Հավելված
ՀՀ կառավարության 2026 թվականի
մայիսի 27-ի N 767 - Ն որոշման

ԿԱՐԳ
ՊԵՏԱԿԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԻ ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՄԱՆ ՇԵՐՏԻ ՍՏԵՂԾՄԱՆ ԵՎ ԿԻՐԱՌՄԱՆ

1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն կարգով կարգավորվում են պետական տեղեկատվական համակարգի տվյալների փոխանակման շերտի ստեղծման և կիրառման պայմանները՝ ներառյալ դրա ներդրման, կառավարման և զարգացման, ինչպես նաև շերտին միանալու և այն օգտագործելու հետ կապված հարաբերությունները:
2. Սույն կարգի դրույթները չեն տարածվում «Հանրային տեղեկությունների մասին» օրենքի 11-րդ հոդվածի 5-րդ մասով նախատեսված տվյալների շտեմարանների, ինչպես նաև պետական գաղտնիք պարունակող տեղեկատվական համակարգերի վրա:
3. Սույն կարգում կիրառվող հասկացություններն են՝
   1) **տվյալների փոխանակման շերտ (այսուհետ՝ ՏՓՇ կամ ՀՏՓՇ (ADEL (Armenian Data Exhcange Layer)**՝ օգտագործվում է «Հանրային տեղեկությունների մասին» օրենքով սահմանված իմաստով.
   2) ***Իքս Ռոադ (X-Road)***՝ բաց կոդով ճարտարապետություն (այսուհետ՝ X-Road) – տեղեկատվական համակարգերի միջև ապահով և ստանդարտացված տվյալների փոխանակման համար նախատեսված միջազգային ճանաչում ունեցող բաց կոդով ծրագրային լուծում, որի տեխնիկական նկարագիրը և պայմանները սահմանվում են Տեղեկատվական համակարգերի կարգավորման հանձնաժողովի (այսուհետ՝ հանձնաժողով) կողմից.
   3) ***ՏՓՇ անդամ***՝ պետական կամ տեղական ինքնակառավարման մարմին, իրավաբանական կամ ֆիզիկական անձ, որի տեղեկատվական համակարգն օրենքով և սույն կարգով սահմանված կարգով միացված է ՏՓՇ-ին.
   4) ***տվյալը որպես ծառայություն (այսուհետ՝ տվյալների ծառայություն)***՝ ՏՓՇ անդամի կողմից մատուցվող ծառայություն, որի միջոցով ապահովվում է հասանելիություն տվյալներին և իրականացվում է թվային տվյալների փոխանակում.
   5) ***տվյալների ծառայության մատուցող***՝ ՏՓՇ անդամ, որը ՏՓՇ-ի միջոցով տվյալների ծառայություն է մատուցում այլ ՏՓՇ անդամներին.

6) ***տվյալների ծառայության օգտագործող***՝ ՏՓԾ անդամ, որն օգտագործում է այլ ՏՓԾ անդամի կողմից մատուցվող տվյալների ծառայություն.
7) ***տվյալների ծառայության հոսթ***՝ ՏՓԾ անդամ, որը սեփական տեղեկատվական համակարգը չունեցող հավակնորդին թույլ է տալիս մուտք գործել ՏՓԾ՝ իր տեղեկատվական համակարգի միջոցով.
8) ***տվյալների ծառայության վերջնական օգտագործող***՝ ֆիզիկական անձ, որն օգտագործում է տվյալների ծառայություն՝ ՏՓԾ անդամի տեղեկատվական համակարգի միջոցով.
9) ***հաղորդագրություն***՝ ***ֆորմատավորված*** տվյալների փաթեթ, որը փոխանակվում է տվյալների ծառայության մատուցողի և տվյալների ծառայության օգտագործողի միջև ՏՓԾ-ի միջոցով.
10) ***ենթահամակարգ***՝ ՏՓԾ անդամի տեղեկատվական համակարգի տեխնոլոգիապես և կազմակերպորեն սահմանված մաս՝ տվյալների ծառայության մատուցման կամ տվյալների ծառայության օգտագործման համար.
11) ***մուտքի իրավունք***՝ տվյալների ծառայության օգտագործման հնարավորության ակտիվացում ՏՓԾ ծրագրային լուծում (software).
12) ***ՏՓԾ հիմնարար մասնագիր (protocol)***՝ կանոնների համախումբ, որ ապահովում է տվյալների անվտանգ փոխանակումը համակարգչային ցանցի միջոցով.
13) ***անվտանգության սերվեր***՝ ՏՓԾ հիմնարար մասնագրի փաթեթին համապատասխանող ծրագրային ապահովում (software).
14) ***ՏՓԾ հաղորդագրության մասնագիր (protocol)***՝ ՏՓԾ հիմնարար մասնագրի մաս, որը թույլ է տալիս ՏՓԾ անդամներին փոխանակել և մշակել հաղորդագրություններ.
15) ***հարցումների մատյան (a message log)***՝ անվտանգության սերվերի բաղադրիչ մաս՝ հիմնված ՏՓԾ հիմնարար մասնագրերի վրա, որտեղ պահպանվում են ՏՓԾ-ում փոխանակված տվյալների կամ տեղեկությունների վերաբերյալ հաղորդագրությունները՝ հաստատված էլեկտրոնային կնիքով:

4. Սույն կարգում կիրառվող մյուս հասկացություններն ունեն «Հանրային տեղեկությունների մասին» օրենքով և դրա հիման վրա ընդունված այլ ենթաօրենսդրական նորմատիվ իրավական ակտերով սահմանված իմաստը:

2. ՏՓԾ-Ի ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ՍԿԶԲՈՒՆՔՆԵՐԸ

5. ՏՓԾ-ի գործունեության սկզբունքներն են՝

1) **անվտանգություն**՝ տվյալների հատկությունները, ինչպիսիք են գաղտնիությունը, ամբողջականությունը և հասանելիությունը, չեն փոխվում տվյալների՝ ՏՓԾ-ով փոխանակման ընթացքում.
2) **հասանելիություն**՝ ՏՓԾ-ի կենտրոնական բաղադրիչների թիվը նվազագույնի է հասցված, և ՏՓԾ օգտագործող երկու տեղեկատվական համակարգերի միջև տվյալների փոխանակման գործունեությունը երաշխավորված է նույնիսկ կենտրոնական բաղադրիչների խափանման դեպքում: ՏՓԾ ենթակառուցվածքը ներառում է հակամիջոցներ թե՛ ժամանակավոր խափանման, թե՛ ծառայության մերժման դեպքում.
3) **գաղտնիություն՝** գաղտնիությունն ապահովվում է տվյալների ծածկագրմամբ և ծառայության օգտագործման երկկողմանի լիազորմամբ.
4) **հարթակից (platform) և ճարտարապետությունից անկախություն**՝ ՏՓԾ-ն ապահովում է ՏՓԾ անդամի ցանկացած ծրագրային հարթակի վրա գործող տեղեկատվական համակարգին փոխանակել տեղեկություններ ծառայություն մատուցողի ցանկացած ծրագրային հարթակի վրա գործող տեղեկատվական համակարգի հետ.
5) **բազմակողմանիություն**՝ ՏՓԾ անդամը հնարավորություն ունի հարցում ներկայացնել ՏՓԾ-ի միջոցով մատուցվող բոլոր ծառայություններին՝ օրենքով և սույն կարգով սահմանված իրավունքների առկայության դեպքում:

3. ՏՓԾ-Ի ԿԱՌԱՎԱՐՈՒՄԸ ԵՎ ԶԱՐԳԱՑՈՒՄԸ

6. Հանձնաժողովը համակարգում է ՏՓԾ-ի կառավարումն ու զարգացումը և պատասխանատու է ՏՓԾ-ի անխափան և անվտանգ գործունեության համար: Հանձնաժողովը՝
   1) կառավարում է ՏՓԾ անդամների, ՏՓԾ-ում գրանցված անվտանգության սերվերների և ՏՓԾ-ում գրանցված ենթահամակարգերի մասին տեղեկատվությունը, որոնք ապահովում են տվյալների անվտանգ փոխանակումը և տվյալների ծառայություններն օգտագործելու համար անհրաժեշտ տեղեկատվությունը.
   2) կազմակերպում է ՏՓԾ-ին միանալը, ենթահամակարգի և անվտանգության սերվերի գրանցումը.
   3) մշակում է ՏՓԾ-ին անդամակցելու և օգտագործելու պայմաններն ու դրույթները և հրապարակում դրանք իր պաշտոնական կայքէջում.
   4) ապահովում է ՏՓԾ անխափան հասանելիությունը ՏՓԾ անդամին.

5) մշտադիտարկում է ՏՓԾ օգտագործումը, այդ թվում՝ հավաքել տվյալների ծառայությունների մշտադիտարկման մատյանները (լոգերը), կազմել և հրապարակել ՏՓԾ օգտագործման վիճակագրությունը՝ չանձնավորված ձևով.
6) «Կիբեռանվտանգության մասին» օրենքով սահմանված կարգով կարգավորում է, կառավարում և հսկում կիբեռմիջադեպերի գրանցմանը, կանխարգելմանը, լուծմանը և հետևանքների վերացմանն ուղղված գործողությունները.
7) օրենքով նախատեսված դեպքերում և կարգով սահմանափակում է ՏՓԾ օգտագործման հնարավորությունը.
8) խորհրդատվություն է տրամադրում ՏՓԾ անդամներին ՏՓԾ-ին վերաբերող հարցերի վերաբերյալ.
9) տեղեկացնում է ՏՓԾ անդամներին ՏՓԾ կառավարման կամ օգտագործման փոփոխությունների, ինչպես նաև բոլոր հանգամանքների կամ տեխնիկական սպասարկման աշխատանքների մասին, որոնք կարող են խոչընդոտել ՏՓԾ օգտագործմանը.
10) կառավարում և կազմակերպում է ՏՓԾ միացումը տվյալների փոխանակման այլ միջավայրերի հետ.
11) ապահովում է անվտանգության սերվերի ստանդարտ ծրագրային լուծման անվճար հասանելիությունը ՏՓԾ անդամների համար.
12) ապահովում է տվյալների ծառայության վերջնական օգտագործողի համար նախատեսված ստանդարտ ենթահամակարգի համապատասխանությունը ՏՓԾ հաղորդագրության մասնագրին և դրա ծրագրային լուծման անվճար հասանելիությունը ՏՓԾ անդամներին.
13) մշակում և իրականացնում է ՏՓԾ ենթակառուցվածքի զարգացման ծրագրերն ու ապահովում ՏՓԾ ճարտարապետական ամբողջականությունը.
14) սույն կարգով և օրենքով սահմանված դեպքերում սահմանափակում է տվյալների ծառայություններից օգտվելու համար անհրաժեշտ տեղեկատվության հասանելիությունը ՏՓԾ անդամի անվտանգության սերվերին.
15) կառավարում և զարգացնում է անդամների ու վստահության ծառայությունների գրանցման համար անհրաժեշտ լուծումները՝ ՏՓԾ գործունեությունն ու մշտադիտարկումն ապահովելու համար.
16) պահպանում է սույն կետի 5-րդ ենթակետում նշված մշտադիտարկման մատյանները (լոգերը), որոնք պարունակում են ՏՓԾ անդամի անունից հարցում կատարող անձին նույնականացնելու տվյալներ՝ դրանց հավաքագրման օրվանից հինգ տարի ժամկետով, որից հետո տվյալները դարձնում է անանուն:

4. ՏՓԾ-ԻՆ ՄԻԱՆԱԼՈՒ ՊԱՅՄԱՆՆԵՐԸ

7. ՏՓԾ-ին միանալն իրականացվում է հանձնաժողովի միջոցով:
8. ՏՓԾ-ին միանալու համար ՏՓԾ անդամության հավակնորդի տեղեկատվական համակարգը պետք է ունենա եզակի նույնականացուցիչ՝ հանձնաժողովի կողմից սահմանված ՏՓԾ տեխնիկական պայմաններին համապատասխան: Հանձնաժողովը եզակի նույնականացուցիչի հիման վրա տրամադրում է էլեկտրոնային կնիք՝ համաձայն հանձնաժողովի պաշտոնական կայքում հրապարակված պահանջների կամ հավակնորդը պարտավոր է ունենալ որակավորված էլեկտրոնային վստահության ծառայություններ՝ հանձնաժողովի կողմից սահմանված ՏՓԾ տեխնիկական պայմաններին համապատասխան:
9. Պետական մարմինների ՏՓԾ-ին միացումն իրականացվում է «Հանրային տեղեկությունների մասին» օրենքով սահմանված կարգով: Հանձնաժողովը պարտավոր է ապահովել ՏՓԾ-ի օգտագործումը պետական մարմինների համար՝ համաձայն սույն կարգում նշված ՏՓԾ սպասարկման չափանիշների:
10. Տեղական ինքնակառավարման մարմինների, իրավաբանական կամ ֆիզիկական անձանց տեղեկատվական համակարգերի (այսուհետ՝ ոչ պետական տեղեկատվական համակարգերի) միացումը ՏՓԾ-ին իրականացվում է հանձնաժողովի հետ կնքվող պայմանագրի հիման վրա, եթե ՏՓԾ-ի միջոցով միացվող տվյալների շտեմարանի կառավարչի հետ կնքվել է շտեմարանին միանալու պայմանագիր: ՏՓԾ-ին միանալու պայմանագիրը կարող է կնքվել, եթե ոչ պետական տեղեկատվական համակարգը բավարարում է ՏՓԾ-ին միանալու՝ «Հանրային տեղեկությունների մասին» օրենքով և այլ իրավական ակտերով նախատեսված պահանջները: Օրենքով և իրավական ակտերով նախատեսված պահանջները բավարարելու հանգամանքը գնահատում է հանձնաժողովը, որի արդյունքում կազմվում և տրամադրվում է եզրակացություն: ՏՓԾ-ին միացման պայմանագիրը կնքվում է հանձնաժողովի կողմից հաստատված օրինակելի ձևին համապատասխան: ՏՓԾ-ին միանալու համար գանձվելու է պետական տուրք:
11. ՏՓԾ անդամը պարտավոր է՝
    1) միանալով ՏՓԾ-ին՝ ապահովել իր տեղեկատվական համակարգի շարունակականությունը, կառավարումը, զարգացումը և անվտանգ ու անխափան գործունեությունը.
    2) ներդնել տվյալների անվտանգ և ստանդարտացված փոխանակումն ապահովող տարրերը՝ ստեղծել տվյալների փոխանակման անվտանգ համակարգ, ապահովել տվյալների փոխանակման ամբողջականությունը՝ հավաստված էլեկտրոնային կնիքով.

3) սահմանել ենթահամակարգը, համապատասխանեցնել տվյալների ծառայության մատուցման պահանջները, որոշել տվյալների ծառայության օգտագործողին՝ մուտքի իրավունքներ տրամադրելով.
4) իրականացնել միջոցառումներ՝ տվյալների ամբողջականությունը, գաղտնիությունը և օգտագործումն ապահովելու նպատակով, անվտանգության ռիսկերը մեղմելու համար, և ապահովել իրականացված միջոցառումների անկախ աուդիտ՝ առնվազն չորս տարին մեկ անգամ.
5) կատարել հանձնաժողովից ստացված ցուցումները՝ օրենքով նախատեսված դեպքերում և կարգով.
6) անհապաղ տեղեկացնել հանձնաժողովին իր կոնտակտային տվյալների ցանկացած փոփոխության մասին.
7) անհապաղ տեղեկացնել հանձնաժողովին ՏՓԾ օգտագործման հետ կապված ցանկացած խնդրի և ցանկացած հանգամանքի մասին, որը կարող է ազդել հանձնաժողովի կամ ՏՓԾ անդամի պարտավորությունների կատարման վրա.
8) անհապաղ տեղեկացնել հանձնաժողովին ՏՓԾ օգտագործման հետ կապված անվտանգության միջադեպի կամ դրա անմիջական սպառնալիքի մասին.
9) հանձնաժողովի պահանջով վերջինիս ներկայացնել անվտանգության սերվերի անվտանգության գնահատման համար անհրաժեշտ տեղեկատվությունն ու անվտանգության կանոնները, ինչպես նաև իրականացված անվտանգության միջոցառումների իրականացման նկարագրությունը.
10) հանձնաժողովի մշտադիտարկման սերվերին տրամադրել մուտքի իրավունք իր անվտանգության սերվերի մշտադիտարկման տվյալներին.
11) տվյալների փոխանակման շերտի միջոցով չփոխանակել պետական և տեղական ինքնակառավարման մարմինների կողմից մշակվող, սակայն տվյալների կատալոգում չներառված տվյալ.
12) հանձնաժողովին 48 ժամ առաջ տեղեկացնել ցանկացած նախատեսված փոփոխության կամ իրավիճակի մասին, որը կարող է կարևոր լինել ՏՓԾ-ի օգտագործման համար, այդ թվում՝ հարցումների ծավալի զգալի աճի հանգեցնող փոփոխության կամ իրավիճակի մասին.
13) միանալ ՏՓԾ թեստային միջավայրին՝ նախքան արտադրական միջավայրին միանալը, և այնտեղ տրամադրել համապատասխան ծառայությունները՝ տեխնիկական պահանջներին համապատասխան փաստաթղթավորմամբ և թեստային տվյալներով.
14) պահուստավորել ծառայության հարցումների մատյանները (լոգերը).
15) մշակել պահուստավորման ընթացակարգ, որը սահմանում է պահուստավորման հաճախականությունը և պահուստավորման ենթակա տեղեկությունների ցանկը.

16) գրանցել տվյալների ծառայության կողմից փոխանակվող տվյալները տվյալների կատալոգում.
17) գրանցել մատուցվող ծառայությունները ծառայության նկարագրությամբ և ծառայության մատուցման սկզբունքներով կառավարչական համակարգում.
18) թարմ պահել ծառայությանը վերաբերող տվյալները տվյալների կատալոգում.
19) տեղեկացնել ծառայության փոփոխությունների մասին կառավարչական համակարգի միջոցով.
20) պահպանել «Կիբեռանվտանգության մասին» օրենքով, սույն կարգով և ՏՓԾ-ին միացման պայմանագրով սահմանված պայմանները և պահանջները:

5. ՏՓԾ-ԻՆ ՄԻԱՆԱԼՈՒ ԴԻՄՈՒՄԸ ՄԵՐԺԵԼԸ

12. Հանձնաժողովը կայացնում է ՏՓԾ-ին միանալու դիմումը մերժելու մասին որոշում, եթե չեն ապահովվում ՏՓԾ-ին միանալու սույն կարգով, «Տեղեկատվական համակարգերի կարգավորման մարմնի մասին», «Կիբեռանվտանգության մասին» կամ «Հանրային տեղեկությունների մասին» օրենքներով սահմանված պահանջները:

6. ԱՆՎՏԱՆԳ ԵՎ ՍՏԱՆԴԱՐՏԱՑՎԱԾ ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՈՒՄՆ ԱՊԱՀՈՎՈՂ ՏԱՐՐԵՐԸ

13. ՏՓԾ-ում անվտանգ և ստանդարտացված տվյալների փոխանակումն ապահովվում է հետևյալ բոլոր պայմանների կատարմամբ՝
    1) տվյալների փոխանակման շերտի կիրառմամբ՝ համաձայն 7-րդ գլխի պահանջների.
    2) տվյալների փոխանակման ամբողջականության ապահովման համար էլեկտրոնային կնիքի օգտագործմամբ՝ համաձայն 8-րդ գլխի պահանջների.
    3) ենթահամակարգի սահմանմամբ՝ համաձայն 9-րդ գլխի պահանջների.
    4) տվյալների ծառայության նկատմամբ պահանջներով՝ համաձայն 11-րդ գլխի պահանջների.
    5) ՏՓԾ անդամը կարող է օգտագործել անվտանգության սերվերի միայն այն ծրագրային լուծումը, որը համապատասխանում է հանձնաժողովի կողմից սահմանած ՏՓԾ հիմնարար մասնագրին:

7. ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՄԱՆ ՇԵՐՏԻ ԿԻՐԱՌՈՒՄԸ

14. ՏՓՇ-ի կիրառումն ապահովելու համար ՏՓՇ անդամը պետք է տեղադրի անվտանգության սերվերի ծրագրային լուծումը տեղեկատվական համակարգում և գրանցի անվտանգության սերվերի նույնականացման հավաստագիր, որը պետք է համապատասխանի հանձնաժողովի կայքում հրապարակված տեխնիկական պահանջներին:
15. X-Road-ը օգտագործման համար թույլատրված անվտանգության սերվերի ծրագրային լուծում է, որը համապատասխանում է հանձնաժողովի կողմից տեխնիկական պահանջներով սահմանված ՏՓՇ հիմնարար մասնագրերին: Այլ տեխնոլոգիական լուծման հիման վրա անվտանգության սերվերի ծրագրային լուծումները պետք է համապատասխանեն հանձնաժողովի կողմից սահմանված տեխնիկական և անվտանգության չափանիշներին:
16. Անվտանգության սերվեր օգտագործելիս ՏՓՇ անդամը պարտավոր է՝
    1) ապահովել ՏՓՇ-ում փոխանակված հաղորդագրությունների՝ էլեկտրոնային կնիքով հաստատված հարցումների մատյանի գոյությունը, իսկ հարցումների մատյանի արխիվացման դեպքում մշակել հարցումների մատյանի արխիվացման ընթացակարգ, որը ներառում է արխիվացման հաճախականությունը և արխիվացվող տեղեկությունների ցանկը.
    2) որոշել այն անձանց շրջանակը, ովքեր և ինչ պայմաններով կունենան մուտք անվտանգության սերվերի արխիվացված հարցումների մատյանին՝ հարցումների մատյանի արխիվացման դեպքում.
    3) հարցումների մատյանի արխիվացման դեպքում ապահովել արխիվացված հաղորդագրությունների մշակման ժամանակ նույն գաղտնիության պահանջները, ինչպես պահանջվում է տվյալների ծառայության օգտագործման ժամանակ:
17. Հանձնաժողովի կողմից տրամադրված անվտանգության սերվեր օգտագործելիս ՏՓՇ անդամը, սույն կարգի 16-րդ կետում նշված պարտականությունները կատարելուց բացի, պարտավոր է՝
    1) անվտանգության սերվերի ծրագրային լուծումներն օգտագործել հանձնաժողովի կայքում հրապարակված ցուցումներին համապատասխան.
    2) թարմացնել անվտանգության սերվերի ծրագրային լուծումները ոչ ուշ, քան երկու ամիս անց՝ հանձնաժողովի կողմից ծրագրային լուծումների թարմացումները հասանելի դարձնելուց հետո:
18. Իր անվտանգության սերվերը մեկ այլ ՏՓՇ անդամի հետ համատեղ օգտագործելիս ՏՓՇ անդամը պետք է օգտագործի ծածկագրված կապ և երկկողմանի

նույնականացում անվտանգության սերվերի և ենթահամակարգի միացման համար:

8. ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՄԱՆ ԱՄԲՈՂՋԱԿԱՆՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄՆ ԷԼԵԿՏՐՈՆԱՅԻՆ ԿՆԻՔՈՎ

19. Տվյալների փոխանակման ամբողջականությունը և ՏՓԾ-ում փոխանակված հաղորդագրության և ՏՓԾ անդամի միջև կապի նույնականացումն ապահովվում են էլեկտրոնային կնիքով, որի ստեղծման համար ՏՓԾ անդամը պարտավոր է անվտանգության սերվերում օգտագործել օրենքով նախատեսված վստահության հետևյալ ծառայությունները՝
    1) էլեկտրոնային կնիքի որակավորված վկայականներ.
    2) վկայականների վավերականության հաստատման ծառայություն.
    3) ժամանակի դրոշմի ծառայություն:
20. ՏՓԾ անդամը կարող է օգտագործել հանձնաժողովի կողմից տրված էլեկտրոնային կնիքը:
21. ՏՓԾ-ում ստեղծված էլեկտրոնային կնիքը վավեր է, եթե օգտագործված վկայականի վավերականության հաստատման և ժամանակի դրոշմի միջև ժամանակային տարբերությունը ոչ ավելի է, քան ութ ժամը:
22. ՏՓԾ անդամին արգելվում է մշակել ՏՓԾ-ում փոխանակված տվյալները, որոնք չեն կարող հաստատվել սույն կարգի 20-րդ կետում նշված էլեկտրոնային կնիքով:

9. ՏՓԾ-ԻՆ ՄԻԱՑՎԱԾ ԵՆԹԱՀԱՄԱԿԱՐԳԸ

23. ՏՓԾ-ը կարող է օգտագործվել և տրամադրվել միայն հանձնաժողովի կողմից կառավարչական համակարգում գրանցված ենթահամակարգի կողմից:
24. Հանձնաժողովում ՏՓԾ-ը ենթահամակարգը գրանցվում է ՏՓԾ անդամի կողմից:
25. ՏՓԾ-ում կարող են գրանցվել միայն այնպիսի ենթահամակարգեր, որոնց համար նշանակված է ենթահամակարգի գործունեության համար պատասխանատու ֆիզիկական անձ և ենթահամակարգին սպասարկող անվտանգության սերվերի ադմինիստրատոր:
26. Ենթահամակարգը գրանցելուց հետո ՏՓԾ անդամը պարտավոր է նշանակել աշխատանքային տեղեր և պաշտոններ, որոնք իրավունք ունեն օգտագործել ենթահամակարգը և դրանով ենթահամակարգին տրամադրված տվյալների ծառայությունները, և կազմակերպության ներսում մուտք թույլ տալ միայն լիազորված անձանց և ապահովել ՏՓԾ-ին միացված ենթահամակարգի անվտանգ

և անխափան գործունեությունը և ՏՓԾ անդամների միջև տվյալների ծառայության օգտագործման պայմանագրի պահպանումը:

27. Հանձնաժողովն իրավունք ունի մերժել ենթահամակարգի գրանցման դիմումը կամ ջնջել գրանցված ենթահամակարգը գրանցումից, եթե չեն կատարվում սույն կարգում սահմանված պահանջներից որևէ մեկը:

10. ՏԵԽՆԻԿԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԱՀԱՆՋՆԵՐԸ

28. ՏՓԾ-ի օգտագործումը հնարավոր է միայն հանձնաժողովի կողմից նախապես տրված հավաստագրով հագեցած անվտանգության սերվերի միջոցով, որտեղ տվյալների փոխանակումը ծածկագրված է և ստորագրված անվտանգության սերվերի հավաստագրով և ապահովված կրիպտոգրաֆիկորեն կապված մատյաններով (լոգերով)՝ ապահովելու դրա հետագա չկեղծումը և ամբողջականությունը: Մատյանները (լոգերը) պետք է պահվեն առնվազն հինգ տարի: ՏՓԾ անդամը կարող է սահմանել մատյանների (լոգերի) պահպանման ավելի երկար ժամկետ:
29. ՏՓԾ-ի օգտագործմանը վերաբերող տեխնիկական խնդիրները ներկայացվում և գրանցվում են կառավարչական համակարգում:
30. ՏՓԾ-ի օգտագործմանը վերաբերող կիբեռմիջադեպերը «Կիբեռանվտանգության մասին» օրենքով սահմանված կարգով գրանցվում են կիբեռմիջադեպերի գրանցամատյանում:
31. ՏՓԾ անդամը պատասխանատվություն է կրում իր տվյալների շտեմարանը պահպանելու համար օգտագործվող տեղեկատվական համակարգի անվտանգության համար՝ «Կիբեռանվտանգության մասին» օրենքով սահմանված պահանջներին համապատասխան:

11. ՏՎՅԱԼՆԵՐԻ ԾԱՌԱՅՈՒԹՅԱՆ ՆԿԱՏՄԱՄԲ ՊԱՀԱՆՋՆԵՐԸ

32. Տվյալների ծառայությունը պետք է՝
    1) համապատասխանի հանձնաժողովի կողմից սահմանված ՏՓԾ հաղորդագրությունների մասնագրին.
    2) փաստաթղթավորված լինի, թարմացված և հանձնաժողովի տեխնիկական պահանջներին համապատասխան, ներառի տեղեկատվություն տվյալների ծառայությունից օգտվելու համար անհրաժեշտ անվտանգության միջոցառումների մասին՝ հաշվի առնելով տվյալների ծառայությունում ներառված տվյալների կազմը և տվյալների ծառայության բնույթը.
    3) հասանելի և կիրառելի լինի ՏՓԾ թեստային միջավայրում:

12. ՏՎՅԱԼՆԵՐԻ ԾԱՌԱՅՈՒԹՅԱՆ ՏՐԱՄԱԴՐՈՒՄԸ ԵՎ ՕԳՏԱԳՈՐԾՈՒՄԸ

33. Պետական մարմինների տեղեկատվական համակարգերի միջև տվյալների ծառայությունը մատուցվում է օրենքով սահմանված կարգով հաստատված այն շտեմարանի կանոնակարգի հիման վրա, որը մատուցում է տվյալների ծառայությունը: Շտեմարանի կանոնակարգը պետք է սահմանի՝
    1) տվյալների ծառայությունից օգտվելու համար անհրաժեշտ տեղեկատվական անվտանգության միջոցառումները և տվյալների ծառայության օգտագործողի ենթահամակարգից պահանջվող կազմակերպչական, ֆիզիկական և տեղեկատվական տեխնոլոգիաների հետ կապված անվտանգության միջոցառումները՝ հաշվի առնելով մշակվող տվյալների կազմը.
    2) տվյալների ծառայությունը երրորդ կողմին որպես տվյալների ծառայության հոսթ մատուցելու թույլտվությունը՝ համաձայն սույն կարգի 13-րդ գլխի պահանջների.
    3) ծառայության սպասարկման չափանիշները:
34. Տվյալների ծառայություն մատուցողը պարտավոր է՝
    1) գրանցել տվյալների ծառայությունը՝ ներառյալ տվյալների ծառայության տեխնիկական նկարագրությունն անվտանգության սերվերում և թարմացնել անվտանգության սերվերում տվյալների ծառայության նկարագրությունը.
    2) ապահովել, որ տվյալների ծառայությունների օգտագործողը ձեռնարկի բավարար միջոցներ՝ տվյալների ամբողջականությունը, գաղտնիությունը և մշակման պիտանիությունն ապահովելու համար՝ անվտանգության ռիսկերը մեղմելու համար.
    3) ապահովել մուտքի իրավունք համաձայն շտեմարանի կանոնակարգի:
35. Տվյալների ծառայության օգտագործողները և մատուցողները պարտավոր են՝
    1) ամրագրել անվտանգության սերվերում ստացված հաղորդագրությունները ժամանակային դրոշմով.
    2) հավաստել տվյալների փոխանակման ամբողջականությունը սույն կարգի 8-րդ գլխում նշված էլեկտրոնային կնիքի միջոցով:

13. ՏՎՅԱԼՆԵՐԻ ԾԱՌԱՅՈՒԹՅԱՆ ՀՈՍԹԻՆԳԸ

36. Սեփական տեղեկատվական համակարգը չունեցող հավակնորդին ՏՓԾ անդամը կարող է ենթահամակարգին մուտքի իրավունք տրամադրել միայն այն դեպքում, եթե՝
    1) ՏՓԾ անդամը մշակել և հրապարակել է ընթացակարգ, որը ներառում է տվյալների ծառայության հոսթինգի հիմքեր.

2) ՏՓԾ անդամը գրանցվել է որպես ՏՓԾ-ում տվյալների ծառայության հոսթ:

37. Տվյալների հոսթինգի ընթացակարգը պետք է պարունակի՝
    1) տվյալների հոսթինգի հիմքերը.
    2) տվյալների ծառայությունն օգտագործող ենթահամակարգի կողմից երրորդ կողմի նույնականացման և լիազորման ընթացակարգը.
    3) տվյալների ծառայությունն օգտագործող ենթահամակարգի կողմից երրորդ կողմի նույնականացման և լիազորման մատյանների (լոգերի) արխիվացման ընթացակարգը և մատյանների (լոգերի) պահպանման ժամկետը.
    4) ՏՓԾ հարցումների մատյանի (լոգերի) արխիվացման և արխիվ մուտք գործելու կարգը և պահպանման ժամկետը:
38. ՏՓԾ անդամը, որպես տվյալների ծառայության հոսթ, պետք է.
    1) պահպանի իր կողմից սահմանված տվյալների ծառայության հոսթինգի ընթացակարգը.
    2) տեղեկացնի հանձնաժողովին և այն տվյալների ծառայության մատուցողին, որի տվյալների ծառայությանը հոսթը մուտքի իրավունք ունի, տվյալների ծառայության հոսթինգի ընթացակարգի ցանկացած փոփոխության մասին:

14. ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՄԱՆ ՇԵՐՏՈՒՄ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՊԱՅՄԱՆՆԵՐԸ

39. ՏՓԾ օգտագործման շրջանակներում հանձնաժողովը մշակում է այն անձնական տվյալները, որոնք հնարավորություն են տալիս նույնականացնել ՏՓԾ անդամի անունից հարցում ներկայացրած անձին: Նշված տվյալները հավաքագրվում են տվյալների ծառայության մշտադիտարկման գրանցամատյանում: Անձնական տվյալների մշակումն իրականացվում է «Անձնական տվյալների պաշտպանության մասին» օրենքի պահանջներին համապատասխան:
40. Մշտադիտարկման գրանցամատյանում հավաքագրվում են հետևյալ տվյալները՝
    1) այն անձի հանրային ծառայությունների համարանիշը, ով ՏՓԾ անդամի անունից հարցում ներկայացրել ՏՓԾ այլ անդամի.
    2) հարցումն ուղարկելու և պատասխանն ստանալու ամսաթվերը և ժամերը. ՏՓԾ միջավայրի, ՏՓԾ անդամի և դրանց ենթահամակարգի անվանումները.
    3) օգտագործված ծառայության կոդը և տարբերակի նույնականացուցիչները, հարցման և պատասխանի չափերը, ինչպես նաև կցված փաստաթղթերի քանակը:
41. Հանձնաժողովը պահպանում է մշտադիտարկման գրանցամատյանի տվյալները հավաքագրումից հետո հինգ տարի: Նշված ժամկետից հետո անձնական տվյալներ

պարունակող մասը (այսինքն՝ հանրային ծառայությունների համարանիշը) հեռացվում է գրանցամատյանից և տվյալները պահպանվում են ոչ անձնական ձևաչափով՝ մշտապես:

42. Հանձնաժողովը մշտադիտարկման գրանցամատյանի տվյալները կարող է օգտագործել հետևյալ նպատակներով՝
    1) կիբեռհարձակումների, կիբեռմիջադեպերի և կիբեռսպառնալիքների վերլուծության, կանխման, հայտնաբերման, արձագանքման ու լուծման համար.
    2) սարքային կամ ծրագրային կամ ցանցային միացման կամ ցանկացած այլ բնույթի տեխնիկական խափանումները վերլուծելու, հայտնաբերելու և վերացնելու համար.
    3) ՏՓԾ անդամների կողմից հաղորդված տեխնիկական խնդիրների պատճառները պարզելու և վերացնելու համար.
    4) ՏՓԾ անդամներից ստացված տեղեկատվության մշակման համար (հնարավոր անվտանգության խնդիրների կամ տեխնիկական խափանումների վերաբերյալ ծանուցումներ):
43. Հանձնաժողովը մշտադիտարկման գրանցամատյանի տվյալները բացահայտում է՝
    1) ՏՓԾ օգտագործման վերաբերյալ վիճակագրական տվյալները հանձնաժողովի կայքում հրապարակելու միջոցով: Նշված վիճակագրական տվյալները հրապարակվում են որպես բաց տեղեկություններ՝ ընդհանրացված և չեն պարունակում անձնական տվյալներ.
    2) ՏՓԾ համակարգի և ծառայությունների մատուցման ադմինիստրատորներին, ովքեր անմիջականորեն ներգրավված են ՏՓԾ շահագործման գործընթացներում.
    3) կիբեռմիջադեպերը և կիբեռհարձակումները վերլուծող և ուսումնասիրող պետական մարմինների ծառայողներին.
    4) օրենքով նախատեսված այլ դեպքերում (օրինակ՝ քրեական դատավարության ընթացքում իրավապահ մարմնին կամ տվյալների սուբյեկտին՝ նրանց հարցման հիման վրա):
44. Գրանցամատյաններին մուտքը կազմակերպվում է խիստ փաստաթղթավորված ձևով՝ հիմնվելով մուտքի իրավունքների կամ լիազորությունների վրա:

15. ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆԱԿՄԱՆ ՇԵՐՏԻ ՍՊԱՍԱՐԿՄԱՆ ՉԱՓԱՆԻՇՆԵՐԸ

45. Հանձնաժողովի կողմից ՏՓԾ կենտրոնական բաղադրիչների սպասարկման չափանիշներն են՝

1) ՏՓԾ արտադրական միջավայրի ենթակառուցվածքների պլանային սպասարկումը տեղի է ունենում յուրաքանչյուր ամսվա երրորդ հինգշաբթի օրը՝ ժամը 18:00-ից մինչև 01:00-ն.
2) ՏՓԾ անդամները տեղեկացվում են ծառայությունների աշխատանքային ժամերին ՏՓԾ արտադրական միջավայրի ցանկացած ընդհատման և ցանկացած մեծածավալ սպասարկման աշխատանքների մասին առնվազն 2 աշխատանքային օր առաջ.
3) տեղեկատվական համակարգի մատյանները (լոգերը) պահվում են մեկ տարի, բացառությամբ մշտադիտարկման մատյանների (լոգերի), որոնք պահվում են դրանց հավաքագրումից հետո հինգ տարի, որից հետո դրանք դառնում են անանուն.
4) աշխատանքային ժամանակը համաձայնեցված ժամանակահատված է, որի ընթացքում ՏՓԾ անդամին պետք է տրամադրվի ծառայության օգնություն (խորհրդատվություն օգտագործման վերաբերյալ, չպլանավորված ընդհատումների լուծումներ գտնելը և այլն): Աշխատանքային ժամանակը սահմանվում է երկուշաբթի-ուրբաթ՝ 9:00-ից մինչև 18:00.
5) ՏՓԾ անդամի կողմից կենտրոնական բաղադրիչներին միաժամանակյա հարցումների թույլատրելի առավելագույն քանակը գլոբալ կարգավորման համար սահմանվում է 10 հարցում մեկ րոպեում.
6) պլանավորված ընդհատումը նախապես համաձայնեցված ժամանակահատված է, որի ընթացքում ծառայությունը անհասանելի է: Պլանավորված ընդհատումներ են համարվում միայն ծառայության աշխատանքային ժամերին տեղի ունեցող պլանավորված ընդհատումները: Պլանավորված ընդհատումներն օգտագործվում են սպասարկման, փորձարկման կամ բարելավման համար: Պլանավորված ընդհատումների տևողությունը հաշվարկվում է աշխատանքային ժամերով (բացառությամբ ընդհատման մասին նախապես ծանուցելու ժամանակի): Սահմանվում է՝ նախատեսված ընդհատման մասին նախապես տեղեկացնելու ժամանակը - 48 ժամ, պլանավորված ընդհատման առավելագույն տևողությունը - 8 ժամ, տարեկան պլանավորված ընդհատումների թույլատրելի առավելագույն տևողությունը - 24 ժամ, ամսական պլանավորված ընդհատումների առավելագույն թույլատրելի քանակը - 2.
7) ծառայության վերականգնման ընթացքում անհասանելի տվյալների առավելագույն քանակը, այսինքն՝ ծառայության վերականգնման կետի դասը սահմանվում է 24 ժամ.

8) գլոբալ կարգավորման հարցման արձագանքման ժամանակը (հարցումների 90%-ը պետք է տեղավորվի առավելագույն տևողության մեջ) սահմանվում է՝ միջին տևողությունը - 5 վայրկյան, առավելագույն տևողությունը - 30 վայրկյան.
9) չպլանավորված ընդհատման առավելագույն տևողությունը՝ առավելագույն թույլատրելի ժամանակահատվածը, որի ընթացքում պետք է վերականգնվի ծառայության գործունեությունը սահմանվում է 24 ժամ: Ծառայությունը վերականգնվում է աշխատանքային ժամերի ընթացքում: Տարեկան չպլանավորված ընդհատումների թույլատրելի առավելագույն տևողությունը սահմանվում է 72 ժամ:

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ՎԱՐՉԱՊԵՏԻ ԱՇԽԱՏԱԿԱԶՄԻ
ՂԵԿԱՎԱՐԻ ՏԵՂԱԿԱԼ Ա. ԽԱՉԱՏՐՅԱՆ

29.05.2026
ՀԱՎԱՍՏՎԱԾ Է
ԷԼԵԿՏՐՈՆԱՅԻՆ
ՍՏՈՐԱԳՐՈՒԹՅԱՄԲ