Հավելված
ՀՀ կառավարության 2026 թվականի
նոյեմբերի 19-ի N 1691-Ն որոշման

Կ Ա Ր Գ

ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ՀԱՄԱԿԱՐԳԻ ՍՏԵՂԾՄԱՆ ԵՎ ԴՐԱ ԿԻՐԱՌՄԱՆ

1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն կարգով կարգավորվում են պետական և տեղական ինքնակառավարման մարմինների տվյալների շտեմարաններում պարունակվող տվյալների մշակման համար օգտագործվող տեղեկատվական համակարգերի և դրանց հետ փոխկապակցված ենթակառուցվածքների անվտանգության միջոցառումների համակարգի ստեղծման և դրա կիրառման կարգի հետ կապված հարաբերությունները:

2. Տեղեկատվական համակարգերի անվտանգության միջոցառումների համակարգը (այսուհետ՝ ՏՀԱՄ համակարգ) տեղեկատվական համակարգերի հիմնարար (բազային) պաշտպանության համակարգ է, որը բաղկացած է կազմակերպչական, ֆիզիկական անվտանգության և տեղեկատվական տեխնոլոգիաների անվտանգության միջոցառումներից և պարտադիր է պետական տեղեկատվական համակարգի (այսուհետ՝ ՊՏՀ) կառավարչական համակարգում գրանցված պետական մարմինների տվյալների շտեմարանների, ինչպես նաև ՊՏՀ-ին միացած այլ տեղեկատվական համակարգերի անվտանգության ապահովման համար:

3. ՊՏՀ-ին միացած այլ տեղեկատվական համակարգեր ներառում են ինչպես պետական մարմինների ենթակայությամբ գործող, այնպես էլ համայնքային (մունիցիպալ) տեղեկատվական համակարգերը, եթե դրանք ներգրավված են պետական տվյալների փոխանակման կամ պետական էլեկտրոնային ծառայությունների մատուցման միասնական ենթակառուցվածքներում: Մասնավոր (ոչ պետական) տեղեկատվական համակարգերը սույն համակարգի կարգավորման դաշտում ներառվում են միայն այն դեպքերում, երբ դրանք տեխնիկապես կամ գործառութային առումով

ինտեգրված են ՊՏՀ-ին կամ ապահովում են պետական մարմինների կողմից տրամադրվող ծառայությունների մատուցումը:

4. ՏՀԱՄ համակարգի գործունեությունը հիմնված է տեղեկատվական անվտանգության ISO/IEC 27001 ստանդարտի սկզբունքների հիման վրա՝ նպատակ ունենալով ապահովել տեղեկատվական համակարգերում մշակվող տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը:

5. ՊՏՀ ՏՀԱՄ համակարգի կառավարիչը «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքով նախատեսված հանձնաժողովն է (այսուհետ՝ Ինքնավար մարմին), որը կազմակերպում է ՏՀԱՄ համակարգի ներդրման մեթոդաբանական ապահովումը, հրապարակում է մեթոդաբանություններ և ուղեցույցներ, իրականացնում է մոնիթորինգ ու համակարգում է համապատասխանության գնահատման ընդհանուր մոտեցումները:

6. Սույն կարգը չի տարածվում «Հանրային տեղեկությունների մասին» օրենքի 11-րդ հոդվածի 5-րդ մասով նախատեսված այն տվյալների շտեմարանների վրա, որոնք ստեղծված են պաշտպանության, ազգային անվտանգության, արտաքին հարաբերությունների, կամ արտաքին հետախուզական գործունեության ոլորտներում լիազորված մարմինների կողմից և որոնց միջոցով ֆիզիկական կամ իրավաբանական անձանց ծառայություններ չեն մատուցվում:

7. ՏՀԱՄ համակարգը ներառում է տեխնիկական, կազմակերպչական և ֆիզիկական բազային համապարփակ միջոցներ՝ տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը (Confidentiality, Integrity, Availability - CIA) ապահովելու համար:

8. ՏՀԱՄ համակարգի ներդրումն իրականացվում է տեղեկատվական անվտանգության նպատակներին համապատասխանող անվտանգության դասերի որոշման և տեղեկատվական համակարգերի համար 6-րդ կետում նշված բազային անվտանգության միջոցառումների ընտրության ու ներդրման միջոցով: Ինքնավար մարմինը մշակում և իր պաշտոնական կայքում հրապարակում է տվյալների անվտանգության վերլուծության մեթոդաբանությունը, անվտանգության դասերին համապատասխանող բազային վերահսկողության կատալոգը, նվազագույն տեխնիկական բազային

պահանջները, ինչպես նաև ներդրման և լրացուցիչ անվտանգության միջոցառումների ուղեցույցները:

9. Սույն կարգում կիրառվող հասկացություններն են՝

1) **ծառայություն մատուցող** - կիրառվում է «Կիբեռանվտանգության մասին» օրենքի 3-րդ հոդվածով սահմանված իմաստով.

2) «**տվյալների անվտանգության վերլուծություն**» - տվյալների կարևորության և տեղեկատվական անվտանգության բացակայությունից կամ խախտման հետևանքով հնարավոր առաջացող վնասի գնահատում, որն իրականացվում է անվտանգության դասը որոշելու համար.

3) **բազային անվտանգության միջոցառումներ** - ստանդարտ անվտանգության միջոցառումներ, որոնք ընտրվում և կիրառվում են կախված անվտանգության դասից և տվյալները մշակող տեղեկատվական համակարգի կազմից.

4) **բազային անվտանգություն** - անվտանգության միջոցառումներ, որոնք անհրաժեշտ են տեղեկատվական անվտանգության հասնելու և պահպանելու համար.

5) **տեղեկատվական համակարգ** - կիրառվում է «Կիբեռանվտանգության մասին» օրենքի 3-րդ հոդվածով սահմանված իմաստով.

6) **տեղեկատվական անվտանգություն** - կազմակերպչական, տեխնիկական-անվտանգային միջոցառումների իրականացման ընտրության և կիրառման գործընթացների ամբողջություն.

7) **անվտանգության միջոցառումներ** - կազմակերպչական գործողություններ և միջոցներ, տեխնիկական գործընթացներ և տեխնիկական միջոցների կիրառում՝ տվյալների ձեռքբերման և պահպանման, ինչպես նաև տեղեկատվական համակարգերի տվյալների անվտանգության ապահովման համար.

8) **անվտանգության դաս** - Տեղեկատվական անվտանգության պահանջվող մակարդակը բխում է տվյալների կարևորությունից և արտահայտվում է չորս մակարդակի սանդղակով, որը բաղկացած է երեք անվտանգության ենթադասերից.

9) **անվտանգության ենթադաս** - տեղեկատվական անվտանգության ապահովման պահանջվող մակարդակ, որը բխում է չորս մակարդակի սանդղակով

արտահայտված տվյալների կարևորությունից: Անվտանգության երեք ենթադասերը բխում են տեղեկատվական անվտանգության երեք նպատակներից:

2. ՏՀԱՄ ՀԱՄԱԿԱՐԳԻ ՍԱՀՄԱՆՄԱՆ ԸՆԹԱՑԱԿԱՐԳԸ՝ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԴԱՍԵՐԸ ԵՎ ԵՆԹԱԴԱՍԵՐԸ

10. ՏՀԱՄ համակարգի սահմանման և տեղեկատվական անվտանգության համապատասխան դասը որոշելու համար տվյալների շտեմարանի կառավարիչն իրականացնում է տվյալների շտեմարանում մշակվող տվյալների վերլուծություն՝ Ինքնավար մարմնի հրապարակած մեթոդաբանության հիման վրա, որը ներառում է իրավական, գործառնական, ֆինանսական և սոցիալական ազդեցության չափանիշներ, և որոշում համապատասխան անվտանգության դասը:

11. Տվյալների շտեմարանի կառավարիչն ապահովում է ՏՀԱՄ համակարգի ներդրումը և կիրառումը՝ սույն կարգով սահմանված պահանջներին համապատասխան: ՏՀԱՄ համակարգի ներդրման և կիրառման ընթացքում, դրանց գործողության ոլորտում ընդգրկված տեղեկատվական համակարգերի նկատմամբ, պահպանվում են նաև «Ծառայություն մատուցողների կողմից շահագործվող տեղեկատվական համակարգերի (այդ թվում՝ կիրառվող տեղեկատվական տեխնոլոգիաների, ծառայությունների, գործընթացների և արտադրանքների մասով՝ հաշվի առնելով սույն օրենքի 16-րդ հոդվածի 4-րդ մասով թվարկված ոլորտների, ենթաոլորտների կամ ծառայության տեսակների առանձնահատկությունները) և կրիտիկական տեղեկատվական ենթակառուցվածքների կիբեռանվտանգության ապահովման նվազագույն պահանջները հաստատելու մասին» Տեղեկատվական համակարգերի կարգավորման հանձնաժողովի որոշմամբ սահմանված պահանջները, ինչպես նաև Հայաստանի Հանրապետության կառավարության 2026 թվականի մայիսի 14-ի N 662-Ն որոշմամբ սահմանված՝ կիբեռանվտանգության ոլորտում կիրառելի միջազգային ստանդարտները՝ դրանցով նախատեսված դեպքերում:

12. Տվյալների շտեմարանում մշակվող տվյալները դասակարգվում են ըստ անվտանգության դասերի: Նույն տվյալների շտեմարանի տարբեր տվյալներ կարող են դասակարգվել տարբեր անվտանգության դասերի: Այդ դեպքում ՏՀԱՄ

համակարգը սահմանվում է՝ հիմք ընդունելով տվյալների շտեմարանի ամենաբարձր դասում դասակարգված տվյալներին համապատասխանող անվտանգության միջոցառումները:

13. Պահանջվող անվտանգության մակարդակը որոշվում է տվյալների ամբողջականության, գաղտնիության և հասանելիության պարամետրերի միջոցով՝ հետևյալ պահանջների հաշվառմամբ՝

1) տվյալների ամբողջականություն - տվյալների ճշգրտության, ամբողջականության, արդիականության, իսկության երաշխիք և չարտոնված փոփոխություններ կատարելու հնարավորության բացառում.

2) տվյալների գաղտնիություն - տվյալներին հասանելիության հնարավորություն միայն համապատասխան լիազորություններ ունեցող անձանց համար կամ որոշակի տեխնիկական միջոցների կիրառմամբ.

3) տվյալների հասանելիություն - անհրաժեշտ տվյալներին ժամանակին և դյուրին հասանելիություն, նախապես հայտնի և պահանջվող աշխատանքային ժամերին (անհրաժեշտ և պահանջվող պահին ու անհրաժեշտ և պահանջվող ժամանակահատվածի ընթացքում) համապատասխան լիազորություններ ունեցող անձանց համար կամ տեխնիկական միջոցների կիրառմամբ:

14. Տվյալների շտեմարանում մշակվող տվյալների գաղտնիության, ամբողջականության և հասանելիության հիմնարար սկզբունքները (CIA) սահմանում է տվյալների շտեմարանի կառավարիչը՝ «Հանրային տեղեկությունների մասին» օրենքի 14-րդ հոդվածի 4-րդ մասով նախատեսված կարգավորումների շրջանակում:

15. Շտեմարանում մշակվող տվյալների վերլուծության արդյունքում տվյալների շտեմարանի կառավարիչն իրականացնում է տվյալների անվտանգության ենթադասերի որոշում՝ սույն կարգով սահմանված ընթացակարգով:

16. Տվյալների հասանելիության հիման վրա (Availability) անվտանգության ենթադասերը որոշվում են հետևյալ սանդղակով՝

1) A0 – Հասանելիություն (availability) – ոչ կարևոր, արտադրողականություն (performance) – ոչ կարևոր.

2) A1 – Հասանելիություն - 90% (շաբաթական թույլատրելի ընդհանուր անջատումներ ~ 16.8 ժամ), առավելագույն ծանրաբեռնվածության դեպքում պահանջվող արձագանքման ժամանակի թույլատրելի աճ – ժամեր (1÷10).

3) A2 – Հասանելիություն - 99% (շաբաթական թույլատրելի ընդհանուր անջատումներ ~ 1.68 ժամ), առավելագույն ծանրաբեռնվածության դեպքում պահանջվող արձագանքման ժամանակի թույլատրելի աճ – րոպեներ (1÷10).

4) A3 – Հասանելիություն – 99.9% (շաբաթական թույլատրելի ընդհանուր անջատումներ ~ 10.08 րոպե), առավելագույն ծանրաբեռնվածության դեպքում պահանջվող արձագանքման ժամանակի թույլատրելի աճ – վայրկյաններ (1÷10):

17. Տվյալների ամբողջականության հիման վրա (integrity) անվտանգության ենթադասերը որոշվում են հետևյալ սանդղակով՝

1) I0 – տեղեկության աղբյուրը, փոփոխությունների կամ ոչնչացման փաստի հայտնաբերելիությունը – ոչ կարևոր, տեղեկության ճշգրտության, ամբողջականության և արդիականության ստուգումը – ոչ անհրաժեշտ.

2) I1 – տեղեկության աղբյուրը, դրա փոփոխման և ոչնչացման փաստի հայտնաբերելիություն, տեղեկության ճշգրտության, ամբողջականության և արդիականության ստուգումն ըստ անհրաժեշտության՝ առանձին դեպքերում իրականացվող.

3) I2 – տեղեկության աղբյուրը, դրա փոփոխման և ոչնչացման փաստի հայտնաբերելիություն, տեղեկատվության ճշգրտության, ամբողջականության և արդիականության պարբերական ստուգումը պարտադիր.

4) I3 – տեղեկատվության աղբյուրը, դրա փոփոխման և ոչնչացման փաստի հայտնաբերելիություն, ապացուցողական արժեք ունեցող, տեղեկատվության ճշգրտության, ամբողջականության և արդիականության ստուգումը իրական ժամանակում իրականացվող:

18. Տվյալների գաղտնիության հիման վրա անվտանգության ենթադասերը որոշվում են հետևյալ սանդղակով՝

1) C0 – հանրային տեղեկություն. տեղեկությանը հասանելիությունը սահմանափակված չէ (բոլոր շահագրգիռ անձինք իրավունք ունեն կարդալ տվյալները.

տվյալները փոփոխելու իրավունքը որոշվում է ամբողջականության ապահովման անհրաժեշտությամբ).

2) C1 – ներքին օգտագործման տեղեկություն. տեղեկությանը հասանելիությունը թույլատրվում է այն դեպքում, եթե դրա համար դիմող անձն ունի համապատասխան լիազորություն.

3) C2 – սահմանափակ տեղեկություն. տեղեկությանը հասանելիություն թույլատրվում է միայն որոշակի օգտատերերի խմբերի համար. տեղեկությանը հասանելիություն թույլատրվում է այն դեպքում, եթե հասանելիության համար դիմող անձն ունի տեղեկության նկատմամբ իրավունք (օրինակ՝ տվյալների սուբյեկտ) կամ օրենքով նախատեսված հիմքեր.

4) C3 – օրենքով պաշտպանվող գաղտնիք համարվող տեղեկություն. C3 դասակարգման տեղեկությունը ներառում է օրենքով պաշտպանվող տեղեկատվության (բացառությամբ պետական գաղտնիք համարվող տեղեկությունների) երկու տարբեր ռեժիմներ, որոնք համակարգում պետք է հստակ տարանջատվեն՝

- Օրենքով պաշտպանվող գաղտնիք (Legally Protected Secret) – օրենքով պաշտպանված, բայց պետական գաղտնիք չհամարվող տեղեկություն (օր.՝ բանկային, հարկային, անձնական տվյալներ և այլն), որի հասանելիությունը սահմանվում է համապատասխան իրավական հիմքով և նպատակային անհրաժեշտությամբ (legal basis + need-to-know).
- Սահմանափակ ծառայողական տեղեկատվություն (Restricted Official Information) – պետական մարմնի ներքին օգտագործման համար նախատեսված տեղեկատվություն, որի բացահայտումը կարող է խաթարել գործառնական աշխատանքը կամ ներքին գործընթացները: Հասանելիությունը տրամադրվում է միայն ծառայողական անհրաժեշտության հիման վրա (need-to-know within institution):

19. Տվյալների անվտանգության դասի նշանը (կոդը) ձևավորվում է ըստ 16-րդ, 17-րդ և 18-րդ կետերի սանդղակների հերթականության, տառերի և թվերի համադրություններից (օրինակ՝ A2I3C1): Տվյալների անվտանգության դասը որոշվում է՝

1) բարձր (H), եթե տվյալների անվտանգության պրոֆիլում առնվազն մեկ ցուցիչ ունի 3 արժեք.

2) միջին (M), եթե տվյալների անվտանգության պրոֆիլում 3 արժեք չկա, սակայն առնվազն մեկ ցուցիչ ունի 2 արժեք.

3) ցածր (L), եթե տվյալների անվտանգության պրոֆիլի բոլոր ցուցիչները 0 կամ 1 են:

3. ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ՆԿԱՐԱԳՐՈՒԹՅՈՒՆԸ

20. Ծառայություն մատուցողն իրականացնում է տեղեկատվական համակարգերի, դրանց միջոցով մատուցվող ծառայությունների ու գործընթացների քարտեզագրում, պետական տեղեկատվական համակարգերի կառավարչական համակարգում գրանցում է տվյալ համակարգի ռիսկերի վերլուծությունը, ինչպես նաև պլանավորում և իրականացնում է կանխարգելիչ միջոցառումներ:

21. Ծառայություն մատուցողը պարտավոր է սույն կարգի 20-րդ կետում նշված տեղեկությունները պահպանել դրանց կազմման օրվանից առնվազն յոթ տարի, իսկ գրանցամատյանների, կոնֆիգուրացիաների, աուդիտի գրառումների և կիբեռմիջադեպերի վերաբերյալ տվյալների պահպանման ժամկետները սահմանել տարբերակված պահպանման քաղաքականությամբ՝ համաձայն Ինքնավար մարմնի ուղեցույցների, ընդ որում՝ կիբեռմիջադեպերի վերաբերյալ տվյալները պահպանվում են առնվազն երեք տարի, եթե օրենքով ավելի երկար ժամկետ նախատեսված չէ, և անհրաժեշտության դեպքում տրամադրել Ինքնավար մարմնին:

22. Ծառայություն մատուցողը պարտավոր է թարմացնել սույն կարգի 20-րդ կետում նշված տեղեկությունները՝

1) էական ազդեցություն ունեցող կիբեռմիջադեպից անմիջապես հետո.

2) համակարգում անվտանգության վրա ազդեցություն ունեցող փոփոխություն կատարելուց անմիջապես հետո.

3) ոչ ուշ, քան նախորդ թարմացումից մեկ տարի անց:

23. Տեղեկատվական համակարգերի ծրագրային ապահովման կոդի աղբյուրը (source code), տվյալները և վերականգնման հրահանգները պետք է պահուստավորվեն մեկուսացված կամ տրամաբանորեն տարանջատված անվտանգ

միջավայրերում՝ ապահովելով հավելյալ պահուստավորում, գաղտնագրում, տարբերակների կառավարում և մուտքի վերահսկում:

24. Ծառայություն մատուցողը պետք է ապահովի հետևյալ նվազագույն անվտանգության միջոցառումները և դրանց իրականացման համար անհրաժեշտ նվազագույն տեխնիկական պահանջները՝

1) տեղեկատվական համակարգ մուտքի իրավասությունների կառավարում, համակարգից օգտվողների նույնականացում և լիազորությունների սահմանում, ներառյալ դերերի վրա հիմնված հասանելիությունների կառավարումը (RBAC) և, անհրաժեշտության դեպքում, բազմագործոն նույնականացումը (MFA).

2) ծառայության մատուցման համար անհրաժեշտ տվյալների կրկնօրինակման և վերականգնման համար կանոնավոր ընթացակարգերի պատրաստում, փորձարկում և կիրառում.

3) տեղեկատվական համակարգերը գործարկող և տվյալների մշակումն ապահովող ծրագրային ապահովումների թարմացում, ամրապնդում (hardening) և խոցելիությունների պարբերական կառավարում.

4) տեղեկատվական համակարգերում կատարված գործողությունների և գրանցամատյանների գրանցում, պահպանում և մոնիթորինգ՝ գործողությունն իրականացրած անձի, գործողության տեսակի և ժամանակի նշումով.

5) ծրագրային և տեխնիկական լուծումներ՝ համակարգերի անվտանգությանը սպառնացող գործողությունները, ծրագրերը և ցանցային կամ API մակարդակի սպառնալիքները հայտնաբերելու, կանխարգելելու և դրանց արձագանքելու համար.

6) ընթացակարգեր կիբեռմիջադեպերին արձագանքելու, տեղեկատվական համակարգերի անվտանգությունը կամ ծառայության շարունակականությունը վերականգնելու համար: Միաժամանակ իրականացվում է կիբեռմիջադեպերի վերաբերյալ տվյալների գրանցում և պահպանում.

7) տվյալների պաշտպանության և գաղտնիության, անվտանգ փոխգործելիության, ինչպես նաև ծրագրային ապահովման անվտանգ մշակման պահանջների կիրառում:

25. Տվյալների շտեմարանի կառավարիչը «Հանրային տեղեկությունների մասին» օրենքի 14-րդ հոդվածի 4-րդ մասով նախատեսված կարգավորումների շրջանակում սահմանում է տվյալների շտեմարանի տվյալների անվտանգության դասերին համապատասխան կիրառվող բազային անվտանգության միջոցառումները՝ հիմք ընդունելով Ինքնավար մարմնի կողմից հրապարակված ուղեցույցները:

26. Բազային անվտանգության միջոցառումների ուղեցույցը, կախված տվյալների անվտանգության դասից, մշակում և իր պաշտոնական կայքում հրապարակում է Ինքնավար մարմինը:

27. ՏՀԱՄ համակարգի պահանջների պահպանման գնահատման նպատակով ծառայություն մատուցողը կազմակերպում է պարբերական անկախ աուդիտ՝ Ինքնավար մարմնի սահմանած ընդհանուր մոտեցումների համաձայն և տվյալների անվտանգության դասին համաչափ հաճախականությամբ, բայց ոչ պակաս, քան երեք տարին մեկ անգամ:

28. Սույն կարգով սահմանված պահանջների չկատարման կամ ոչ պատշաճ կատարման դեպքում կիրառվում են օրենքով նախատեսված պատասխանատվության միջոցներ:

29. Սույն կարգով սահմանված պահանջները չկատարելու կամ ոչ պատշաճ կատարելու դեպքում Ինքնավար մարմինը «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին» օրենքի 16-րդ հոդվածի 1-ին մասի 3-րդ կետի հիման վրա հարուցում է իրավախախտման վերաբերյալ վարույթ և Վարչական իրավախախտումների վերաբերյալ Հայաստանի Հանրապետության օրենսգրքով սահմանված կարգով կիրառում է վարչական պատասխանատվության միջոցներ:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏԻ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐ Լ. ՄԱԿՈՒՆՑ

19.11.2026
ՀԱՎԱՍՏՎԱԾ Է
ԷԼԵԿՏՐՈՆԱՅԻՆ
ՍՏՈՐԱԳՐՈՒԹՅԱՄԲ