողմից հրապարակված զեկույցների, որոնք լույս են տեսել 2020[22] և 2024[23] թթ., 2020 թ. առաջատարի դիրքը զբաղեցնում էր ԱՄՆ-ն՝ 100 միավորով, ինչը վկայում է կիբեռանվտանգության հիմնական հինգ չափանիշներին իր ամբողջական համապատասխանության մասին (իրավական, տեխնիկական, կազմակերպչական, կարողությունների զարգացում, համագործակցություն): Երկրորդ, երրորդ և չորրորդ տեղերում են համապատասխանաբար՝ Մեծ Բրիտանիան, Սաուդյան Արաբիան (որոնք կիսում էին երկրորդ տեղը՝ 99.54 միավորով), Էստոնիան (99.48) և Հարավային Կորեան, Սինգապուրը, Իսպանիան՝ 98.52 միավորով:

2024 թ. առաջատարների ցանկում փոխվել է աշխարհագրական կենտրոնացումը՝ առաջատարն է Իտալիան: Նիդեռլանդները, Լյուքսեմբուրգը և Իսլանդիան նույնպես մտել են T1 խմբի մեջ՝ մոտավոր 99.7-99.8 միավորներով: Սա վկայում է եվրոպական փոքր ու միջին երկրների կիբեռանվտանգության քաղաքականությունների արդյունավետության մասին[24]: Ընդհանուր առմամբ, փոփոխությունները ցույց են տալիս, որ վերջին տարիներին առաջատար դառնալու համար վճռորոշ է դարձել ոչ միայն տեխնիկական ներուժը, այլև կիբեռանվտանգության կառավարման ամբողջական և հավասարակշռված մոտեցումը, ներառյալ օրենսդրական հստակությունը, մասնագետների պատրաստումը և միջազգային համագործակցությունը:

Ինչ վերաբերում է Հայաստանին, ապա 2020 թվականին ՀՀ-ն ունեցել է մոտավորապես 47.5 միավոր, իսկ 2024 թ. ցուցանիշը բարձրացել է մինչև 53.8: Սա վկայում է կիբեռանվտանգության ոլորտում ընդամենը 4 տարվա ընթացքում մոտ 13%-անոց աճի մասին[25]**:** Եթե համեմատական անցկացնենք տարածաշրջանի երկրների հետ, ապա Հայաստանը զիջում է բոլոր հարևան պետություններին: Օրենսդրական միջոցառումների ցուցանիշը Հայաստանում համեմատաբար բարձր է (առաջատար դիրքում է մյուս չափորոշիչների համեմատությամբ), իսկ կազմակերպչական միջոցառումների ցուցանիշը գրե-

[22] Տե՛ս International Telecommunication Union. (2021). Global Cybersecurity Index (GCI) 2020. ITU, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[23] Տե՛ս International Telecommunication Union. (2024). Global Cybersecurity Index (GCI) 2024. ITU, https://www.itu.int/hub/publication/d-hdb-gci-01-2024/

[24] Տե՛ս International Telecommunication Union. (2021). Global Cybersecurity Index (GCI) 2020. ITU, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[25] Տե՛ս International Telecommunication Union. (2024). Global Cybersecurity Index (GCI) 2024. ITU, https://www.itu.int/hub/publication/d-hdb-gci-01-2024/

թե զրոյին մոտ է, ինչը ցույց է տալիս լուրջ թերացում այդ ոլորտում:

Այսպիսով՝ կարող ենք փաստել, որ **օրենսդրական ոլորտում** Հայաստանն արդեն իսկ բավական ուժեղ է (կիբեռանվտանգության մասին օրենքներ, քաղաքական փաստաթղթեր, ռազմավարություններ), սակայն այդ օրենսդրական շրջանակները դեռևս **անարդյունավետ են գործում առանց կազմակերպչական մեխանիզմների**: Այլ խոսքով՝ «օրենքը կա, բայց գործառույթները բավարար չեն», իսկ կազմակերպչական ոլորտը (օրինակ՝ ազգային կիբեռանվտանգության գործակալություն, CIRT/CERT-ի թիմեր, պետական համակարգված կառույցներ) գրեթե բացակայում է, և դա է Հայաստանի GCI-ի ամենաթույլ կողմը: Եթե այստեղ ներդրումներ արվեն, ապա, անգամ առանց օրենսդրական դաշտի էական փոփոխության, հնարավոր է զգալի առաջընթաց GCI-ի ընդհանուր միավորում:

Աղյուսակ 2

Կիբեռանվտանգության գլոբալ ինդեքսի ցուցանիշները ՀՀ հարևան երկրներում 2020 և 2024 թթ.[26]

Երկիր	*Տարի*	*Ընդհանուր միավոր*	*Համաշխարհային վարկանշավորում*	*Դասակարգում*
Թուրքիա	2020	97.49	11	Tier 1 (Role-modeling)
	2024	98.52	4	
Հայաստան	2020	47.5	97	Tier 4 (Evolving)
	2024	53.81	88	
Վրաստան	2020	54	82	Tier 2 (Advancing)
	2024	58.3	76	
Ադրբեջան	2020	40	104	Tier 2 (Advancing)
	2024	93.76	13	
Իրան	2020	50	89	Tier 3 (Establishing)
	2024	54.5	84	

Հայաստանը թեև կիբեռանվտանգության ոլորտում զիջում է տարածաշրջանի առաջատարներին՝ Թուրքիային և Ադրբեջանին, վերջին տարիներին, այնուամենայնիվ, ապահովել է նկատելի առաջընթաց: Դա վկայում է, որ իրականացվում են որոշ բարեփոխումներ և գործարկվում են համապատասխան նախաձեռնություններ: Սակայն 2020–2024 թթ., ըստ գլոբալ *կիբեռանվտանգության ինդեքսի* (GCI), Հայաստանի առաջընթացը սահմանափակ է եղել. միավորներն աճել են ընդամենը +6.31-ով, և երկիրը պահպանել է Tier 4 (Evolving) կարգավիճակը: Ի տարբերություն Հայաստանի՝ Ադրբեջանը կարողացել է զգալիորեն բարելավել իր դիրքերը և ներկայումս գտնվում է Tier 2 (Advancing) մակարդակում: Սա վկայում է արդյունավետ պետական քաղաքականության, ներդրումների և համակարգված քայլերի մասին: Վրաստանն էլ է առաջընթաց գրանցել՝ 2024 թվականին հասնելով Tier 2 մակարդակին: Թուրքիան շարունակել է պահպանել իր բարձրակարգ դիրքը՝ մնալով Tier 1-ում, ինչը վկայում է կայուն և զարգացած կիբեռանվտանգության համակարգի մասին: Իրանը 2024 թ. ստացել է մոտ 54.5 միավոր՝ դասվելով Tier 3 (Establishing) կարգին: Սա միջին մակարդակի զարգացում է, որը, սակայն, զգալիորեն զիջում է տարածաշրջանի առաջատարներին: Հայաստանի ցու-

[26] Տե՛ս International Telecommunication Union. (2024). *Global Cybersecurity Index 2024 (GCIv5).* ITU-D, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2024-PDF-E.pdf

ցանիշների համեմատաբար անփոփոխ լինելը մատնանշում է, որ ոլորտում դեռևս առկա են թերություններ և անհրաժեշտ է ռազմավարական վերանայում: Մինչդեռ Ադրբեջանն ու Վրաստանը վերջին չորս տարում կարողացել են անցնել միջինից դեպի առավել կայուն մակարդակ, ինչը հստակ արդյունք է պետական ծրագրերի և ներդրումների: Թուրքիայի Tier 1 կարգավիճակը ևս մեկ անգամ ընդգծում է նրա առաջատար դերը տարածաշրջանում՝ քաղաքականության, տեխնոլոգիական պատրաստվածության և կազմակերպչական հզորությունների տեսանկյունից: Հայաստանը, չնայած ներկայիս համեստ դիրքին, ունի զարգացման զգալի ներուժ: Հատկապես կարևոր է կենտրոնանալ օրենսդրական և կազմակերպչական շրջանակների ամրապնդման վրա, ինչպես նաև խորացնել միջազգային համագործակցությունը: Ներդրումներն այս ուղղությամբ կնպաստեն տեխնիկական կարողությունների զարգացմանը, ինչն էլ, ի վերջո, հնարավորություն կտա բարելավելու Հայաստանի դիրքն ըստ GCI-ի ինդեքսի, և մեր երկիրն ավելի մրցունակ կդառնա տարածաշրջանում:

Ազգային կիբեռանվտանգության ինդեքսը (**National Cyber Security Index, NCSI)** համաշխարհային գործիք է, որի նպատակն է գնահատել տարբեր երկրների ազգային կիբեռպաշտպանության մակարդակը և պատրաստվածությունը կիբեռանվտանգության ոլորտում: Այս ինդեքսը մշակվել է Էստոնիայի e-Governance Academy-ի (EGA) կողմից՝ որպես անկախ չափիչ համակարգ, որն օբյեկտիվ և համակարգված ձևով կուտակում և վերլուծում է կիբեռանվտանգության քաղաքականության, ենթակառուցվածքների և իրավակարգավորումների վերաբերյալ տվյալները[27]:

Ազգային կիբեռանվտանգության ինդեքսի վերջին տվյալների հիման վրա[28] առաջատար երկրների խմբում ընդգրկված են մի շարք պետություններ, որոնք ցուցաբերում են բարձրագույն մակարդակի պատրաստվածություն կիբեռանվտանգության սպառնալիքների կանխարգելման, հայտնաբերման և արձագանքման գործընթացներում: Առաջին հորիզոնականները զբաղեցնում են Դանիան, Ֆինլանդիան և Միացյալ Թագավորությունը. յուրաքանչյուրն ունի 100 միավոր, ինչը վկայում է ամբողջական համապատասխանության և լիարժեք կարողությունների առկայության մասին բոլոր գնահատվող չափանիշներով:

Այդ երկրներին հաջորդում են Բելգիան (96.81), Շվեդիան (95.10), Էստոնիան (95.04) և Գերմանիան (93.84), որոնք, թեև մի փոքր զիջում են առաջատարներին ընդհանուր միավորներով, այնուամենայնիվ, ցուցադրում են համապարփակ և կայուն համակարգեր կիբեռանվտանգության ապահովման համար:

Առաջատար երկրների ուժեղ կողմերը կարելի է համադրել հետևյալ հիմնական ուղղություններով.

1. **Օրենսդրական և կարգավորող միջավայր**. առաջատար երկրներն ունեն հստակ ձևակերպված ազգային կիբեռանվտանգության ռազմավարություններ և օրենսդրական բազա, որը ներառում է տվյալների

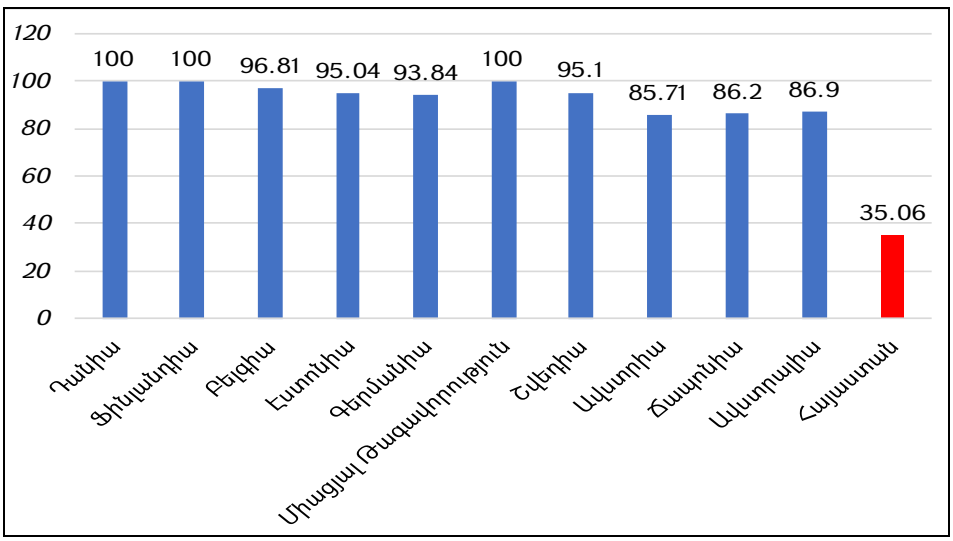
[27] Տե՛ս E-Governance Academy (2023). National Cyber Security Index (NCSI) 3.0 Methodology, https://ncsi.ega.ee/methodology/

[28] Տե՛ս National Cyber Security Index (2024). *NCSI rankings and country profiles*. e-Governance Academy, https://ncsi.ega.ee

պաշտպանության, ցանցային անվտանգության և թվային ենթակառուցվածքների պաշտպանվածության իրավական նորմեր:

2. **Տեխնիկական միջոցառումներ և հզոր ենթակառուցվածքներ**. առկա են մշտադիտարկման, սպառնալիքների կանխարգելման և արձագանքման զարգացած համակարգեր, ներառյալ CERT/CSIRT կենտրոններ և ավտոմատացված նախազգուշացման մեխանիզմներ:
3. **Կազմակերպական կարողություններ**. պետական և մասնավոր հատվածների համագործակցությունն ապահովում է ճկուն կառավարման մոդելներ, որոնք թույլ են տալիս արագ արձագանքել նոր առաջացող սպառնալիքներին:
4. **Միջազգային համագործակցություն**. ակտիվ ներգրավվածություն բազմակողմ կառույցներում և միջազգային ծրագրերում, որոնք միտված են կիբեռանվտանգության ոլորտում փորձի և տեղեկատվության փոխանակմանը[29,30]:

Այս գործոնների համադրված ազդեցությունը թույլ է տալիս առաջատար երկրներին ոչ միայն ունենալ բարձր վարկանիշ NCSI-ում, այլև ապահովել իրական և գործնական պաշտպանվածություն թվային սպառնալիքների նկատմամբ:



Գծապատկեր 5. ***Հայաստանի և առաջատար երկրների National Cyber Security Index (NCSI) 2022 թվականի ցուցանիշներ***[31]

Հայաստանի 2022 թ. National Cyber Security Index (NCSI) հաշվետվությունը ներկայացնում է երկրի կիբեռանվտանգության համակարգի ընդհանուր գնահատականը՝ հիմնված 12 առանցքային ցուցիչների վրա: Վերջիններս ընդգրկում են քաղաքականություն, սպառնալիքների վերլուծություն,

[29] Տե՛ս European Union Agency for Cybersecurity (ENISA). (2022). Good Practices in National Cybersecurity Strategies, https://www.enisa.europa.eu/publications/good-practices-in-national-cybersecurity-strategies

[30] Տե՛ս OECD (2023), International Cybersecurity Cooperation: Trends and Developments, https://www.oecd.org/digital/international-cybersecurity-cooperation.htm

[31] Estonian e-Governance Academy (2022), National Cyber Security Index: Armenia 2022 [PDF]. https://ncsi.ega.ee/country/am_2022/?pdfReport=1

կրթություն, գլոբալ համագործակցություն, թվային ծառայությունների պաշտպանություն, կարևոր ծառայությունների պաշտպանություն, էլեկտրոնային նույնականացում, անձնական տվյալների պաշտպանության, կիբեռմիջադեպերի արձագանքման, ճգնաժամային կառավարման, կիբեռհանցագործությունների դեմ պայքար և ռազմական կիբեռգործողություններ:

Digital Development Level (DDL)-ը համարվում է թվային զարգացման ցուցանիշ, որը հաշվարկվում է ըստ երկու հիմնական ինդեքսների՝

1. **E-Government Development Index (EGDI)**. էլեկտրոնային կառավարումների զարգացումն արտացոլող ինդեքս է, որն ընդգրկում է թվային ծառայությունների մատուցման մակարդակը, տեղեկատվական ենթակառուցվածքների հասանելիությունը և մարդկային կապիտալի զարգացումը:
2. **Networked Readiness Index (NRI)**. ցանցային պատրաստվածության ինդեքս է, որը չափում է, թե որքանով է երկիրը պատրաստ օգտվելու տեղեկատվական և հաղորդակցման տեխնոլոգիաներից (ՏՀՏ)՝ տնտեսական և սոցիալական զարգացման համար:

DDL-ի հաշվարկի սկզբունքները ներառում են՝

- DDL-ը համադրում է EGDI-ի և NRI-ի արդյունքները՝ ստեղծելով համընդհանուր թվային զարգացման մակարդակի գնահատում:
- Այս համադրման շնորհիվ DDL-ն արտացոլում է ոչ միայն տեխնոլոգիական ենթակառուցվածքների մակարդակը, այլև երկրի քաղաքական, սոցիալական ու տնտեսական պատրաստվածությունը թվային դաշտում:
- DDL-ի արժեքը սովորաբար ներկայացվում է 0-ից 1 կամ 0–100 կշռային սանդղակով՝ ապահովելով համեմատելիություն տարբեր երկրների միջև:

Այս ցուցանիշներից զատ հաշվարկվում է նաև NCSI և DDL ցուցանիշների տարբերությունը.

- **Եթե տարբերությունը դրական է** ((NCSI–DDL)>0), ապա երկրի կիբեռանվտանգության մակարդակն ավելի բարձր է, քան նրա ընդհանուր թվային զարգացման մակարդակը: Այսինքն՝ տվյալ պետությունը համեմատաբար ավելի լավ է պաշտպանված, քան կարելի է սպասել նրա թվային ենթակառուցվածքների զարգացումից: Սա կարող է նշանակել, որ պետությունը հատուկ շեշտ է դնում կիբեռանվտանգության վրա, նույնիսկ եթե տեխնոլոգիական զարգացումը դեռ չափավոր է:
- **Եթե տարբերությունը բացասական է** ((NCSI–DDL)<0), ապա երկրի կիբեռանվտանգության մակարդակը հետ է մնում ընդհանուր թվային զարգացման մակարդակից: Այսինքն՝ պետությունը տեխնոլոգիապես ավելի զարգացած է, քան կիբեռանվտանգության պատրաստվածության մակարդակն է: Սա սովորաբար վկայում է օրենսդրության կամ գործնական մեխանիզմների մեջ անվտանգության պակաս ռեսուրսների մասին:

Այս համատեքստում NCSI-ի և DDL-ի ցուցանիշների համադրությունը համապարփակ պատկերացում է տալիս Հայաստանի կիբեռանվտանգության մակարդակի մասին՝ ընդգծելով ուժեղ կողմերն ու զարգացումների հնարավորությունները, ինչպես նաև մատնանշելով այն ոլորտները, որտեղ անհրաժեշտ են լրացուցիչ միջոցառումներ և ռազմավարական ուղղորդում: Նման իրավիճակում իրավական և ինստիտուցիոնալ հիմքերի ամրապնդումը դառնում է

առաջնահերթություն, քանի որ միայն թվային ենթակառուցվածքների զարգացումը բավարար չէ արդյունավետ պաշտպանվածություն ապահովելու համար:

Աղյուսակ 3

NCSI 2022 թ. հիմնական ցուցանիշները Հայաստանի և տարածաշրջանի երկրների համար[32]

Երկիր	*NCSI միավոր*	*DDL*	*NCSI-DDL*	*Տարածաշրջանային դիրք*
Վրաստան	43.21	75	-31.79	75-րդ տեղ
Ադրբեջան	37.84	66	-28.16	91-րդ տեղ
Հայաստան	35.06	66.88	-31.82	96-րդ տեղ
Թուրքիա	52.15	82.6	-30.45	48-րդ տեղ
Իրան	29.42	60	-30.58	110-րդ տեղ

Հայաստանում կիբեռհանցագործությունների իրավական կարգավորումը սկսել է ձևավորվել դեռևս 2000-ականներից, երբ տեղեկատվական տեխնոլոգիաների արագ զարգացումը պահանջեց նոր իրավական մոտեցումներ: Զգալի առաջընթաց արձանագրվեց հատկապես 2017–2022 թվականներին, երբ կիբեռանվտանգությունը պետական մակարդակով հայտարարվեց առաջնահերթություն:

2021 թվականին ուժի մեջ մտած նոր քրեական օրենսգիրքը[33] ներառեց կիբեռհանցագործություններին առնչվող հստակ հոդվածներ, որոնք սահմանում են նմանատիպ արարքները և նախատեսում պատժամիջոցներ: Տեղեկատվական և կիբեռանվտանգության ոլորտը ներկայումս կարգավորվում է մի շարք օրենքներով և ենթաօրենսդրական ակտերով, որոնք ապահովում են անձնական տվյալների պաշտպանությունը, տեղեկատվական իրավունքները և կիբեռհանցագործությունների կանխարգելման հիմքերը:

2022 թ. ՀՀ քրեական օրենսգրքի դրույթները ներառում են հեղինակային իրավունքների խախտման[34, 35], համակարգչային հափշտակության[36], թվային միջավայրում ատելության քարոզի և հանրային անվտանգությանն սպառնացող այլ հանցագործությունների վերաբերյալ հոդվածներ[37]: Դրանցում նախատեսված պատժամիջոցները համահունչ են միջազգային փաստաթղթերին, ինչպիսիք են Բուդապեշտի կոնվենցիան կիբեռհանցագործությունների դեմ[38], ՄԱԿ-ի[39] և Եվրոպայի խորհրդի համաձայնագրերը[40]: Բացի քրեական օրենսգրքից՝ Հայաստանի օրենսդրական դաշտում առանցքային դեր ունեն

---

[32] Տե՛ս նույն տեղը:

[33] Տե՛ս ՀՀ քրեական օրենսգիրք, https://www.irtek.am/views/act.aspx?aid=154256

[34] Տե՛ս ՀՀ քրեական օրենսգրքի հավելված N 2. Կիբեռհանցագործություններ, հոդված 227, 2-րդ մաս, 2-րդ կետ:

[35] Տե՛ս Criminal code of the Republic of Armenia, https://legislationline.org/sites/default/files/2023-12/Criminal%20Code%20of%20the%20Republic%20of%20Armenia%20%282022%29%20%28English%29.pdf, Article 227. Infringement of Copyright and Related Rights, էջ 171:

[36] Տե՛ս https://www.irtek.am/views/act.aspx?aid=154256

[37] Տե՛ս ՀՀ քրեական օրենսգրքի հավելված N 2. Կիբեռհանցագործություններ, հոդված 329, 359-365, https://www.irtek.am/views/act.aspx?aid=154256

[38] Տե՛ս https://www.coe.int/en/web/cybercrime/the-budapest-convention

[39] Տե՛ս https://www.unodc.org/unodc/en/cybercrime/global-programme-on-cybercrime.html

[40] Տե՛ս Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2016/679/oj

«Տեղեկատվական անվտանգության մասին»[41] և «Անձնական տվյալների պաշտպանության մասին»[42] օրենքները, ՀՀ Սահմանադրության համապատասխան դրույթները[43], ինչպես նաև էլեկտրոնային փաստաթղթաշրջանառության և թվային անվտանգության կարգավորող նորմերը[44]:

Կարևոր նշանակություն ունի նաև 2023 թվականին ընդունված Կիբեռանվտանգության ազգային ռազմավարությունը[45], որը համակարգված մոտեցում է ապահովում պետական մարմինների, ֆինանսական համակարգի, ենթակառուցվածքների և քաղաքացիների պաշտպանության համար: Այս ռազմավարությունը, ինչպես նաև 2020 թվականի Ազգային անվտանգության ռազմավարությունը ընդգծում են ոչ միայն տեխնիկական պաշտպանությունը, այլև ապատեղեկատվության դեմ պայքարի և հասարակական կայունության պահպանման կարևորությունը: Միջազգային համագործակցությունը ևս կարևոր դեր ունի. Հայաստանը անդամակցում է Բուդապեշտի կոնվենցիային[46], մասնակցում է ԵՄ Eastern Partnership նախաձեռնությանը (EU4Digital ծրագրով)[47], ինչպես նաև ներգրավված է ՆԱՏՕ-ի կիբեռանվտանգության համագործակցության պլատֆորմներում[48]: Այս մասնակցությունը հնարավորություն է տալիս համահունչ լինելու միջազգային լավագույն փորձին, զարգացնելու ազգային կարողությունները և ընդլայնելու համագործակցության հնարավորությունները:

Այսպիսով՝ Հայաստանի կիբեռանվտանգության դաշտը դինամիկ զարգանում է. մի կողմից՝ այն ունի օրենսդրական ամուր հիմքեր և միջազգային պարտավորությունների համակարգ, մյուս կողմից՝ կազմակերպչական և ինստիտուցիոնալ մակարդակներում դեռ առկա են բարելավման լուրջ անելիքներ:

Եզրակացություն: Հայաստանի տեղեկատվական և կիբեռանվտանգության ոլորտի վերլուծությունը վկայում է, որ այն դեռևս գտնվում է ձևավորման փուլում և առերեսվում է բազմաթիվ կազմակերպչական, իրավական և տեխնիկական մարտահրավերների: Թեև վերջին տարիներին արձանագրվել է որոշակի առաջընթաց իրավական դաշտի բարելավման, ռազմավարական փաստաթղթերի ընդունման և պետական կառույցների կարողությունների զարգացման առումներով, սակայն կիբեռանվտանգության համակարգի ընդհանուր արդյունավետությունն ու ինքնաբավությունը դեռևս սահմանափակ են:

Հաշվի առնելով միջազգային համատեքստը՝ Հայաստանի համար առաջնահերթ խնդիր է համապարփակ և երկարաժամկետ կիբեռանվտանգության

---

[41] Տեղեկատվական անվտանգության մասին ՀՀ օրենք, https://www.e-draft.am/projects/8642/about

[42] Անձնական տվյալների պաշտպանության մասին ՀՀ օրենք, https://www.arlis.am/hy/acts/98338

[43] Տե՛ս ՀՀ Սահմանադրության տեղեկատվական իրավունքներին վերաբերող դրույթներ, https://www.arlis.am/hy/acts/102510

[44] Տե՛ս «Էլեկտրոնային փաստաթղթի և էլեկտրոնային ստորագրության մասին» ՀՀ օրենք, https://www.arlis.am/hy/acts/98388

[45] Կիբեռանվտանգության ոլորտի ռազմավարություն 2022–2026, https://www.e-draft.am/projects/6656/justification

[46] Տե՛ս https://www.coe.int/en/web/cybercrime/the-budapest-convention

[47] Տե՛ս https://www.eeas.europa.eu/eeas/eastern-partnership_en

[48] Տե՛ս The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub, https://ccdcoe.org/

քաղաքականության իրականացումը, որը կներառի ոչ միայն պետական կառույցների, այլև մասնավոր հատվածի ու հասարակության ներգրավումը: Անհրաժեշտ է զարգացնել կիբեռանվտանգության կրթական և գիտական կարողությունները, ներդնել ժամանակակից տեխնոլոգիաներ և ստեղծել ճգնաժամային արձագանքման արդյունավետ մեխանիզմներ:

Կարողությունների զարգացումը հնարավորություն կտա բարելավելու Հայաստանի դիրքերը **Global Cybersecurity Index (GCI)**-ում և դառնալ ավելի մրցունակ տարածաշրջանում: Ըստ *ազգային կիբեռանվտանգության ինդեքսի* **(NCSI)** վերջին տվյալների՝ Հայաստանը դեռևս զգալիորեն հետ է մնում առաջատարներից՝ Դանիայից, Ֆինլանդիայից և Միացյալ Թագավորությունից, որոնք ցուցաբերում են ամբողջական համակարգեր կիբեռանվտանգության ոլորտում: Հայաստանի **NCSI = 35.06**, իսկ **DDL = 66.88**, ինչը վկայում է, որ երկրի կիբեռանվտանգության մակարդակը թվային զարգացման համեմատությամբ զգալիորեն ցածր է: Սա նշանակում է, որ տեխնոլոգիական առաջընթացը չի ուղեկցվում համապատասխան պաշտպանական համակարգերի ձևավորմամբ:

Հետևաբար՝ Հայաստանի կիբեռանվտանգության համակարգի զարգացումը պետք է դիտվի ոչ միայն որպես տեխնիկական, այլև ռազմավարական խնդիր՝ ուղղված պետական ինքնիշխանության, տնտեսական կայունության և թվային անվտանգության ամրապնդմանը: Միայն իրավական, ինստիտուցիոնալ և կրթական հիմքերի համակցված զարգացումն է, որ կարող է ապահովել երկրի անվտանգ ու կայուն առաջընթացը թվային դարում:

Օգտագործված գրականություն

1. Armenian Law on Electronic Document and Electronic Signature (n.d.), https://www.arlis.am/hy/acts/98388
2. Armenian Law on Information Security (n.d.), https://www.e-draft.am/projects/8642/about
3. Armenian Law on Personal Data Protection (n.d.), https://www.arlis.am/hy/acts/98338
4. Budapest Convention on Cybercrime (n.d.). Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention
5. Criminal Code of the Republic of Armenia (2022). Legislationline, https://legislationline.org/sites/default/files/2023-12/Criminal%20Code%20of%20the%20Republic%20of%20Armenia%20%282022%29%20%28English%29.pdf
6. E-Governance Academy (2023), National Cyber Security Index (NCSI) 3.0 methodology, https://ncsi.ega.ee/methodology/
7. ENISA (2022), Good practices in national cybersecurity strategies, https://www.enisa.europa.eu/publications/good-practices-in-national-cybersecurity-strategies
8. Estonian e-Governance Academy (2022), National Cyber Security Index: Armenia 2022, https://ncsi.ega.ee/country/am_2022/?pdfReport=1
9. European Union (2016), General Data Protection Regulation (GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj

10. Gartner (2024, August 28), Gartner forecasts global information security spending to grow 15% in 2025, https://www.gartner.com/en/newsroom/press-releases/2024-08-28
11. Himmat M., Ibrahim M. A., Hammam N., Eldirdiery H. F., Algazoli G. (2023), The current trends, techniques, and challenges of cybersecurity. *European Journal of Information Technologies and Computer Science, 3*(4), https://doi.org/10.24018/compute.2023.3.4.93
12. IBM (2024), *Cost of a data breach report 2024*, IBM, https://www.ibm.com/reports/data-breach
13. ITU (2021), *Global Cybersecurity Index (GCI) 2020*. International Telecommunication Union, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
14. ITU (2024), *Global Cybersecurity Index (GCI) 2024*. International Telecommunication Union, https://www.itu.int/hub/publication/d-hdb-gci-01-2024/
15. Jobera (n.d.). Remote work cybersecurity statistics, https://jobera.com/remote-work-cybersecurity-statistics/
16. Kadena E., Gupi M. (2021), Human factors in cybersecurity: Risks and impacts. *Security Science Journal, 2*(2).
17. Media Initiatives (2017), *Internet freedom in Armenia and execution of basic human rights*, https://mediainitiatives.am/wp-content/uploads/2018/03/Internet-Freedom-Research-Report-2017-in-English.pdf
18. MixMode (2024, June 12), Global cybercrime report 2024: Which countries face the highest risk? https://mixmode.ai/blog/global-cybercrime-report-2024-which-countries-face-the-highest-risk
19. Mordor Intelligence (2025), *Security orchestration market size and share analysis – forecasts 2025–2030*, https://www.mordorintelligence.com/industry-reports/security-orchestration-market
20. Mowbray T. J. (2013), *Cybersecurity: Managing systems, conducting testing, and investigating intrusions* (1st ed.). Wiley.
21. National Cyber Security Index (2024), NCSI rankings and country profiles, https://ncsi.ega.ee
22. NCSI (2023), Finland – National Cyber Security Index, https://ncsi.ega.ee/country/fi/
23. Nedjah N., Abd El-Latif A. A., Gupta B. B., Mourelle L. M. (Eds.). (2022). *Robotics and AI for cybersecurity and critical infrastructure in smart cities* (Vol. 1030). Springer Nature.
24. OECD (2023). *International cybersecurity cooperation: Trends and developments*, https://www.oecd.org/digital/international-cybersecurity-cooperation.htm
25. QKS Group (2025, March 26). Market share: Security orchestration and automation (SOAR), 2024, worldwide, https://qksgroup.com/market-research/market-share-security-orchestration-and-automation-soar-2024-worldwide-2773
26. Saeed S., Gull H., Aldossary M. M., Altamimi A. F., Alshahrani M. S., Saqib M., Zafar Iqbal S., Almuhaideb A. M. (2024). Digital transformation in energy sector: Cybersecurity challenges and

implications. *Information, 15*(12), https://doi.org/10.3390/info15120764
27. Sisoyan A. (2020), New cybersecurity challenges: Digital transformation and political implications. *YSU Journals*, https://journals.ysu.am/index.php/j-pol-sci/article/view/12695
28. Spînu N. (2020), *Armenia cybersecurity governance assessment*. Geneva Centre for Security Sector Governance, https://www.dcaf.ch/sites/default/files/publications/documents/ArmeniaCybersecurityGovernanceAssessment.pdf
29. Statista (2023), Global cybersecurity spending report 2023–2025. https://www.statista.com/statistics/1104773/global-cybersecurity-spending/
30. Statista (2024), Average cost of a data breach worldwide by country or region. https://www.statista.com/statistics/463714/cost-data-breach-by-country-or-region/
31. Statista (2024), Cybersecurity standards usage for control systems worldwide. https://www.statista.com/statistics/1273188/cybersecurity-standards-usage-control-systems/
32. Tarala J. (2021), Cybersecurity standards scorecard: 2021 SANS edition. Cyber Risk and Assurance, https://crfsecure.org/cybersecurity-standards-scorecard-2021-sans-editio
33. UNODC (n.d.), Global programme on cybercrime. United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/cybercrime/global-programme-on-cybercrime.html

АРМЕН КАЗАРЯН
Заведующий кафедры информационных систем и информационных технологий бизнеса АГЭУ, кандидат экономических наук, доцент

АРГАМ АРТАШЯН
Доцент кафедры информационных систем и информационных технологий бизнеса АГЭУ, кандидат экономических наук

АНУШ ТУМАНЯН
Доцент кафедры информационных систем и информационных технологий бизнеса АГЭУ, кандидат экономических наук

НАРЕК КЕСОЯН
Доцент кафедры актуарной и финансовой математики АГЭУ, кандидат экономических наук

КАТЯ КИРАКОСЯН
Магистрант кафедры информационных систем и информационных технологий бизнеса АГЭУ, магистрант

Глобальные вызовы информационной и кибербезопасности и положение Армении в международном контексте.– Одним из важнейших условий устойчивого экономического разви-

тия и национальной безопасности является информационная безопасность и кибербезопасность. Формирующаяся в мире цифровая реальность, отличающаяся масштабным оборотом данных, глобальным доступом к интернету и широким использованием инновационных технологий, создает как новые возможности развития, так и серьезные угрозы. В этих условиях обеспечение информационной безопасности должно стать одним из приоритетов правительства Армении, поскольку напрямую связано с экономической стабильностью страны, эффективностью государственного управления и повышением качества жизни граждан.

Комплексный анализ текущего состояния информационной безопасности показывает, что Армения продолжает оставаться уязвимой, особенно с точки зрения организационных и институциональных возможностей. Несмотря на определенный прогресс в правовой сфере, уровень самодостаточности страны остается низким: цифровая инфраструктура страны существенно зависит от внешних факторов, а зависимость от импорта увеличивает вероятность возникновения киберрисков. В данной статье предпринята попытка исследования организационных, правовых и технических основ системы кибербезопасности Армении, анализа позиции страны в международных сопоставлениях, а также оценки последствий и потенциальных рисков импортозависимости. Результаты анализа свидетельствуют о том, что игнорирование вопросов кибербезопасности может стать серьезной угрозой стабильности как системы государственного управления, так и экономики.

В этой связи первостепенное значение приобретает реализация комплексной и жизнеспособной политики, направленной на повышение уровня кибербезопасности не только государственных институтов, но и частного сектора и общества. Реализация целенаправленной политики должна включать углубление сотрудничества с международными партнерами, снижение технологической зависимости и расширение местных производственных и организационных возможностей, что создаст основу для безопасного и устойчивого хода цифрового развития Армении.

Ключевые слова: *кибербезопасность, информационная безопасность, цифровое развитие, управление рисками, институциональные возможности, национальная безопасность*
JEL: L86, O33
DOI: 10.52174/29538114_2025.2-168

ARMEN GHAZARYAN
Head of the chair of Business Information Systems and Information Technologies, ASUE, PhD in Economics, Associate Professor

ARGAM ARTASHYAN
Associate Professor of the Chair of Business Information Systems and Information Technologies, ASUE, PhD in Economics

ANUSH TUMANYAN
Associate Professor of the Chair of Business Information Systems and Information Technologies, ASUE, PhD in Economics

NAREK KESOYAN
Associate Professor of the chair of Actuarial and Financial Mathematics, Associate Professor, ASUE, PhD in Economics

KATYA KIRAKOSYAN
Master's student of the Chair of Business Information Systems and Information Technologies, ASUE

Global Challenges of Information and Cybersecurity and Armenia's Position in the International Context.– One of the key prerequisites for sustainable economic development and national security is information security and cybersecurity. The digital reality that has emerged globally, which is distinguished by large-scale data circulation, global access to the Internet and the widespread use of innovative technologies, creates both new development opportunities and serious threats. In these conditions, ensuring information security should be one of the priorities of the Armenian government, as it is directly related to the country's economic stability, the effectiveness of public administration and the improvement of the quality of life of citizens.

A comprehensive analysis of the current state of information security shows that Armenia remains vulnerable, especially in terms of organizational and institutional capabilities. Although some progress is observed in the legal field, the level of self-sufficiency is still low: the country's digital infrastructure is significantly dependent on external factors, and dependence on imports increases the likelihood of cyber risks.

This peper studies the organizational, legal and technical foundations of Armenia's cybersecurity system, analyzes the country's position in international comparisons, as well as assesses the consequences and potential risks of import dependence. The results of the analysis indicate that ignoring cybersecurity issues can become a serious threat to the stability of both the state governance system and the economy.

In this regard, the implementation of a comprehensive and viable policy aimed at increasing the level of cybersecurity not only of state institutions, but also of the private sector and society is of primary

importance. The implementation of a targeted policy should include deepening cooperation with international partners, reducing technological dependence, and expanding local production and organizational capabilities, which will create a basis for the safe and sustainable course of Armenia's digital development.

Keywords: *cybersecurity, information security, digital development, risk management, institutional capabilities, national security*
JEL: L86, O33
DOI: 10.52174/29538114_2025.2-168