Հավելված

ՀՀ տրանսպորտի և կապի նախարարի

« 20 » 05 2011թ. N 275-Ա հրամանի

«Հավելված
ՀՀ տրանսպորտի և կապի նախարարի
08 . 04 . 2011թ. N 169-Ա հրամանի

ԹՎԱՅԻՆ ՏԱԽՈԳՐԱՖԻ ՀԱՄԱԿԱՐԳԻ ՀԱՄԱՐ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԻՐԱՎԱՍՈՒ ՄԱՐՄՆԻ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆԸ

Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարություն

Չափման համակարգ

Տրամադրված է	Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարության կողմից Նալբանդյան 28, Երևան
Տեղեկատվություն	Պատասխանատու անձի կոնտակտային տվյալները
Հեղինակներ	Լեհական արժեթղթերի արտադրության ֆաբրիկա <<PWPW>> ԲԸ և Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարություն
Տարբերակ	0.4
Ամսաթիվ	04-04-2011

Փաստաթղթի հաստատում

	Անուն, Ազգանուն	**Կազմակերպություն**	**Ամսաթիվ**	**Ստորագրություն**
Վիկտոր Մահիյու	Մահմետ Քոլակ	ԵԵՀՄ	02/05/2011	

Հայաստանի Հանրապետության թվային տախոգրաֆի համակարգի հավաստագրման քաղաքականության տարբերակների նախապատմություն

Տարբերակ	Ամսաթիվ	Փոփոխման նկարագրություն
0.1 տարբերակի նախագիծ	16-02-2011	Նախնական տարբերակ
0.2	18-02-2011	Հանված տախոգրաֆի և արագության սենսորների մասեր
0.3	21-02-2011	Խմբագրական փոփոխություններ
0.4	04-04-2011	Վերջնական խմբագրական փոփոխություններ

Համապատասխան պահանջներ

ԵԵՀՄ քաղաքականության տարբ.2.1	ԱՊ Հայաստանի Հանրապետության քաղաքականություն	Դիտողություններ
§5.3.1	§1.1	
§5.3.2	§6.2.1, §6.2.3, §6.2.4, §6.4	
§5.3.3	§6.2.1, §6.2.3 , §9.3.1	
§5.3.4	§6.2.2	
§5.3.5	§6.2.1	
§5.3.6	§6.4	
§5.3.7	§6.4	
§5.3.8	§6.4	
§5.3.9	§6.4	
§5.3.10	§6.4	
§5.3.11	§6.2.7	
§5.3.12	§5.1.1, §7.1, §7.2	
§5.3.13	§3.1.2, §5.1.7.3, §6.2.1, §6.2.3, §7.1, §7.2	
§5.3.14	§3.1.6, §5.1.7.3, §6.2.3, §7.2.3	
§5.3.15	§6.2.4	
§5.3.16	§5.1.7.3, §6.4, §7.2.3	
§5.3.17	§6.2.5, §7.2.5	
§5.3.18	§6.3	
§5.3.19 §5.3.20	Կիրառելի չէ	Հայաստանի Հանրապետությունում չկան արագության սենսորներ արտադրողներ: Եթե հետագայում ԱՊՄ-ն ստորագրի համաձայնագիր արագության սենսորների առաքման վերաբերյալ, ապա համապատասխան քաղաքականությունը կլրամշակվի և նորից կներկայացվի ԵԵՀՄ-ի հաստատմանը:
§5.3.21	§3.1.4, §6.3	
§5.3.22	Կիրառելի չէ	Հայաստանի Հանրապետությունում չկան տախոգրաֆ արտադրողներ: Եթե հետագայում ԱՊՄ-ն ստորագրի համաձայնագիր արագության սենսորների առաքման վերաբերյալ, ապա համապատասխան քաղաքականությունը

		կլրամշակվի և կրկին կներկայացվի ԵԵՀՄ-ի հաստատմանը:
§5.3.23	§3.4.1, §6.3	
§5.3.24	§6.3	
§5.3.25	Կիրառելի չէ	Կիրառելի է միայն թվային տախոգրաֆի քարտերի համար: Հայաստանի Հանրապետությունում չկան թվային տախոգրաֆներ արտադրողներ:
§5.3.26	§6.1, §6.2.1	
§5.3.27	§6.2	
§5.3.28	§6.2.3	
§5.3.29	§8.1.1	
§5.3.30	§6.2.3, §8.5	
§5.3.31	§8.7, §8.9	
§5.3.32	§8.4	
§5.3.33	§8.4	
§5.3.34	Կիրառելի չէ	Հայաստանի Հանրապետությունում չկան թվային տախոգրաֆներ արտադրողներ:
§5.3.35	§5.1.2, §5.1.7.5	
§5.3.36	§6.2.6	
§5.3.37	§9.7, §9.7.2	
§5.3.38	§9.1, §9.2	
§5.3.39	§9.3.2, §9.3.3, §9.3.4, §9.3.5	
§5.3.40	§9.5, §9.6	
§5.3.41	§10	
§5.3.42	§12	
§5.3.43	§11.2	
§5.3.44	§11.1	
§5.3.45	§11.5	
§5.3.46	§11.4	

Բովանդակություն

1. Ներածություն

Սույն փաստաթուղթը հանդիսանում է Հայաստանի Հանրապետության թվային տախոգրաֆի համակարգի հավաստագրման քաղաքականությունը:

Սույն քաղաքականությունը համապատասխանում է

- Տախոգրաֆ համակարգի մասին Խորհրդի կանոնակարգին, 2135/98,
- Հանձնաժողովի 1360/2002 կանոնակարգին (այսուհետ՝ կանոնակարգ),
- <<Ազգային հավաստագրման մարմնի (այսուհետ՝ ՀՄ) քաղաքականության հայտարարությանը և ձևանմուշին>>,
- <<Ընդհանուր անվտանգության հայտարարություններին>>:

1.1. Պատասխանատու կազմակերպություն

Սույն քաղաքականության համար պատասխանատու է Հայաստանի Հանրապետությունում իրավասու պետական կառավարման մարմինը (այսուհետ՝ ՀՀ-Մ):
Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարությունը:
Երևան, Նալբանդյան 28:
http://www.mtc.am

Հայաստանի Հանրապետությունում քարտ տրամադրող մարմին (այսուհետ՝ ՔՏՄ) է նշանակված Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարությունը:
Երևան, Նալբանդյան 28:
http://www.mtc.am

Հայաստանի Հանրապետությունում Անդամ-պետության հավաստագրող մարմին (այսուհետև՝ ԱՊՀՄ) է նշանակված արժեթղթերի արտադրության լեհական ֆաբրիկա <<ՊՎՊՎ>> բաժնետիրական ընկերությունը:
Կարցունկովսկայի փողոց 30, 02-871 Վարշավա,
Լեհաստան:

Հայաստանի Հանրապետությունում քարտերի անհատականացման կազմակերպություն (այսուհետև՝ ՔԱԿ) է նշանակված արժեթղթերի արտադրության լեհական ֆաբրիկա <<ՊՎՊՎ>> բաժնետիրական ընկերությունը:
Կարցունկովսկայի փողոց 30, 02-871 Վարշավա,
Լեհաստան:

ՀՀ-ԱՊՀՄ-ն կամ ՀՀ-ՔԱԿ-ը կարող են իրենց վերապահված գործողությունների որոշ մասերը փոխանցել ենթակապալառուների կամ այլ սպասարկող գործակալությունների, որոնց դիմելը չի նվազեցնում ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔԱԿ-ի ընդհանուր պատասխանատվությունները:

1.2. Հաստատում

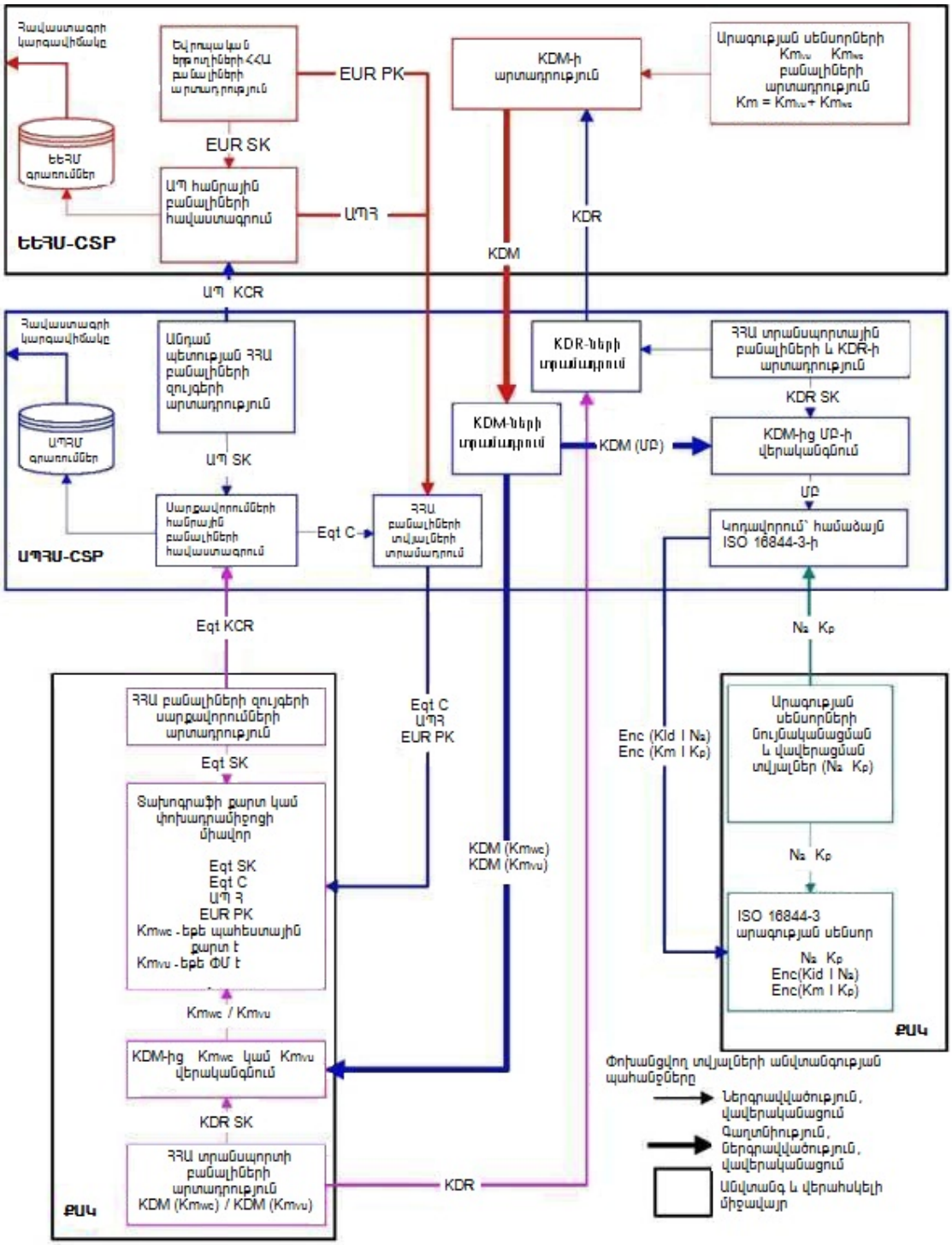
ՀՀ-Մ քաղաքականությունը հաստատված է.
Եվրոպական Հանձնաժողովի Թվային տախոգրաֆների երթուղիների հավաստագրման մարմնի հետագծելիության և խոցելիության գնահատման բաժին
Եվրոպական հանձնաժողով
Միավորված հետազոտական կենտրոն, ISPRA հաստատություն (TP.360)
Վիա Է. Ֆերմի, 1
Ի-21020 Իսպրայի (ՎՄ) միջոցով
02.05.2011 թ., No Ares (2011)475597-ով

1.3. Հասանելիություն և կոնտակտային տվյալներ

Իրավասու մարմնի քաղաքականությունը հանրության համար հասանելի է http://www.mtc.am կայք էջում:
Սույն ՀՀ-Մ քաղաքականությանն առնչվող հարցերը պետք է հասցեագրվեն
Հայաստանի Հանրապետության տրանսպորտի և կապի նախարարությանը
Երևան, Նալբանդյան 28
http://www.mtc.am

2. Շրջանակ և կիրառելիությունը

Սույն իրավասու մարմնի քաղաքականությունը վավեր է միայն թվային տախոգրաֆի համակարգի համար:
ՀՀ-ԱՊՀՄ-ի կողմից տրամադրվող բանալիները և հավաստագրերը կիրառելի են միայն թվային տախոգրաֆի համակարգի շրջանակում:
Համակարգի կողմից տրամադրվող քարտերը կիրառելի են միայն թվային տախոգրաֆի համակարգի շրջանակում:
Ստորև ներկայացված է թվային տախոգրաֆի համակարգի շրջանակում սույն իրավասու մարմնի քաղաքականության սխեման:



3. Ընդհանուր դրույթներ

Սույն բաժնում նախատեսված են դրույթներ, որոնք առընչվում են ԱՊՄ-ի, ՀՀ-ՔՏՄ-ի, ՀՀ-ԱՊՀՄ-ի, ՀՀ-ՔԱԿ-ի, սպասարկող գործակալությունների և օգտագործողների համապատասխան պարտավորություններին և օրենսդրությանը ու վեճերի լուծման ընթացակարգերին:

3.1. Պարտավորություններ

Սույն բաժինում նախատեսված են դրույթներ, որոնք առընչվում են համապատասխանաբար՝

- ԱՊՄ-ին և ՀՀ-ՔՏՄ-ին,
- ՀՀ-ԱՊՀՄ-ի և համապատասխան ծառայություն մատուցող գործակալությանը (առկայության դեպքում),
- ՀՀ-ՔԱԿ-ի և համապատասխան ծառայություն մատուցող գործակալությանը (առկայության դեպքում),
- Օգտագործողների (քարտատերերի, ՓՄ արտադրողների և արագության սենսորներ արտադրողների) պարտավորություններին:

3.1.1. ԱՊՄ-ի և ՀՀ-ՔՏՄ-ի պարտավորություններ

Սույն քաղաքականության շրջանակներում՝ ԱՊՄ-ն և ՀՀ-ՔՏՄ-ն ունեն հետևյալ պարտավորությունները.
ԱՊՄ-ն պարտավոր է՝
1) Հաստատել Հայաստանի Հանրապետության թվային տախոգրաֆի հավաստագրման քաղաքականությունը,
2) Նշանակի ՀՀ-ԱՊՀՄ և ՀՀ-ՔԱԿ,
3) Աուդիտի ենթարկել ՀՀ-ԱՊՀՄ-ն և ՀՀ-ՔԱԿ-ն՝ ներառյալ համապատասխան ծառայություններ մատուցող գործակալությունները,
4) Հաստատի ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կողմից ներկայացված փորձի մասին վկայող հայտարարությունը,
5) Սույն քաղաքականության մասին տեղեկացնի նշանակված կողմերին,
6) Սույն քաղաքականության մասին տեղեկացնի ՓՄ արտադրողներին և արագության սենսորներ արտադրողներին,
7) Ներկայացնել սույն քաղաքականությունը Հանձնաժողովի հաստատմանը:

ՀՀ-ՔՏՄ-ն պարտավոր է՝
1) Ապահովել, որ թվային տախոգրաֆի քարտերի պատվիրման ժամանակ ՀՀ-ԱՊՀՄ-ին և ՀՀ-ՔԱԿ-ին տրամադրվի դիմումատուի մասին ճշգրիտ տվյալներ,
2) Թվային տախոգրաֆի քարտեր օգտագործողներին տեղեկացնի սույն քաղաքականության պահանջների մասին,

3.1.2. ՀՀ-ԱՊՀՄ-ի պարտավորություններ

Նշանակված ՀՀ-ԱՊՀՄ-ն պարտավոր է՝
1) Կատարի սույն քաղաքականությամբ սահմանված պահանջները,
2) Հրապարակի ՀՀ-ԱՊՀՄ սույն քաղաքականությունը ընդգրկող գործնական հայտարարությունը, որը պետք է հաստատվի ԱՊՄ-ի կողմից,
3) Սույն քաղաքականության պահանջներին համապատասխան կազմակերպի համապատասխան միջոցառումներ, հաստատի ֆինանսական աղբյուրները և

վնասների համար կրի պատասխանատվություն:

ՀՀ-ԱՊՀՄ-ն պետք է ապահովի, որ սույն քաղաքականությամբ իրեն վերապահված բոլոր պահանջները կիրառվեն:
ՀՀ-ԱՊՀՄ-ն պատասխանատու է սույն քաղաքականությամբ սահմանված ընթացակարգերի համար, նույնիսկ այն դեպքում երբ ՀՀ-ԱՊՀՄ-ի սահմանված գործառույթներն իրականացվում են ենթակապալառուների կամ սպասարկող գործակալությունների կողմից: ՀՀ-ԱՊՀՄ-ն պատասխանատու է համապատասխան ծառայություններ մատուցող ցանկացած ենթակապալառուի կամ սպասարկող գործակալության կողմից մատուցած բոլոր ծառայությունների, դրանց փորձի և սույն քաղաքականության պահանջների ապահովման համար:

3.1.3. ՀՀ-ՔԱԿ-ի պարտավորություններ

Նշանակված ՀՀ-ՔԱԿ-ը պարտավոր է՝

1) Կատարի սույն քաղաքականությամբ իրեն վերապահված պահանջները,
2) Հրապարակի ՀՀ-ՔԱԿ-ի սույն քաղաքականությունը ընդգրկող գործնական հայտարարությունը, որը պետք է հաստատվի ԱՊՄ-ի կողմից:
3) Հաստատել սույն քաղաքականության պահանջներից բխող համապատասխան կազմակերպչական միջոցառումներ և ֆինանսական աղբյուրներ, ինչպես նաև վնասների համար կրել պատասխանատվություն:

ՀՀ-ՔԱԿ-ը պետք է ապահովի, որ սույն քաղաքականությամբ սահմանված բոլոր պահանջները կատարվեն:
ՀՀ-ՔԱԿ-ը կրում է պատասխանատվություն սույն քաղաքականությամբ սահմանված ընթացակարգերի համար, նույնիսկ այն դեպքում երբ սահմանված գործառույթներն իրականացվում են ենթակապալառուների կամ սպասարկող գործակալությունների կողմից:

3.1.4. Սպասարկող գործակալության պարտավորություններ

Սպասարկող գործակալությունը պայմանագրային պահանջներին համապատասխան ունի պարտավորություններ ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի, ինչպես նաև օգտագործողների նկատմամբ:

3.1.5. Քարտատիրոջ պարտավորություններ

ՀՀ-ՔՏՄ-ն պետք է համաձայնագրի միջոցով (տես 5.1.2) քարտը օգտագործողին (ներառյալ կազմակերպությանը) պարտավորեցնի իրականացնել հետևյալ պարտականությունները.

1) Սույն քաղաքականության պահանջներին համապատասխան ՀՀ-ՔՏՄ ներկայացնել ճշգրիտ և ամբողջական տվյալներ՝ մասնավորապես հաշվառման վայրի վերաբերյալ,
2) բանալիները և հավաստագիրը պետք է կիրառվեն միայն տախոգրաֆ համակարգում,

3) քարտը պետք է կիրառվի միայն Տախոգրաֆ համակարգում,
4) սարքավորումների, բանալու և քարտի չլիազորված օգտագործումից խուսափելու համար պետք է իրականացվի խելամիտ աշխատանք,
5) օգտագործողը պետք է կիրառի միայն իր բանալիները, հավաստագիրը և քարտը (համաձայն կանոնակարգ 14.4.a),
6) օգտագործողը պետք է ունենա միայն մեկ վավեր վարորդական քարտ (համաձայն կանոնակարգ 14.4.a),
7) օգտագործողը կարող է միայն հատուկ և արդարացված դեպքերում ունենա արհեստանոցի և կազմակերպության քարտ (համաձայն հավելված 1B VI:1), կամ արհեստանոցի և վարորդական քարտ, կամ մի քանի արհեստանոցի քարտեր,
8) օգտագործողը չպետք է կիրառի վնասված կամ ժամկետանց քարտ (համաձայն կանոնակարգ 14.4.a),
9) օգտագործողը պետք է առանց ուշացման (բացառությամբ խելամիտ դեպքերի) տեղեկացնի ՀՀ-ՔՏՄ-ին մինչև հավաստագրով սահմանված վավերականության ժամկետի ավարտը հետևյալի մասին՝
   - սարքավորումների, բանալու կամ քարտի կորուստի, գողություն կամ պոտենցիալ վտանգի (համաձայն կանոնակարգ 15.1),
   - հավաստագրի բովանդակությունը ոչ ճշգրիտ է կամ դառնում է ոչ ճշգրիտ:

3.1.6. ՓՄ արտադրողների պարտավորություններ (անհատականացնող կազմակերպության դեր ունեցող)

Հայաստանի Հանրապետության համար կիրառելի չէ և ընդգրկված չէ սույն քաղաքականության շրջանակներում:

3.1.7. Արագության սենսորներ արտադրողների պարտավորություններ

Հայաստանի Հանրապետության համար կիրառելի չէ և ընդգրկված չէ սույն քաղաքականության շրջանակներում:

3.2. Պատասխանատվություն

ՀՀ-ԱՊՀՄ-ն և ՀՀ-ՔԱԿ-ը պատասխանատվություն չի կրում քարտ օգտագործողների նկատմամբ, կրում է միայն ԱՊՄ-ի և ՀՀ-ՔՏՄ-ի հանդեպ:

Քարտ օգտագործողների համար պատասխանատու է ԱՊՄ-ն և ՀՀ-ՔՏՄ-ն:

ԱՊՄ-ն և ՀՀ ՔՏՄ-ն պատասխանատու է՝

Տախոգրաֆ քարտերը, բանալիները և հավաստագրերը կիրառելի են միայն Տախոգրաֆ համակարգի շրջանակներում: Տախոգրաֆ համակարգում առկա ցանկացած այլ հավաստագիր սույն քաղաքականության պահանջներին հակասում է հետևաբար ԱՊՄ-

ն, ՀՀ-ՔՏՄ-ն, ՀՀ-ԱՊՀՄ-ն և ոչ էլ ՀՀ-ՔԱԿ-ը պատասխանատվություն չեն կրում դրանց համար:

3.2.1. Քարտ օգտագործողների և վստահելի կողմերի նկատմամբ ԱՊՄ-ի և ՀՀ-ՔՏՄ-ի պատասխանատվություն

ԱՊՄ-ն և ՀՀ-ՔՏՄ-ն իրենց կողմից անփութորեն կատարված աշխատանքի պատճառով (սույն քաղաքականության պահանջներին անհամապատասխան) ստացված վնասների համար կրում են պատասխանատվություն: Եթե ԱՊՄ-ն կամ ՀՀ-ՔՏՄ-ն գործել են սույն քաղաքականության պահանջներին համապատասխան ապա չի համարվում, որ նրանք գործել են անփութորեն:

3.2.2. ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի պատասխանատվությունը ԱՊՄ-ի և ՀՀ-ՔՏՄ-ի նկատմամբ

ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի կողմից անփութորեն կատարված աշխատանքի պատճառով (սույն քաղաքականության պահանջներին և համապատասխան հայտարարությանը անհամապատասխան) ստացված վնասների համար կրում են պատասխանատվություն ԱՊՄ-ի և ՀՀ-ՔՏՄ-ի նկատմամբ: Եթե ՀՀ-ԱՊՀՄ-ն և ՀՀ-ՔԱԿ-ն գործել են սույն քաղաքականության պահանջներին և համապատասխան հայտարարության համաձայն ապա չի համարվում, որ նրանք գործել են անփութորեն:

3.3. Մեկնաբանություն և պարտավորություն

3.3.1. Կառավարում

Սույն Քաղաքականությամբ սահմանված դրույթները պետք է մեկնաբանվեն համաձայն <<Միջազգային ավտոճանապարհային փոխադրումներ կատարող տրանսպորտային միջոցների անձնակազմի աշխատանքի մասին>> Եվրոպական համաձայնագրի (AETR) և Հայաստանի Հանրապետության կողմից սահմանված թվային տախոգրաֆի համակարգի վերաբերյալ օրենսդրության պահանջներին:

3.4. Գաղտնիության պահպանում

Գաղտնիության պահպանումը սահմանափակված է <<Անձնական տվյալների մշակման և այդ տվյալների տեղաշարժի առնչությամբ անհատների պաշտպանության>> մասին 95/46/EC դիրեկտիվայով:

3.4.1. Գաղտնի տեղեկատվության տեսակներ

ՀՀ-ԱՊՀՄ-ի, ՀՀ-ՔԱԿ-ի, ենթակապալառուների կամ սպասարկող գործակալության կողմից պահվող ցանկացած անհատական կամ հավաքական տեղեկատվություն, որը արտացոլված չէ քարտերում կամ հավաստագրերում, համարվում է գաղտնի և չպետք է հրապարակվի առանց նախապես օգտագործողի համաձայնության, եթե օրենքով այլ բան նախատեսված չէ:

Սույն քաղաքականության շրջանակներում ՀՀ-ԱՊՀՄ, ՀՀ-ՔԱԿ-ի գործունեության ժամանակ կիրառվող և օգտագործվող բոլոր մասնավոր և գաղտնի բանալիները պետք

է պահվեն գաղտնի:

Աուդիտի գրանցման մատյանները և արձանագրություններն ընդհանուր առմամբ չպետք է հասանելի լինեն, եթե օրենքով այլ բան նախատեսված չէ:

3.4.2. Գաղտնի չհամարվող տեղեկատվության տեսակներ

Հավաստագրերը չեն համարվում գաղտնի:

Նույնականացման տեղեկատվությունը կամ այլ անհատական կամ հավաքական տեղեկատվությունը, որը արտացոլված է քարտերում կամ հավաստագրերում, չի համարվում գաղտնի, եթե նման պահանջ սահմանված չէ հատուկ համաձայնագրերով:

4. Հայտարարություն (այսուհետ՝ Հ)

ՀՀ-ԱՊՀՄ-ն և ՀՀ-ՔԱԿ-ը պետք է ունենան սույն քաղաքականությամբ սահմանված պահանջներին համապատասխան կիրառվող փորձի և ընթացակարգերի Հ-եր: ԱՊՄ-ն պետք է հաստատի ընթացակարգի Հ-րը:
Մասնավորապես՝

1) Հ-ն պետք է սահմանի ՀՀ-ԱՊՀՄ և ՀՀ-ՔԱԿ ծառայություններին աջակցող բոլոր արտաքին կազմակերպությունների պարտավորությունները՝ ներառյալ կիրառվող քաղաքականությունները և փորձը:
2) Հ-ն պետք է հասանելի լինի ԱՊՄ-ի, Տախոգրաֆ համակարգի օգտագործողների և վստահելի կողմերի համար (օր.՝ վերահսկող մարմիններ): Այնուամենայնիվ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ից հիմնականում չի պահանջվում իր փորձի հետ կապված բոլոր մանրամասները հանրորեն հասանելի դարձնել օգտագործողների համար:
3) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կառավարման պատասխանատվությունն է ապահովել Հ-րի պատշաճ կերպով իրականացումը:
4) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ն պետք է սահմանի Հ-րի համար վերանայման գործընթաց:
5) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ն պետք է սահմանված ժամկետներում ծանուցի այն փոփոխությունների մասին, որոնք նախատեսում է կատարել իր Հ-ում, և պետք է հաստատումից հետո անմիջապես հասանելի դարձնի վերանայված Հ-ը:

5. Սարքավորումների կառավարում

Սարքավորումը Տախոգրաֆ համակարգում սահմանված է որպես

- Տախոգրաֆ քարտեր
- Փոխադրամիջոցների միավորներ
- Արագության սենսորներ

Սարքավորումը գործածվում է և կառավարվում մի քանի նշանակությամբ.

- ՀՀ-ՔՏՄ (գրանցում, նորացում և այլն),

- ՀՀ-ԱՊՀՄ (հավաստագրեր, բանալիներ),
- ՀՀ-ՔԱԿ (տեսողական և էլեկտրոնային անհատականացում, տրամադրում, ապաակտիվացում),
- ՓՄ արտադրողներ և Արագության սենսորներ արտադրողներ:

ԱՊՄ-ի կողմից իրականացվում են հետևյալ գործառույթները.

- Որակի վերահսկում (տեսակի հաստատում),
- Հ-ի հաստատում:

ՀՀ-ՔՏՄ-ի կողմից իրականացվում են հետևյալ գործառույթները.

- Քարտերի ստացման համար դիմումների ընդունում,
- Դիմումների հաշվառում,
- Սարքավորման գրանցում և տվյալների պահպանում (Տվյալների բազա),
- Դիմորդի/Քարտատերի նույնականացում (ընդունում է դիմումներ, վավերացնում է ներկայացված տվյալները, ստուգում է դիմորդի ինքնությունը),
- Քարտատերերի տվյալների փոխանցում ՀՀ-ՔԱԿ-ին,
- Անհատականացված քարտի տրամադրում,
- PIN կոդերի փոխանցում արհեստանոցի քարտատերերին,
- Քարտերի <<սպիտակ>> և <<սև>> ցուցակների վարում,
- Քարտերի գրանցմանն և տրամադրմանն առնչվող տվյալների բազայի վարում:

ՀՀ-ՔԱԿ-ի կողմից իրականացվում են հետևյալ գործառույթները.

- Բանալու և հավաստագրի տեղադրում
- Քարտերի անհատականացում
- PIN կոդերի փոխանցումը ՀՀ-ՔՏՄ-ին
- Դիմորդների ստուգում տախոոնետ ցանցում
- Որակի վերահսկում

ՀՀ-ԱՊՀՄ-ի կողմից իրականացվում են հետևյալ գործառույթները.

- Անդամ-պետության մարմնի բանալիների արտադրություն և գրանցում,
- Քարտի հավաստագրերի թողարկում և գրանցում,
- Եվրոպական բանալիների արտադրության հավաստագրերի գրանցում,
- Անդամ-պետության բանալիների ներակայացում ԵԵՀՄ-ին՝ հավաստագրման համար,
- Քարտերի հավաստագրերի փոխանցում ՀՀ-ՔԱԿ-ին:

ՓՄ արտադրողների գործառույթները սույն քաղաքականության շրջանակներում ներառված չեն:
Արագության սենսորներ արտադրողների գործառույթները սույն քաղաքականության շրջանակներում ներառված չեն:

5.1. Տախոգրաֆ քարտեր

5.1.1. Որակի վերահսկում

ՀՀ-ԱՊՀՄ-ն և ՀՀ-ՔԱԿ-ը պետք է ապահովեն, որ Տախոգրաֆ համակարգում միայն Կանոնակարգի պահանջներին համապատասխան տեսակի հաստատում ունեցող քարտերը անհատականացվեն: Տես նաև 5.1.7.5:

5.1.2. Քարտի դիմում

ՀՀ-ՔՏՄ-ն պետք է տեղեկացնի օգտագործողին քարտի օգտագործման պայմանների մասին: Այս տեղեկատվությունը պետք է հասանլի լինի հայերեն լեզվով, ըստ անհրաժեշտության նաև անգլերեն լեզվով:

Օգտագործողը պետք է ընդունի պայմանները, քարտի դիմումը ներկայացնելուց և առաքված քարտը ստանալուց:

5.1.2.1. Օգտագործողի դիմում

Տախոգրաֆ քարտերի համար ներկայացված դիմումը պետք է համապատասխանի Հայաստանի Հանրապետության կառավարության 2011 թվականի մարտի 10-ի <<Հայաստանի Հանրապետությունում հսկիչ սարքերում (թվային տախոգրաֆներում) օգտագործվող քարտերի ձևը և դրանց տրամադրման կարգը հաստատելու մասին>> N 231-Ն որոշման պահանջներին: Դիմումն ընդգրկում է տվյալներ, որոնք ապահովելու են դիմորդի ճշգրիտ նույնականացումը, իսկ Կազմակերպության քարտի կամ Վերահսկողության քարտի դեպքում այն ապահովելու է համապատասխան կազմակերպությունների ճշգրիտ նույնականացումը:

5.1.2.2. Համաձայնություն

Դիմորդը, քարտի համար դիմելով և առաքված քարտը ստանալով, համաձայնության է գալիս ԱՊՄ-ի (կամ ՀՀ-ՔՏՄ-ի) հետ, որով սահմանվում է հետևյալը.

1. Օգտագործողը համաձայն է Տոխագրաֆ քարտի կիրառման և օգտագործման պայմանների հետ,
2. Օգտագործողը համաձայն է և հավաստում է քարտը ստանալու պահից և դրա օգտագործման ողջ ժամանակահատվածի համար, եթե ՀՀ-ՔՏՄ-ն չի ծանուցվում այլ օգտագործողի կողմից,
    1) օգտագործողի քարտը հասանելի չէ ոչ մի չլիազորված անձի համար,
    2) օգտագործողի կողմից ՀՀ-ՔՏՄ-ին տրված ամբողջ տեղեկատվությունը, որը արտացոլված է քարտում ճիշտ է,
    3) քարտը բարեխղճորեն օգտագործվում է՝ համաձայն քարտի օգտագործման սահմանափակումներին:

5.1.2.3. ՀՀ-ՔՏՄ-ի կողմից վարորդական քարտի տրամադրման պայմանները.

Վարորդական քարտը կարող է տրամադրվել միայն Հայաստանի Հանրաեթությունում մշտական բնակություն ունեցող անձանց:
ՀՀ-ՔՏՄ-ն ապահովելու է, որ դիմորդը չունենա այլ Անդամ-պետությունում տրամադրված վավեր վարորդական քարտ: Դիմորդի ստուգումը Տախոնետ ցանցում իրականացնում է ՀՀ-ՔԱԿ-ը, որը կարող է վավերացվել ՀՀ-ՔՏՄ-ի կողմից:
ՀՀ-ՔՏՄ-ն պետք է ապահովի, որ վարորդական քարտի դիմումատուն ունենա համապատասխան կարգի վավեր վարորդական իրավունքի վկայական:

5.1.3. ՀՀ-ՔՏՄ-ի կողմից քարտի նորացման իրականացում.

Արհեստանոցի քարտերը վավեր պետք է լինեն տրամադրման պահից առավելագույնը մեկ տարի ժամկետով (Համաձայն կանոնակարգ 12.1):

Վարորդի քարտերը վավեր պետք է լինեն տրամադրման պահից առավելագույնը հինգ տարի ժամկետով (Հանաձայն կանոնակարգ 14.4.a):

Կազմակերպության քարտերը վավեր պետք է լինեն տրամադրման պահից առավելագույնը հինգ տարի ժամկետով:

Վերահսկողության քարտերը վավեր պետք է լինեն տրամադրման պահից առավելագույնը երկու տարի ժամկետով:

ՀՀ-ՔՏՄ-ն պետք է ունենա միջոցառումներ համաձայն որի օգտագործողներին ծանուցի քարտի ժամկետի ավարտի մասին:

Քարտի ժամկետի երկարացման դիմումը ընդունվում է սույն քաղաքականության 5.1.2. բաժնի համաձայն:

5.1.3.1. Վարորդական քարտեր

Օգտագործողը պետք է դիմի քարտի նորացման համար դրա վավերականության ժամկետի ավարտից առնվազն 15 օր առաջ: (Համաձայն կանոնակարգի հոդված 15.1)

Եթե օգտագործողը քարտը օգտագործել է սույն պահանջներին համապատասխան, ՀՀ-ՔՏՄ-ն պետք է նախքան փոխարինման ենթակա քարտի վավերականության ավարտը տրամադրի նոր վարորդական քարտ: (Համաձայն կանոնակարգի հոդված 14.4.a)

5.1.3.2. Արհեստանոցի քարտեր

Օգտագործողը պետք է դիմի քարտի նորացման համար դրա վավերականության ժամկետի ավարտից առնվազն 15 օր առաջ:

ՀՀ-ՔՏՄ-ն պետք է նորացված քարտը տրամադրի դիմումը ստանալուց հետո 5-օրյա

ժամկետում: (Համաձայն կանոնակարգի հոդված 12.1)

5.1.3.3. Կազմակերպության քարտեր

Օգտագործողը պետք է դիմի քարտի նորացման համար դրա վավերականության ժամկետի ավարտից առնվազն 15 օր առաջ:

Եթե օգտագործողը քարտը օգտագործել է սույն պահանջներին համապատասխան, ՀՀ-ՔՏՄ-ն պետք է նախքան փոխարինման ենթակա քարտի վավերականության ավարտը տրամադրի նոր քարտ:

5.1.3.4. Վերահսկողության քարտեր

Օգտագործողը պետք է դիմի քարտի նորացման համար դրա վավերականության ժամկետի ավարտից առնվազն 15 օր առաջ:
ՀՀ-ՔՏՄ-ն պետք է նորացված քարտը տրամադրի դիմումը ստանալուց հետո 5-օրյա ժամկետում:

5.1.4. Քարտի նորացում կամ փոխանակում

Օգտագործողը, փոխելով իր բնակության երկիրը, կարող է պահանջել փոխանակել իր վարորդական քարտը:
Եթե քարտը վավեր է, դիմումը ընդունելու համար օգտագործողը կարող է ներկայացնել միայն բնակության վայրի փոփոխությունը հավաստող փաստաթուղթը:

ՀՀ-ՔՏՄ-ն պետք է նոր քարտի տրամադրման պահից իր պատականելության տակ վերցնի նախորդ քարտը և այն ուղարկի դրա ծագման ԱՊՄ: (Համաձայն Կանոնակարգի հոդված 14.4.c):

Մնացած դեպքերում բնակության երկիրը փոխելիս քարտի փոխանակումը պետք է իրականացվի նոր քարտի տրամադրման պահանջներին համապատասխան:

5.1.5. Կորցրած, գողացված, վնասված կամ թերի գործողության քարտեր.

Եթե քարտը կորել կամ գողացվել է, օգտագործողը պետք է դրա մասին հայտնի տեղի ոստիկանությանը և ստանա իր հայտարարության մասին տեղեկանք:
Գտնված քարտի դեպքում կարելի է հայտնել դրա օգտագործողին կամ ոստիկանությանը, որի մասին էլ ոստիկանությունը անհապաղ տեղեկացնում է ՀՀ-ՔՏՄ-ին:
Գողացված կամ կորցրած քարտերի մասին տեղեկատվությունը պետք է տեղադրվի <<սև ցուցակում>>, որը հասանելի է բոլոր անդամ-պետությունների համապատասխան մարմիններին:

Վնասված կամ թերի գործողության քարտերը պետք է ուղարկվեն տրամադրված ՀՀ-ՔՏՄ, որտեղ կենթարկվեն տեսողական և էլեկտրոնային չեղարկման և կանցկացվեն <<սև ցուցակ>>:

Եթե քարտը կորցրած է, վնասված կամ թերի գործողության, օգտագործողը պետք է 7 օրվա ընթացքում դիմի քարտի փոխարինման համար: (Համաձայն Կանոնակարգի հոդված 15.1):

Ընդունելով, որ օգտագործողը հետևել է վերոնշյալ պահանջներին՝ ՀՀ-ՔՏՄ-ն պետք է դիմումը ստանալուց հետո 5-օրյա ժամկետում տրամադրի փոխարինող քարտ նոր բանալիներով և հավաստագրով: (Համաձայն Կանոնակարգի հոդված 14.4.a):

Փոխարինող քարտը պետք է ունենա նույն վավերականության ժամկետն, ինչ՝ նախորդը: (Համաձայն Կանոնակարգի հավելված 1B: VII):
Եթե փոխարինվող քարտը ավելի պակաս վավերականության ժամկետ ունի, քան երկու ամիսը, ՀՀ-ՔՏՄ-ն կարող է փոխարենը տրամադրել նոր քարտ:

5.1.6. Դիմումի հաստատման համար գրանցումը իրականացվում է ՀՀ-ՔՏՄ-ի կողմից.

ՀՀ-ՔՏՄ-ն պետք է հաստատված դիմումները գրանցի տվյալների բազայում: Տվյալները հասանելի են դարձվում ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի համար, որն օգտագործում է տեղեկատվությունը հավաստագրի մշակման և քարտի անհատականացման համար: Տվյալների բազայի համակարգը կառավարվում է ՀՀ-ՔԱԿ-ի կողմից:

5.1.7. ՀՀ-ՔԱԿ-ի կողմից քարտի անհատականացում.

Քարտերն անհատականացվում են տեսողական և էլեկտրոնային եղանակներով: Որոշ դեպքերում այս գործընթացն իրականացվելու է սպասարկող գործակալների կողմից, որը չի նվազեցնում ԱՊՄ-ի ընդհանուր պատասխանատվությունը:

5.1.7.1. Տեսողական անհատականացում

Քարտերը տեսողական անհատականացման պետք է ենթարկվեն համաձայն Կանոնակարգի հավելված 1B-ի բաժին IV-ի.

5.1.7.2. Օգտագործողի տվյալների մուտքագրում

Համաձայն կանոնակարգի 1B հավելվածի 2-րդ լրացման TCS 403-ի, TCS 408-ի, TCS 413-ի և TCS 418-ի կանոնների պետք է օգտագործողի տվյալները մուտքագրվեն քարտ (կախված քարտի տեսակից):

5.1.7.3. Բանալու մուտք

Մասնավոր բանալին պետք է տեղադրվի քարտում առանց բանալիների արտադրման վայրը փոխելու: Բանալիների արտադրման վայրը պետք է ապահովի, որ որևիցե անձ ոչ մի դեպքում չկարողանա վերահսկել արտադրված մասնավոր բանալիները: Տես նաև բանալու կառավարումը, 7.2:

5.1.7.4. Հավաստագրի տեղադրում

Օգտագործողի հավաստագիրը պետք է տեղադրվի քարտում նախքան օգտագործողին քարտի տրամադրումը:

5.1.7.5. Որակի վերահսկում

Գոյություն ունեցող փաստաթղթային ընթացակարգերը պետք է ապահովեն, որ օգտագործողների քարտերի տեսողական տեղեկատվությունը և տրամադրված քարտերում և հավաստագրերում տեղադրված էլեկտրոնային տեղեկատվությունը համապատասխանեն միմյանց և համապատասխանաբար վավերացված լինեն օգտագործողի կողմից:

5.1.7.6. Չտրամադրված քարտերի չեղարկում (ոչնչացում)

Անհատականացման ժամանակ վնասված կամ ոչնչացված (կամ այլ պատճառներով ավարտին չհասցված կամ չտրամադրված) բոլոր քարտերը պետք է ֆիզիկական և էլեկտրոնային չեղարկման (ոչնչացման) ենթարկվեն:

Բոլոր ոչնչացված քարտերը պետք է գրանցվեն չեղարկման տվյալների բազայում:

5.1.8. Քարտի գրանցում և տվյալների պահպանում (տվյալների բազա)

ՀՀ-ՔԱԿ-ը պատասխանատվություն է կրում օգտագործողներին տրվող քարտերի և քարտերի համարների հետադարձ կապը ապահովելու համար: Տվյալները պետք է ՀՀ-ՔԱԿ-ից փոխանցվեն ՀՀ-ՔՏՄ գրանցման համար:

5.1.9. Քարտի հանձնում օգտագործողին

Քարտի տրամադրումն օգտագործողներին իրականացվում է ՀՀ-ՔՏՄ-ի կողմից: ՀՀ-ՔՏՄ-ի կողմից նման պահանջ ստանալու դեպքում անհատականացված քարտերը ՀՀ-ՔԱԿ-ի կողմից ուղարկվում են ՀՀ-ՔՏՄ-ին:
ՀՀ-ՔԱԿ-ում անհատականացման ժամկետը պետք է նախատեսվի՝ նվազագույնի հասցնելու համար ժամանակը, որը պահանջվում է անհատականացված քարտը չհրկիզվող պահարանում ապահով պահպանելու համար նախքան այն օգտագործողին տրամադրելը: Գիշերվա ընթացքում քարտերի պահպանումը պահանջում է անվտանգ պահպանում չհրկիզվող պահարանում: Փաստաթղթային ձևանմուշները պետք է

նախատեսված լինեն բացառիկ դեպքերի համար՝ ներառյալ արտադրման գործընթացում արձանագրված խախտումները, տրամադրման ձախողումը և քարտերի կորուստը կամ վնասվելը:
Անհատականացված քարտերը պետք է անմիջապես տեղափոխվեն այնտեղ, որտեղից դրանք տրամադրվելու են օգտագործողներին:
Անհատականացված քարտերը միշտ պետք է առանձին պահվեն չանհատականացված քարտերից:
Տախոգրաֆ քարտերը պետք է տրամադրվեն այնպես, որ նվազագույնի հասցվի կորստի ռիսկը:
Օգտագործողին քարտը հանձնելիս պետք է ստուգել օգտագործողի ինքնությունը:
Օգտագործողը պետք է ինքնությունը հաստատող վավեր ապացույց ներկայացնի:
Քարտի ստացումը պետք է հաստատվի օգտագործողի ստորագրությամբ:

5.1.10. Վավերականացման կոդերի (PIN) ձևավորում ՀՀ-ՔԱԿ-ի կողմից

Արհեստանոցի քարտերը պետք է ունենան PIN կոդ, որն օգտագործվում է քարտը ՓՄ-ի հետ վավերականությունը ստուգելու համար: (Համաձայն Կանոնակարգի հավելված 1B, Հայտ 10: Տախոգրաֆ քարտեր: 4.2.2):

PIN կոդերը պետք է լինեն առնվազն 4 նիշից: (Համաձայն Կանոնակարգի հավելված 1B, Հայտ 10: Տախոգրաֆ քարտեր:4.1.2):

5.1.10.1. PIN ձևավորում

PIN կոդերը պետք է ձևավորվեն անվտանգ համակարգում և անվտանգ տեղադրվեն արհեստանոցի քարտում և ուղղակիորեն տպվեն PIN ծրարներում: PIN կոդերը չպետք է պահպանվեն այնպես համակարգչային համակարգում, որ հնարավոր լինի ապահովել կապը PIN-ի և օգտագործողի միջև: PIN-ի ձևավորման համակարգը պետք է բավարարի ITSEC E3, CC EAL4 պահանջներին կամ դրան համարժեք այլ անվտանգության չափանիշների:

5.1.10.2. PIN -ի բաշխում

PIN կոդերը կարող են տրամադրվել փոստային ծառայությունների միջոցով:
PIN կոդերի տրամադրումը չպետք է իրականացվի համապատասխան քարտերի հետ մեկտեղ:

5.1.11. Քարտի ապաակտիվացում

Պետք է մշտապես հնարավոր լինի քարտը և դրանց բանալիները ապաակտիվացնել: Ապաակտիվացման որոշումը պետք է կայացվի ԱՊՄ-ի կամ ՀՀ-ՔՏՄ-ի կողմից, իսկ դրա գործընթացը պետք է իրականացվի ՀՀ-ՔԱԿ-ի կողմից:

Ապաակտիվացումը պետք է տեղի ունենա գործողությանը համապատասխան սարքավորումներով, որի ժամանակ կիրականացվի քարտի գործառույթների և բանալիների ոչնչացումը: Քարտը նաև պետք է տեսողականորեն չեղարկվի:
Քարտի ապաակտիվացումը պետք է գրանցվի քարտերի տվյալների բազայում, և քարտի համարը պետք է անցկացվի <<սև ցուցակ>>:

5.2. Փոխադրամիջոցների միավորներ և Արագության սենսորներ

Ներկայումս կիրառելի չէ Հայաստանի Հանրապետության համար՝ բացառությամբ ՓՄ-ի վնասված կամ ոչ սարքին լինելու դեպքերը: Արհեստանոցը պետք է վերցնի տվյալները ՓՄ-ից և տրամադրի փոխադրող կազմակերպությանը: Եթե դա հնարավոր չէ անել, արհեստանոցի կողմից պետք է տրվի հայտարարություն փոխադրող կազմակերպությանը:

6. Երթուղային և տրանսպորտային բանալիների կառավարում. Եվրոպական երթուղային բանալիներ, Անդամ-պետության բանալիներ, Արագության սենսորների բանալիներ, Տրանսպորտային բանալիներ

Այս բաժինը պարունակում է կառավարման դրույթներ՝

- Եվրոպական երթուղային բանալի. ԵԵՀՄ հանրային բանալի,
- Անդամ-պետության բանալիների, այսինքն՝ Անդամ-պետության ստորագրման բանալու զույգ(եր)ի
- Արագության սենսորների բանալիների,
- Տրանսպորտային բանալիների (ԵԵՀՄ-ի և ՀՀ-ԱՊՀՄ-ի միջև) կառավարման համար:

ԵԵՀՄ հանրային բանալին օգտագործվում է Անդամ-պետության հավաստագրերի ստուգման համար: ԵԵՀՄ-ի գաղտնի բանալուն առընչվող դրույթները սույն քաղաքականությունում չի քննարկվում, քանի որ այն երբեք չի լքում ԵԵՀՄ-ն:
Անդամ-պետության բանալիներն անդամ-պետության ստորագրման բանալիներն են, որոնք կարող են նաև կոչվել Անդամ-պետության երթուղային բանալիներ:
Արագության սենսորների բանալիները համաչափ բանալիներն են, որոնք պետք է տեղադրվեն արհեստանոցի քարտում, ՓՄ-ում և Արագության սենսորներում՝ դրանց փոխադարձ ճանաչման համար: ՀՀ-ԱՊՀՄ-ն ստանում է Արագության սենսորների բանալիները ԵԵՀՄ-ից, դասավորում և տրամադրում է դրանք արտադրողներին:
Տրանսպորտի բանալիները համաչափ բանալիներն են, որոնք գործածվում են ԵԵՀՄ-ի և ՀՀ-ԱՊՀՄ-ի միջև տեղեկատվության ապահով փոխանակման համար:
Եթե ՀՀ-ԱՊՀՄ-ն այլ կրիպտոգրաֆիկ բանալիների կարիք ունենա, դրանք չպետք է համարվեն Տախոգրաֆ համակարգի մաս, և դրանց հետ կապված հարցերը չեն կարող կարգավորվել սույն քաղաքականությամբ:

6.1. ԵԵՀՄ հանրային բանալիներ

ՀՀ-ԱՊՀՄ-ն այնպես պետք է պահի ԵԵՀՄ հանրային բանալին (ԵՄՍ.ՀԲ - EUR.PK), որ ապահովվի դրա ամբողջականությունը ու մատչելիությունը ցանկացած ժամանակ: Եթե ԵՄՍ.ՀԲ-ն սույն կանոններին համապատասխան պահվում է ՀՀ-ՔԱԿ-ում:
ՀՀ-ՔԱԿ-ը պետք է ապահովի, որ ԵՄՍ.ՀԲ-ը մուտքագրվի բոլոր տախոգրաֆ քարտեր և ՓՄ-ներ:

6.2. Անդամ-պետության բանալիներ

Անդամ-պետության բանալիները ՀՀ-ԱՊՀՄ ստորագրման բանալու զույգ(եր)ն են, որոնք գործածվում են բոլոր սարքավորումների հավաստագրերը ստորագրելիս:
Բանալու զույգը բաղկացած է հանրային բանալուց (ԱՊ.ՀԲ - MS.PK) և մասնավոր կամ գաղտնի բանալուց (ԱՊ.ԳԲ):
ՀՀ-ԱՊՀՄ հանրային բանալին հավաստագրված է ԵԵՀՄ-ի կողմից, բայց միշտ արտադրվում է հենց ՀՀ-ԱՊՀՄ-ի կողմից:

Անդամ-պետության բանալիները չպետք է կիրառվեն որևէ այլ նպատակի համար, բացի Տախոգրաֆ սարքավորումների ստորագրումը և ԵԵՀՄ-ի բանալու հավաստագրման պահանջը՝ ԲՀՊ-ն, ինչպես նկարագրված է հավելված A-ում [ԵԵՀՄ քաղաքականություն]:

6.2.1. Անդամ-պետության բանալիների արտադրություն

Անդամ-պետության բանալու զույգի արտադրությունը պետք է իրականացվի սարքի միջոցով, որը պետք է

- համապատասխանի FIPS 140-2 (կամ 140-1) 3-րդ մակարդակի պահանջներին կամ ավելի բարձր [FIPS-ից], կամ
- համապատասխանի CEN 14167-2 [CEN] աշխատանքային համաձայնագրի պահանջներին, կամ
- վստահելի համակարգ է, որը հաստատված է EAL 4-ի կողմից կամ ավելի բարձր մակարդակով՝ ISO 15408-ին [CC], E3-ին կամ ITSEC-ի ավելի բարձր մակարդակին համապատասխան, կամ էլ սրանց համազոր այլ անվտանգության չափանիշներին համաձայն: Սա պետք է լինի անվտանգության նպատակը կամ պաշտպանության պրոֆիլը, որը կհամապատասխանի սույն փաստաթղթի պահանջներին՝ հիմնված ռիսկի վերլուծության վրա, և հաշվի առնելով անվտանգության ֆիզիկական և այլ ոչ տեխնիկական միջոցները:

Բանալու արտադրման սարքը պետք է լինի առանձին, ինքնուրույն:

Կիրառվող գործիքը և պահանջներին համապատասխանությունը պետք է հաստատվեն ՀՀ-ԱՊՀՄ-ի ՈՒ-ով:
ՀՀ-ԱՊՀՄ բանալու զույգի արտադրության համար անհրաժեշտ է երեք տարբեր անհատների մասնակցությունը: Նրանցից առնվազն մեկը պետք է ունենա ՀՄԱ/ԱԱ-ի (հավաստագրման մարմին/անհատականացնող ադմինիստրատոր)

պարտավորությունը, մյուսները կարող են ունենալ այլ պարտավորություններ (տես 9.3.1. բաժինը՝ պարտականությունների նկարագրության համար):

Բանալիները պետք է արտադրվեն RSA ալգորիթմի օգտագործմամբ n=1024 բիտ բանալու երկարության մոդուլով: (Համաձայն Կանոնակարգի հավելված 1B, հայտ 11:2.1/3.2):

ՀՀ-ԱՊՀՄ-ն շարունակականությունը ապահովելու համ ստորագրման հավաստագրերի հետ միասին պետք է ունենա Անդամ-պետության բանալու մեկից ավելի զույգ, քանի որ ԵԵՀՄ-ն չի կարող անմիջապես տրամադրել Անդամ-պետության հավաստագրի փոխարինող:

6.2.2. Անդամ-պետության բանալիների վավերականության ժամկետ

Անդամ-պետության մասնավոր բանալին չպետք է համապատասխան հանրային բանալու հավաստագրումից սկսած 2 տարուց ավել լինի վավեր և չպետք է որևէ նպատակով կիրառվի իր վավերականության ժամկետի սպառումից հետո:

Համապատասխան հանրային բանալին պետք է վավերականության ժամկետի ավարտ չունենա:

6.2.3. Անդամ-պետության մասնավոր բանալիների պահպանում

Խարդախություններից և միջամտություններից խուսափելու նպատակով մասնավոր բանալիները պետք է օգտագործվեն հատուկ կայուն սարքում, որը

- համապատասխանում է FIPS 140-2 (կամ 140-1) 3-րդ մակարդակի պահանջներին կամ ավելի բարձր [FIPS-ից], կամ
- վստահելի համակարգ է, որը հաստատված է EAL 4-ի կողմից կամ ավելի բարձր մակարդակով՝ ISO 15408-ին [CC], E3-ին կամ ITSEC-ի ավելի բարձր մակարդակին համապատասխան, կամ էլ սրանց համազոր այլ անվտանգության չափանիշներին համաձայն: Սա պետք է լինի անվտանգության նպատակը կամ պաշտպանության պրոֆիլը, որը կհամապատասխանի սույն փաստաթղթի պահանջներին՝ հիմնված ռիսկի վերլուծության վրա, և հաշվի առնելով անվտանգության ֆիզիկական և այլ ոչ տեխնիկական միջոցները:

ՀՀ-ԱՊՀՄ մասնավոր ստորագրման բանալիների հասանելիության համար անհրաժեշտ է կրկնակի վերահսկում: Սա նշանակում է, որ ոչ ոք չպետք է ունենա այն միջոցները, որոնք պահանջվում են մասնավոր բանալու պահպանման վայր մուտք գործելու համար: Սա չի նշանակում, որ սարքավորումների հավաստագրերի ստորագրությունը պետք է իրականացվի կրկնակի վերահսկման ներքո:

6.2.4. Անդամ-պետության մասնավոր բանալիների պահոց

Անդամ-պետության մասնավոր ստորագրման բանալիների պահեստավորումը պետք է

իրականացվի առնվազն կրկնակի վերահսկում պահանջող բանալու վերականգնման ընթացակարգի միջոցով: Կիրառվող ընթացակարգը պետք է սահմանվի ՀՀ-ԱՊՀՄ Հ-ում:

6.2.5. Անդամ-պետության մասնավոր բանալիների կրկնօրինակները

Անդամ-պետության մասնավոր ստորագրման բանալիներն կրկնօրինակման ենթակա չեն:

6.2.6. Անդամ-պետության բանալիների վտանգվածությունը

Պետք է լինեն հրահանգներ, որոնք ներառված կլինեն ՀՀ-ԱՊՀՄ Հ-ում և կսահմանեն այն միջոցները, որոնք պետք է ձեռնարկվեն օգտագործողների և ՀՀ-ԱՊՀՄ-ում անվտանգության համար պատասխանատու անձանց կամ Ծառայություն մատուցող գործակալությունների կողմից, եթե Անդամ-պետության մասնավոր բանալիները ցուցադրվել են, կամ որևէ այլ կերպ կարող են համարվել վտանգված կամ առկա են նման կասկածելի հանգամանքներ:

Նման դեպքում ՀՀ-ԱՊՀՄ-ն պետք է նվազագույնը տեղեկացնի ԱՊՄ-ին, ԵԵՀՄ-ին և բոլոր մյուս իրավասու մարմիններին:

6.2.7. Անդամ-պետության բանալիների ժամկետի ավարտը

ՀՀ-ԱՊՀՄ-ն պետք է ունենա ընթացակարգ, որը կապահովի, որ այն միշտ ունենա վավեր, հավաստագրված Անդամ-պետության ստորագրման բանալու զույգ:

Անդամ-պետության ստորագրման բանալու զույգի ժամկետի ավարտի հետ միասին հանրային բանալին պետք է արխիվացվի, իսկ մասնավոր բանալին պետք է

- ոչնչացվի այնպես, որ մասնավոր բանալին այլևս հնարավոր չլինի վերականգնել, կամ
- պահպանվի այնպես, որ անհնար լինի այն նորից օգտագործելը:

6.3. Արագության սենսորների բանալիներ

ՀՀ-ԱՊՀՄ-ն պետք է անհրաժեշտության դեպքում պահանջի ԵԵՀՄ-ից Արագության սենսորների Km, KmVU և KmWC բանալիներ (Կանոնակարգի Հավելված 1B, հայտ 11:3.1.3):

ՀՀ-ԱՊՀՄ-ն պետք է արհեստանոցի բանալին (Km_{WC}) ուղարկի ՀՀ-ՔԱԿ-ին՝ արհեստանոցի քարտերում տեղադրելու համար:

ՀՀ-ՔԱԿ-ը պետք է հանձն առնի ՀՀ-ԱՊՀՄ-ի կողմից տրված առաջադրանքը, ըստ որի հարկավոր է ապահովել, որ KmWC արհեստանոցի բանալին տեղադրվի բոլոր արհեստանոցի քարտերում (Կանոնակարգի Հավելված 1B, հայտ 11:3.1.3):

ՀՀ-ԱՊՀՄ-ն և/կամ ՀՀ-ՔԱԿ-ը պետք է պահպանման, գործածման և տրամադրման ընթացքում պաշտպանեն արագության սենսորների բանալիները բարձր մակարդակի ֆիզիկական և տրամաբանական անվտանգության վերահսկման միջոցով: Բանալիները պետք է պահվեն և օգտագործվեն հատուկ խարդախության և միջամտությունների դեմ կայուն սարքում, որը

- համապատասխանում է FIPS 140-2 (կամ 140-1) 3-րդ մակարդակի պահանջներին կամ ավելի բարձր [FIPS-ից], կամ
- վստահելի համակարգ է, որը հաստատված է EAL 4-ի կողմից կամ ավելի բարձր մակարդակով՝ ISO 15408-ին [CC], E3-ին կամ ITSEC-ի ավելի բարձր մակարդակին համապատասխան, կամ էլ սրանց համազոր այլ անվտանգության չափանիշներին համաձայն: Սա պետք է լինի անվտանգության նպատակը կամ պաշտպանության պրոֆիլը, որը կհամապատասխանի սույն փաստաթղթի պահանջներին՝ հիմնված ռիսկի վերլուծության վրա, և հաշվի առնելով անվտանգության ֆիզիկական և այլ ոչ տեխնիկական միջոցները:

6.4. Տրանսպորտային բանալիներ

Տվյալների անվտանգ փոխանակման համար ԵԵՀՄ-ն տրամադրում է համաչափ տրանսպորտային բանալիներ: ՀՀ-ԱՊՀՄ-ն պետք է պահպանման, օգտագործման և տրամադրման ընթացքում պաշտպանեն արագության սենսորների բանալիները բարձր մակարդակի ֆիզիկական և տրամաբանական անվտանգության վերահսկման միջոցով: Բանալիները պետք է պահվեն և օգտագործվեն հատուկ խարդախության և միջամտությունների դեմ կայուն սարքում, որը

- համապատասխանում է FIPS 140-2 (կամ 140-1) 3-րդ մակարդակի պահանջներին կամ ավելի բարձր [FIPS-ից], կամ
- վստահելի համակարգ է, որը հաստատված է EAL 4-ի կողմից կամ ավելի բարձր մակարդակով՝ ISO 15408-ին [CC], E3-ին կամ ITSEC-ի ավելի բարձր մակարդակին համապատասխան, կամ էլ սրանց համազոր այլ անվտանգության չափանիշներին համաձայն: Սա պետք է լինի անվտանգության նպատակը կամ պաշտպանության պրոֆիլը, որը կհամապատասխանի սույն փաստաթղթի պահանջներին՝ հիմնված ռիսկի վերլուծության վրա, և հաշվի առնելով անվտանգության ֆիզիկական և այլ ոչ տեխնիկական միջոցները:

Բոլոր բանալիների փոխանցումները ՀՀ-ԱՊՀՄ-ի և ԵԵՀՄ-ի միջև պետք է իրականացվեն փոխանակման և արձանագրային միջոցով, որոնք սահմանված են ԵԵՀՄ երթուղու քաղաքականությամբ: Եթե բանալիները փոխանցվում են ֆիզիկական միջոցով, ապա ԱՊՄ-ի կողմից փոխանցումն իրականացնելու համար նշանակվում է լիազոր անձ:

ՀՀ-ԱՊՀՄ-ի բանալու հավաստագրման հայտի համար գործածելի է KCR արձանագրությունը, որը ներկայացված է ԵԵՀՄ երթուղու քաղաքականությունում, Հավելված A-ում:

ՀՀ-ԱՊՀՄ-ն պետք է ընդունի ԵԵՀՄ հանրային բանալին տրամադրման ձևաչափով որը նկարագրված է ԵԵՀՄ երթուղու քաղաքականությունում, Հավելված B-ում:

ՀՀ-ԱՊՀՄ-ն պետք է ապահովի, որ KID-ը և բանալիների մոդուլները, որոնք ներկայացվում են ԵԵՀՄ-ի հավաստագրմանը և արագության սենսորների բանալու տրամադրմանը, միակն են ՀՀ-ԱՊՀՄ-ի տիրույթում:
ՀՀ-ԱՊՀՄ-ն պետք է արագության սենսորների բանալի պահանջի ԵԵՀՄ-ից՝ օգտագործելով KDR արձանագրությունը, որը նկարագրված է ԵԵՀՄ երթուղու քաղաքականությունում, Հավելված D-ում:

7. Սարքավորումների բանալիներ (անհամաչափ)

Սարքավորումների բանալիներն անհամաչափ բանալիներ են, որոնք թողարկվում են տրամադրման/արտադրման գործընթացի ժամանակ և հավաստագրվում են ՀՀ-ԱՊՀՄ-ի կողմից Տախոգրաֆ համակարգի սարքավորման համար.

- Տախոգրաֆ քարտեր
- Փոխադրամիջոցների միավորներ (Հայաստանի համար կիրառելի չէ):

Սույն քաղաքականությունը չի ներառում համաչափ Արագության սենսորների բանալիները:

7.1. ՀՀ-ՔԱԿ/ՀՀ-ԱՊՀՄ ընդհանուր ասպեկտներ՝ ներառյալ Ծառայություն մատուցող գործակալություններ և ՓՄ արտադրողներ

Սարքավորման (Քարտի) կարգաբերումը, բանալու բեռնումը և անհատականացումը պետք է իրականացվեն ֆիզիկապես անվտանգ և վերահսկվող միջավայրում: Մուտքն այս վայր պետք է լինի խստորեն կանոնակարգված, որի դեպքում պահանջվում է առնվազն երկու հոգու ներկայություն համակարգը գործարկելու համար: Պետք է իրականացվի մուտքերի և համակարգում իրականացված գործողությունների գրանցամատյանի վարում:

Բանալու արտադրման համակարգում չպետք է լինի տեղեկատվության արտահոսք խախտելով քաղաքականության պահանջները:

Տախոգրաֆ քարտեր. Քարտի անհատականացման համակարգում չպետք է լինի տեղեկատվության արտահոսք խախտելով քաղաքականության պահանջները:

Կազմակերպությունները (Ենթակապալառուներ, Ծառայություն մատուցող գործակալություններ), որոնք իրականացնում են բանալու արտադրությունը և քարտերի անհատականացումը մեկից ավել Անդամ-պետությունների համար, պետք է իրականացնեն նշված գործառույթները յուրաքանչյուրի համար առանձին-առանձին: Յուրաքանչյուր անհատական գործընթացի համար պետք է վարվի գրանցամատյան, որը պետք է հասանելի լինի համապատասխան ԱՊՄ-ին:

Համակարգի անհատականացման գրանցամատյանը պետք է պարունակի պատվերի հղում և սարքավորումների համապատասխան համարների ցուցակը և հավաստագրերը: Նման պահանջներ ներկայացնելու դեպքում ԱՊՄ-ի կողմից

գրանցամատյանները պետք է լինեն հասանելի:

7.2.Սարքավորումների բանալիների արտադրություն

Բանալիները կարող են արտադրվել կամ սարքավորումներ արտադրողի, կամ էլ ՀՀ-ՔԱԿ-ի կամ ՀՀ-ԱՊՀՄ-ի կողմից: (Հավելված 1B, հավելում 11:3.1.1)

Մարմինը, որն իրականացնում է բանալիների արտադրությունը, պետք է ապահովի, որ բանալիների արտադրությունն ընթանա անվտանգ և սարքավորումների մասնավոր բանալին մնա գաղտնի:

Բանալիների արտադրությունը պետք է իրականացվի հատուկ խարդախության և միջամտությունների դեմ կայուն սարքում կամ

- համապատասխանի FIPS 140-2 (կամ 140-1) 3-րդ մակարդակի պահանջներին կամ ավելի բարձր [FIPS-ից], կամ
- համապատասխանի CEN 14167-2 [CEN] աշխատանքային համաձայնագրի պահանջներին, կամ
- վստահելի համակարգ է, որը հաստատված է EAL 4-ի կողմից կամ ավելի բարձր մակարդակով՝ ISO 15408-ին [CC], E3-ին կամ ITSEC-ի ավելի բարձր մակարդակին համապատասխան, կամ էլ սրանց համազոր այլ անվտանգության չափանիշներին համաձայն: Սա պետք է լինի անվտանգության նպատակը կամ պաշտպանության պրոֆիլը, որը կհամապատասխանի սույն փաստաթղթի պահանջներին՝ հիմնված ռիսկի վերլուծության վրա, և հաշվի առնելով անվտանգության ֆիզիկական և այլ ոչ տեխնիկական միջոցները:

Բանալիները պետք է արտադրվեն RSA ալգորիթմի օգտագործմամբ n=1024 բիտ բանալու երկարության մոդուլով (Կանոնակարգի Հավելված 1B, հայտ 11:2.1/3.2):

Մասնավոր բանալու արտադրման և պահպանման ընթացակարգերը պետք է թույլ չտան, որ այն լինի հասանելի համակարգից դուրս: Սարք մուտքագրվելուց հետո այն պետք է անմիջապես ջնջվի համակարգից:
Բանալին արտադրող մարմնի պատասխանատվությունն է նախաձեռնել համապատասխան միջոցներ ապահովելու համար, որ հանրային բանալին նախքան հավաստագրումը իր տիրույթում լինի միակը:

7.2.1.1. Խմբաքանակով բանալիների արտադրություն

Կրիպտոգրաֆիկ բանալիների արտադրությունը կարող է իրականացվել նախքան հավաստագրման հայտը խմբաքանակով արտադրությունն իրականացնելու միջոցով կամ հավաստագրման հայտի հետ ուղղակի կերպով:

Խմբաքանակով արտադրությունը պետք է իրականացվի առանձին, ինքնուրույն սարքավորումներում, որոնք համապատասխանում են վերոնշյալ անվտանգության

պահանջներին: Բանալու ամբողջականությունը պետք է պաշտպանված լինի նախքան հավաստագրի տրամադրումը:

7.2.2.Սարքավորումների բանալիների վավերականություն

*7.2.2.1.*Բանալիներ քարտերի վրա

Սույն քաղաքականության ներքո տրամադրված հավաստագրերին առնչվող սարքավորումների մասնավոր բանալու գործածումը երբեք չպետք է գերազանցի հավաստագրի վավերականության ժամկետը:

*7.2.2.2.*Փոխադրամիջոցների միավորներ

Ներկայումս կիրառելի չէ Հայաստանի Հանրապետության համար:

7.2.3.Սարքավորումների մասնավոր բանալիների պաշտպանություն և պահպանում-քարտեր

ՀՀ-ՔԱԿԸ-ը պետք է ապահովի, որ քարտի մասնավոր բանալին լինի պաշտպանված և սահմանափակված այն քարտով, որը տրամադրվել է օգտագործողին սույն քաղաքականությամբ հաստատված ընթացակարգերին համաձայն:

Մասնավոր բանալիների կրկնօրինակները տախոգրաֆ քարտից բացի չպետք է պահվեն որևէ այլ տեղում, եթե դա չի պահանջում բանալիների արտադրությունը և անհատականացման սարքը:

Ոչ մի դեպքում քարտի մասնավոր բանալին չպետք է պահվի քարտից դուրս:_

7.2.4.Սարքավորումների մասնավոր բանալիների պաշտպանության և պահպանում-ՓՄ-ներ

Ներկայումս կիրառելի չէ Հայաստանի Հանրապետության համար:

7.2.5.Սարքավորումների մասնավոր բանալիների պահպանում և արխիվացում

Սարքավորումների մասնավոր բանալիները ենթակա չեն պահպանման և արխիվացման:

7.2.6.Սարքավորումների հանրային բանալիների արխիվացում

Բոլոր հանրային բանալիները հավաստագրումը պետք է արխիվացվի ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔՏՄ-ի հավաստագրմամբ:

7.2.7.Սարքավորումների բանալիների հասանելիության ժամկետ

Տախոգրաֆ քարտի օգտագործումը դադարելուց հետո հանրային բանալին պետք է արխիվացվի, իսկ մասնավոր բանալին պետք է՝

- ոչնչացվի այնպես, որ մասնավոր բանալին հնարավոր չլինի վերականգնել, կամ
- պահպանվի այնպես, որ այն հնարավոր չլինի նորից կիրառության մեջ դնել:

8.Սարքավորումների հավաստագրերի կառավարում

Սույն բաժինը նկարագրում է հավաստագրերի գործողության ժամանակահատվածը՝ ներառյալ գրանցման գործառույթը, հավաստագրման տրամադրումը, բաշխումը, օգտագործումը, նորացումը, չեղարկումը (եթե կիրառելի է) և հասանելիությունը:

8.1.Տվյալների մուտքագրում

8.1.1. Տախոգրաֆ քարտեր

Եթե քարտատերերը հայտ չեն ներկայացնում հավաստագրերի համար, նրանց հավաստագրերը տրվում են ըստ տախոգրաֆ քարտի համար լրացված հայտի տեղեկատվության (բաժին 5.1.2) և ՀՀ-ՔՏՄ գրանցման գրասենյակից ստացված տվյալների հիման վրա: Հավաստագրվելիք հանրային բանալին դուրս է բերվում բանալիների արտադրման գործընթացից:

ՀՀ-ՔԱԿ-ը պետք է ապահովի, որ մուտքագրված տվյալները պարունակեն տեղեկատվություն, որը ներկայացված է Հավաստագրի միակ քաղվածքում (ՀՔ): ՀՀ-ԱՊՀՄ-ն պետք է վավերացնի ՀՔ-ի եզակիությունն իր տիրույթում:

8.1.2.Փոխադրամիջոցների միավորներ

Ներկայումս կիրառելի չէ Հայաստանի Հանրապետության համար:

8.2.Տախոգրաֆ քարտերի հավաստագրեր

8.2.1.Վարորդական հավաստագրեր

Վարորդական հավաստագիր տրվում է միայն այն ընտրված հայտատուներին, որոնք դիմել են վարորդի քարտ ստանալու համար:

8.2.2.Արհեստանոցի հավաստագրեր

Արհեստանոցի հավաստագիր տրվում է միայն այն ընտրված հայտատուներին, որոնք դիմել են արհեստանոցի քարտ ստանալու համար:

8.2.3. Վերահսկողության հավաստագրեր

Վերահսկողություն իրականացնող մարմնի հավաստագիր տրվում է միայն այն ընտրված հայտատուներին, որոնք դիմել են վերահսկողության քարտ ստանալու համար:

8.2.4. Կազմակերպության հավաստագրեր

Կազմակերպության հավաստագիր տրվում է միայն այն ընտրված հայտատուներին, որոնք դիմել են կազմակերպության քարտ ստանալու համար:

8.3.Փոխադրամիջոցների միավորների հավաստագրեր

Ներկայումս կիրառելի չէ Հայաստանի Հանրապետության համար:

8.4.Սարքավորումների վավերականության ժամկետ

Հավաստագրերը չպետք է ավելի երկար վավեր լինեն, քան համապատասխան սարքավորումը (բաժին 5):

- Արհեստանոցի հավաստագրերը չպետք է վավեր լինեն 1 տարուց ավել (Կանոնակարգ 12.1):
- Վերահսկողություն իրականացնող մարմնի հավաստագրերը չպետք է վավեր լինեն 2 տարուց ավել:
- Կազմակերպության հավաստագրերը չպետք է վավեր լինեն 5 տարուց ավել:
- Վարորդական հավաստագրերը չպետք է վավեր լինեն 5 տարուց ավել (Կանոնակարգ 14.4.a):

8.5.Սարքավորումների հավաստագրերի տրամադրում

ՀՀ-ԱՊՀՄ-ն պետք է ապահովի իր տրամադրած հավաստագրերի վավերականության և ամբողջականության պահպանումը: Հավաստագրի բովանդակությունը սահմանվում է համաձայն կանոնակարգի Հավելված 1B-ի հավելում 11-ով:

8.6.Սարքավորումների հավաստագրերի նորացում և թարմացում

Տես Սարաքավորումների կառավարումը (բաժին 5): Քանի որ հավաստագրերը և քարտերն ունեն միևնույն վավերականության ժամկետը, ապա դրանց առնչվող հարցերը քննարկվում են միասին:

8.7.Սարաքավորումների հավաստագրերի և տեղեկատվության տարածում

ՀՀ-ԱՊՀՄ-ն պետք է հավաստագրերին առնչվող բոլոր տվյալները տրամադրի ՀՀ-ՔՏՄ-

ին, որպեսզի կապ ապահովվի հավաստագրերի, սարքավորումների և օգտագործողների միջև:

ՀՀ-ՔՏՄ-ն պետք է ապահովի, որ հավաստագրերը ըստ անհրաժեշտության հասանելի լինեն օգտագործողների և համապատասխան կողմերի համար:

ՀՀ-ՔՏՄ-ն պետք է ապահովի, որ ՀՀ-ԱՊՀՄ Հ-րի բոլոր պայմանները և դրույթները, ինչպես նաև համապատասխան տեղեկատվությունը միշտ պատրաստ և հասանելի լինեն բոլոր օգտագործողների, համապատասխան կողմերի և այլ առնչվող խմբերի համար:

8.8.Սարքավորումների հավաստագրերի օգտագործում

Թվային տախոգրաֆի հավաստագրերի կիրառումը պետք է իրականացվի միայն Տախոգրաֆ համակարգի շրջանակներում:

8.9.Սարքավորումների հավաստագրերի չեղարկում

Հավաստագրերը չեն չեղարկվում, անվավեր Տախոգրաֆ սարքավորումներն անցկացվում են <<սև ցուցակ>>, որը կարող է ստուգվել ճանապարհային վերահսկողության ժամանակ:

9.ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի տեղեկատվության անվտանգության կառավարում

Սույն բաժնում նկարագրված են Տեղեկատվության անվտանգության պահպանման միջոցները, որոնք պարտադրվում են սույն քաղաքականությամբ:

9.1.ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի տեղեկատվության անվտանգության կառավարում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ապահովի, որ կիրառվեն կազմակերպչական և կառավարման ընթացակարգեր, որոնք համապատասխանում են ընդունված չափանիշներին:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է պատասխանատվություն կրի բանալիների հավաստագրման ծառայությունների իրականացման բոլոր գործառույթների համար, նույնիսկ եթե որոշ գործառույթներ վերապահված են ենթակապալառուների: Երրորդ կողմերի պատասխանատվությունները պետք է հստակորեն սահմանվեն ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կողմից և անհրաժեշտ է համապատասխան միջոցներ ձեռնարկվեն, որ երրորդ կողմերն իրականացնեն ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կողմից պահանջվող բոլոր գործառույթները:
ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է պատասխանատվություն կրի բոլոր կողմերի

համապատասխան փորձի ցուցաբերման համար:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի շրջանակներում անվտանգության կառավարման համար անհրաժեշտ Տեղեկատվության անվտանգության ապահովման ենթակառուցվածքը պետք է պահպանվի մշտապես: Առկա անվտանգության մակարդակի վրա ազդեցություն ունեցող ցանկացած փոփոխություն պետք է նախ հաստատվի ԱՊՄ-ի կողմից:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ընդունի անվտանգության կառավարման համակարգ, որը հավասարազոր կլինի ISO 17799-ին [ISO 17799]: Պաշտոնական հավաստագրումն պարտադիր չէ:

9.2.Գույքի դասակարգում և ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ կառավարում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ապահովի իր գույքի և տեղեկատվության պաշտպանման համապատասխան մակարդակը: Մասնավորապես

1) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է անցկացնի ռիսկի գնահատում՝ բիզնեսի ռիսկի գնահատման և անհրաժեշտ անվտանգության պահանջներն ու գործարկման ընթացակարգերը որոշելու նպատակով:
2) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է իրականացնի գույքի ցուցակագրում և ռիսկի վերլուծության առկայությամբ գույքին ներկայացվող պաշտպանության պահանջների դասակարգում:

9.3.ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ անձնակազմի անվտանգության վերահսկում

9.3.1.Վստահված կողմերի պարտավորություններ

Աջակցելով սույն իրավասու մարմնի քաղաքականությանը՝ պարտավորությունների բաժանման տարբեր մեխանիզմները կարող են ընդունելի լինեն այն պայմանով, որ կողմնակի ազդեցությունը այնքան մեծ է որքան առաջարկվող մոդելների դեպքում և պայմանով, որ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի Հ-ում նկարագրված գործողությունների պայմանները:
Մեկ անձի միայնակ գործունեության դեպքում անվտանգությունը շրջանցելուց խուսափելու նպատակով ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի համակարգերում պատասխանատվությունները պետք է բաշխվեն մի քանի պարտավորություններով և անհատների միջև: Համակարգերում յուրաքանչյուրի համար տրվող թույլտվությունները պետք է ունենան սահմանափակ հնարավորություններ՝ թույլտվությունը կրողի պարտավորությանը համապատասխան:

Առաջարկվող պարտավորություններն են.

1) Հավաստագրման մարմնի ադմինիստրատոր կամ Անհատականացնող ադմինիստրատոր (ՀՄԱ/ԱԱ),
2) Համակարգի ադմինիստրատոր (ՀԱ)

3) Տեղեկատվության համակարգի անվտանգության աշխատակից (ՏՀԱԱ)

ՀՄԱ/ԱԱ-ի պարտավորությունը ներառում է.

1) բանալու արտադրությունը,
2) հավաստագրի մշակումը, (ստորագրված հավաստագրի հայտերի մշակումը պետք է իրականացվի ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի սարքավորումների կողմից՝ համաձայն նշված կանոնների)
3) սարքավորումների անհատականացումը և անվնաս առաքումը,
4) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի տվյալների բազայի պահպանմանը և վտանգի բացահայտմանը ցուցաբերվող աջակցությանն առնչվող կազմակերպչական գործառույթներ:

ՀԱ պարտավորությունը ներառում է.

1) համակարգի նախնական ձևի իրականացումը՝ ներառյալ համակարգի անվնաս գործարկումը և անջատումը,
2) բոլոր նոր թույլտվությունների նախնական ստեղծում,
3) ցանցի նախնական ձևի ստեղծում,
4) արտակարգ իրավիճակների դեպքում համակարգի վերագործարկման կոշտ սկավառակի ստեղծում, որը թույլ կտա վերականգնել համակարգի աղետալի կորուստը,
5) համակարգի պահուստի, ծրագրային ապահովման վերազինման և վերականգնման իրականացում՝ ներառյալ պահուստի անվտանգ պահպանումը և առաքումն այլ վայր: Պահուստը պետք է իրականացվի առնվազն շաբաթը մեկ, և համակարգը պետք է միացվի/անջատվի պահուստի իրականացումից հետո, որպեսզի իրականացվեն կոշտ սկավառակների ինտեգրման ստուգումներ,
6) Ընդունողի անվան և/կամ ցանցի հասցեի փոփոխությունը:

ՏՀԱԱ-ի պարտավորությունը ներառում է.

1) Անվտանգության արտոնությունների և ՀՄԱ/ԱԱ-ների մուտքի վերահսկման տրամադրումը,
2) Բոլոր նոր թույլտվությունների համար գաղտնաբառերի տրամադրումը,
3) Պահանջվող համակարգի արձանագրությունների արխիվացումը,
4) Աուդիտի գրանցամատյանի վերանայումը՝ ՀՄԱ/ԱԱ-ի համապատասխանությունը համակարգի անվտանգության քաղաքականությանը ի հայտ բերելու նպատակով: Աուդիտի գրանցամատյանի վերանայումը պետք է իրականացվի առնվազն շաբաթը մեկ:
5) Անցկացնել և հսկել ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-երի արձանագրությունների տարեկան ցուցակագրում,
6) Անդամ-պետության բանալիների արտադրմանը մասնակցությունը:

9.3.2. Պարտավորությունների բաշխում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի դեպքում տարբեր անհատներ պետք է ստանձնեն վերոնշյալ երեք

պարտավորություններից յուրաքանչյուրը, և պետք է յուրաքանչյուր հանձնարարության համար նշանակվի առնվազն մեկ անհատ:

9.3.3.Նույնականացում և վավերացում յուրաքանչյուր պարտավորության համար

ՀՄԱ/ԱԱ-ի, ՀԱ-ի և ՏՀԱԱ-ի նույնականացումը և վավերականացումը պետք է լինեն սույն քաղաքականությունում սահմանված ընթացակարգերին և պայմաններին համապատասխան:

9.3.4. Տեղեկատվություն, որակավորում, փորձի և պահանջների ձևակերպում

ՀՄԱ/ԱԱ-ն (Հավաստագրման մարմին/Անհատականացնող ադմինիստրատոր), որը ներառում է հավաստագրերի և բանալիների վերաբերյալ տեղեկատվության ստեղծումը և կառավարումը: ՀՄԱ/ԱԱ պարտավորությունը ստանձնող անհատը պետք է ունենա անառարկելի հավատարմություն, վստահելիություն, լինի համակարգին ինտեգրված և պետք է ցուցաբերի անվտանգության առումով աչալրջություն և իր ամենօրյա գործողությունների բանիմացություն:

Պատասխանատու պաշտոններ զբաղեցնող ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ ամբողջ անձնակազմը՝ ներառյալ առնվազն բոլոր ՀՄԱ/ԱԱ և ՏՀԱԱ (Տեղեկատվական համակարգի անվտանգության աշխատակից) պաշտոնները, պետք է

1) հանձն չառնեն այլ պարտականություններ, որոնք կարող են հակասություններ առաջացնել իրենց պարտականությունների և պատասխանատվությունների հետ որպես ՀՄԱ/ԱԱ և ՏՀԱԱ,
2) նախկինում ազատված չլինեն հանձնարարության կատարումից պարտականությունները չկատարելու կամ դրանք անփութորեն կատարելու պատճառով,
3) ստացած լինեն համապատասխան վերապատրաստում իրենց պարտականությունների կատարման համար:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ կազմակերպությունները նաև կարող են նշել հատուկ պահանջներ, ինչպիսիք են քաղաքացիության, որակավորման և հանցավոր անցյալի բացակայության պահանջները: Այսպիսի պահանջները պետք է սահմանվեն կիրառելի Հ-ում:

9.3.5. Վերապատրաստմանն ուղղված պահանջներ

Անձնակազմը պետք է համապատասխան վերապատրաստում անցնի պարտավորության և աշխատանքի համար:

9.4.ՀՄ համակարգի և անհատականացման համակարգերի անվտանգության վերահսկում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ապահովի, որ անվտանգության համակարգը աշխատի ճշգրիտ, ձախողման նվազագույն ռիսկով: Մասնավորապես՝

1) Համակարգերի և տեղեկատվության ամբողջականությունը պետք է պաշտպանված լինի վիրուսներից, անբարենպաստ և չլիազորված ծրագրային մուտքերից,
2) Միջադեպերի ու անսարքությունների պատճառած վնասները պետք է միջադեպերի արագ արձագանքման և հաշվետվությունների միջոցով հասցնել նվազագույնի:

Հավաստագրման մարմնի համակարգը (ՀՄՀ) և անհատականացման համակարգը պետք է տրամադրեն համակարգի անվտանգության անհրաժեշտ վերահսկում՝ սույն քաղաքականությունում կամ համապատասխան Հ-ում նկարագրված պարտավորությունների բաշխման պարտադրման համար:
Անվտանգության վերահսկումը պետք է անհատական մակարդակով տրամադրի մուտքի վերահսկում՝ ՀՀ-ԱՊՀՄ-ի մասնավոր տրամադրման բանալիների բոլոր փոխանցումների և գործառույթների համար:

9.4.1.Հատուկ համակարգչային անվտանգության տեխնիկական պահանջներ

ՀՀ-ԱՊՀՄ-ի անձնական հավաստագրման բանալիները գործարկող համակարգի ստուգաչափման համար պահանջվում են առնվազն երկու օպերատորներ:

9.4.2.Համակարգչային անվտանգության աստիճան

ՔԱԿ-ի և անհատականացման համակարգերի համար չի պահանջվում պաշտոնական գնահատում, քանի դեռ դրանք բավարարում են սույն բաժնի պահանջներին:

9.4.3.Համակարգի զարգացման վերահսկում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է օգտագործեն հուսալի համակարգեր և արտադրանք, որոնք պաշտպանված են նորացումից:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կողմից ստանձնած ցանկացած համակարգերի զարգացման նախագծի մշակման և պահանջների հստակեցման փուլում պետք է իրականացվի անվտանգությանը ներկայացվող պահանջների վերլուծություն՝ ապահովելու համար, որ անվտանգությունը բավարարի IT համակարգերին:

Փոփոխությունների վերահսկման ընթացակարգեր պետք է ապահովեն ցանկացած գործարկային ծրագրային ապահովման թողարկման, թարմացումների և արտակարգ իրավիճակներում ծրագրային ապահովումն ուղղելու համար:

9.4.4. Անվտանգության կառավարման վերահսկում

Համակարգի պարտավորությունները (բաժին 9.3.1) պետք է իրականացվեն և պարտադրվեն:

9.4.5.Ցանցի անվտանգության վերահսկում

Վերահսկում (օրինակ՝ firewalls) պետք է իրականացնել ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի ներքին ցանցային տիրույթներն արտաքին տիրույթներից պաշտպանելու համար, որոնք հասանելի են երրորդ կողմերից:

Հրապարակման ոչ ենթակա տվյալները ոչ անվտանգ ցանցերով փոխանացվելիս պետք է լինեն պաշտպանված:

9.5.Անվտանգության աուդիտի ընթացակարգեր

Սույն բաժնում անվտանգության աուդիտի ընթացակարգերը վավեր են բոլոր համակարգչային և համակարգի բաղադրիչների համար, որոնք ազդում են սույն քաղաքականության ներքո բանալիների, հավաստագրերի և սարքավորումների տրամադրման գործընթացի վրա:

9.5.1.Արձանագրված միջոցառումների տեսակներ

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ համակարգչին/համակարգին առնչվող անվտանգության աուդիտի գործառույթները աուդիտի նպատակով պետք է հաշվառվեն գրանցամատյանում

1) Թույլտվությունների ստեղծումը (արտոնյալ կամ ոչ),
2) Փոխանցման հայտն այն ներկայացնող թույլտվության արձանագրությունների, արձանագրությունների տեսակի հետ միասին՝ ներառելով նշումը, թե արդյոք փոխանցումն ավարտված է, և անավարտ փոխանցման պատճառը,
3) Նոր ծրագրային ապահովման տեղադրումը կամ ծրագրային ապահովման թարմացումները,
4) Բոլոր պահուստներին վերաբերող ժամանակը և ժամկետը և այլ նկարագրական տեղեկատվություն,
5) Համակարգի անջատումները և վերագործարկումը,
6) Բոլոր կոշտ սկավառակների թարմացումների ժամանակը և ժամկետը,
7) Աուդիտի գրանցամատյանի բեռնաթափումների ժամանակը և ժամկետը,
8) Փոխանցումների արխիվի բեռնաթափումների ժամանակը և ժամկետը:

9.5.2.Աուդիտի գրանցամատյանի վերլուծության հաճախականություն

Գրանցամատյանը պետք է մշակման և վնասակար գործունեության կանխման նպատակով վերլուծության ենթարկվի կանոնավոր հաճախականությամբ: Գրանցումների մատյանի ընթացակարգերը պետք է նկարագրվեն Հ-ում:

9.5.3.Աուդիտի գրանցամատյանի պահման ժամանակաշրջան

Աուդիտի գրանցամատյանը պետք է պահվի նվազագույնը 7 տարի:

9.5.4.Աուդիտի գրանցամատյանի պահպանում

Ինտեգրված գրանցամատյանները պետք է լինեն պատշաճ ամբողջականությամբ պաշտպանված: Բոլոր գրանցումների ժամանակը պետք է համապատասխանաբար ֆիքսվի:
Աուդիտի գրանցամատյանը պետք է ստուգվի և հաստատվի առնվազն ամիսը մեկ: Նվազագույնը երկու անձ՝ ՀԱ և ՏՀԱԱ պարտավորություն ունեցող (տես բաժին 9.3.1), պետք է ներկա լինեն ստուգմանը և հաստատմանը:

9.5.5.Աուդիտի գրանցամատյանի պահպանման ընթացակարգեր

Հաստատված գրանցամատյանի երկու օրինակ պետք է պատրաստվեն և պահվեն տարբեր, ֆիզիկապես անվտանգ վայրերում:

Աուդիտի գրանցամատյանը պետք է պահվի այնպես, որ հնարավոր լինի ուսումնասիրել այն դրա պահպանման ընթացքում:

Աուդիտի գրանցումների մատյանը պետք է պաշտպանված լինի չլիազորված մուտքերից:

9.5.6.Աուդիտի հավաքագրման համակարգ

Պահանջվում է աուդիտի հավաքագրման միայն ներքին համակարգ:

9.6.Արձանագրում

9.6.1.ՀՀ-ՔՏՄ-ի կողմից արձանագրված միջոցառումների տեսակներ

Արձանագրությունները պետք է ներառեն ՀՀ-ՔՏՄ-ի տրամադրության տակ գտնվող բոլոր առնչվող փաստաթղթերը, բայց չսահմանափակվեն

1) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի, օգտագործողների և տեղեկատուի միջև փոխանակված հավաստագրման հայտերով (բոլոր առնչվող հաղորդագրություններով),
2) Օգտագործողների հավաստագրումների և քարտերի տրամադրման հայտերի գրանցման ստորագրված համաձայնություններով՝ ներառյալ հայտը ստանալու համար պատասխանատու անձի ինքնությունը,
3) Քարտերի տրամադրման ընդունման ստորագրությամբ,
4) Հավաստագրերին և ասոցացված քարտերին առնչվող պայմանագրային համաձայնություններով,
5) Հավաստագրերի նորացմամբ և օգտագործողի հետ ունեցած բոլոր հաղորդագրություններով,
6) Չեղարկման հայտերով և հայտի հեղինակի և/կամ օգտագործողի միջև փոխանակված բոլոր արձանագրված հաղորդագրություններով,
7) Ընթացիկ և նախկինում իրականացված քաղաքականության փաստաթղթերով:

9.6.2.ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կողմից արձանագրված միջոցառումների տեսակներ

Արձանագրությունները պետք է ներառեն ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի տրամադրության տակ գտնվող բոլոր առնչվող փաստաթղթերը, բայց չսահմանափակվեն

1) Տրամադրվող հավաստագրերի բովանդակությամբ,
2) Աուդիտի օրագրերով՝ ներառյալ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի Հ-ին համապատասխանության տարեկան աուդիտի արձանագրությունները,
3) Ընթացիկ և նախկինում իրականացված հավաստագրերի քաղաքականության փաստաթղթերով և դրանց առնչությամբ Հ-երին:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կամ Ծառայություն մատուցող գործակալության անձնակազմի (ՀՄԱ/ԱԱ) կողմից ներկայացված բոլոր թվային ստորագրությամբ հայտերի արձանագրությունները պետք է ներառեն յուրաքանչյուր հայտի համար պատասխանատու ադմինիստրատորի ինքնությունը, ինպես նաև հայտի ստուգման ոչ մերժելի ամբողջ տեղեկատվությունը արձանագրության պահպանման ընթացքում:

9.6.3. Արխիվի պահպանման ժամանակաշրջան

Արխիվները պետք է պահպանվեն և պաշտպանված լինեն թարմացումից կամ ոչնչացումից Հ-ով նշված ժամանակահատվածով:

9.6.4.Արխիվային տեղեկատվության ձեռքբերման և հաստատման ընթացակարգեր

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է գործունեություն իրականացնի բաժին 3.4-ում սահմանված գաղտնիության պահպանման վերաբերյալ պահանջներին համապատասխան:

Ըստ պահանջի անհատական փոխանցումների արձանագրությունները կարող են հրապարակվել փոխանցման մեջ ներգրավված մարմիններից ցանկացածի կամ դրանց ճանաչված ներկայացուցիչների կողմից:

Բաժին 11.5-ի համաձայն՝ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ըստ պահանջի հասանելի դարձնի ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի՝ կիրառելի Հ-ին համապատասխանության վերաբերյալ մշակված փաստաթղթերը:

Կախված օրենսդրությունից՝ արձանագրությունների վերականգնման համար կարող է ողջամիտ վճար գանձվել:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ապահովի արխիվի հասանելիությունը, և որ արխիվացված տեղեկատվությունն իր պահպանման ընթացքում պահվի ընթեռնելի ձևաչափով, նույնիսկ եթե ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի գործունեությունն ընդհատվի, արգելվի կամ կասեցվի:

Եթե ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի ծառայությունները պետք է ընդհատվեն, արգելվեն կամ կասեցվեն, ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ն պետք է ծանուցի բոլոր գործակալություններին՝

արխիվի շարունակական հասանելիությունն ապահովելու նպատակով: Արխիվացված տեղեկատվություն մոտքի համար բոլոր հայտերը պետք է ուղարկվեն ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ նախքան դրա ծառայության կասեցումը:

9.7.ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ հաջորդականության պլանավորում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ունենա հաջորդականության բիզնես պլան (ՀԲՊ): Այն պետք է ներառի (բայց չսահմանափակվի) այնպիսի միջոցառումներ, ինչպիսք են

- Բանալիների վտանգված լինելը,
- Տվյալների աղետալի կորուստը, օրինակ՝ գողություն, հրդեհ, կոշտ սկավառակի կամ ծրագրային ապահովման խափանում,
- Այլ տիպերի համակարգի խափանումները:

9.7.1.Անդամ-պետությունների բանալիների ֆիզիկական հասանելիություն

Անդամ-պետության բանալիների վտանգված լինելու հետ կապված հարցերը ներկայացված են բաժին 6-ում:

9.7.2.Վերականգնում այլ աղետների դեպքում

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը և ենթակապալառուները պետք է ունենան ձևանմուշներ համակարգի հետ կապված աղետների ազդեցությունների կանխարգելման և նվազեցման նպատակով: Այս ձևանմուշները ներառում են պահուստի տվյալների ապահով և հեռակառավարելի պահպանումը, տվյալների վերականգնման գործող ընթացակարգեր և այլն, որոնք պետք է մանրամասն ներկայացվեն ՀԲՊ-ում:

9.8.ՀՄ-ի և անհատականացման համակարգերի ֆիզիկական անվտանգության վերահսկում

Ֆիզիկական անվտանգության վերահսկումը պետք է իրականացվի ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔԱԿ-ի կոշտ սկավառակ կամ ծրագրային ապահովում մուտքը վերահսկելու նպատակով: Սա ներառում է ՀՄ-ի և անհատականացման կոշտ սկավառակի և ցանկացած այլ կրիպտոգրաֆիկ կոշտ սկավառակի մոդելի կամ քարտի աշխատանքային կայանները և այլ մասերը: Պետք է պահվի սույն տեղանքի (տեղանքների) բոլոր ֆիզիկական մուտքագրումների գրանցամատյան:
Անդամ-պետության հավաստագրերի ստորագրման բանալիները պետք է ֆիզիկապես և ողջմատորեն պաշտպանված լինեն, ինչպես նկարագրված է Հ-ում:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է տարածման կոշտ սկավառակի պահպանման համար նախատեսի այնպիսի պահոցի վայր, որ կանխարգելվի պահվող տեղեկատվության կորուստը, կեղծումը կամ ոչ լիազորված գործածումը: Պահոցը պետք է պահվի այնպես,

որ հնարավոր լինի և տվյալների վերականգնման և կարևոր տեղեկատվության արխիվացումը: Պահոցի կոշտ սկավառակը նույնպես պետք է ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի համակարգի տեղակայումից տարբեր վայրում պահվի, ինչը թույլ կտա վերականգնումը հիմնական հաստատությանը պատահած բնական աղետի դեպքում:

ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի կենտրոնական սարքավորման հաստատության շինության անվտանգության ստուգում պետք է իրականացվի առնվազն յուրաքանչյուր 24 ժամը մեկ: Եթե այդ հաստատությունում կա մշտական այց, ապա կարելի է իրականացնել տեսողական ստուգում հերթափոխի ընթացքում մեկ անգամ՝ համոզվելու, որ չօգտագործվող համակարգերը և ցանկացած ասոցացված կրիպտոգրաֆիկ սարքերը/քարտերը ապահով կերպով պահված են, որ ֆիզիկական անվտանգության համակարգերը (օր.՝ դռան փականները և ադանշանները) գործում են ըստ պատշաճի, և որ չեն եղել բռնի մուտքի կամ ոչ լիազորված անձանց մուտքի փորձեր:

9.8.1.Ֆիզիկական հասանելիություն

Անդամ-պետության բանալիների և դրանց գործածման միջոցների գտնվելու ֆիզիկական տարածք մուտքի համար պետք է պահանջվի առնվազն երկու անձանց միաժամանակյա ներկայությունը, որոնց անհատապես տրվել է տարածք մուտք գործելու իրավունքը:

Այլ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ հաստատություններ սահմանափակ մուտքը պետք է թույլատրելի լինի միայն այն անձնակազմի համար, որին վերապահված է բաժին 9.3.1-ում նկարագրված պարտականություններից մեկը: Մուտքը կարող է վերահսկվել համակարգի գտնվելու սենյակ մուտքի վերահսկման համակարգի օգնությամբ: Եթե մուտքի վերահսկման համակարգը հնարավոր չէ հատուկ վայրի համար, ընդունելի կարող է լինել ապահովելը, որ ՀՄ և անհատականացմանն առնչվող նյութերը փակի տակ լինեն ապահով սենյակում կամ պահման տարածքում, երբ այն չի օգտագործվում:

10.ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔԱԿ-ի դադարեցում

10.1.Վերջնական դադարեցում – ԱՊՄ-ի պատասխանատվություն

ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔԱԿ-ի վերջնական կասեցում է համարվում այն իրավիճակը, երբ լոգիկ հիմնարկի հետ կապված բոլոր ծառայությունները մշտապես կասեցվում են: Հաշվի չի առնվում այն դեպքը, երբ ծառայությունը փոխանցվում է մի կազմակերպությունից մյուսին, կամ երբ ՀՀ-ԱՊՀՄ ծառայությունն անցնում է հին Անդամ-պետության բանալու զույգից նոր Անդամ-պետության բանալու զույգի կամ ԵԵՀՄ բանալու:

ԱՊՄ-ն պետք է ապահովի ներքոհիշյալ հանձնարարությունների կատարումը:

Նախքան ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը կասեցնի իր ծառայությունները, հարկավոր է ավարտել

հետևյալ նվազագույն ընթացակարգերը.

1) Տեղեկացնել բոլոր օգտագործողներին և կողմերին, որոնց հետ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պայմանավորվածություններ կամ հաստատված հարաբերությունների այլ ձևեր ունի,
2) Իր կասեցման մասին տեղեկատվությունը հրապարակայնորեն հասանելի դարձնել կասեցումից առնվազն 3 ամիս առաջ,
3) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է կասեցնի ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը ենթակապալառուների հավաստագրեր տրամադրելու բոլոր լիազորությունները,
4) ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է նախաձեռնի արձանագրությունների արխիվներ շարունակական մուտքի պահպանումն ու ապահովումը՝ դրանք ԵԵՀՄ-ին հանձնելով:

10.2.ՀՀ-ԱՊՀՄ կամ ՀՀ-ՔԱԿ պատասխանատվության փոխանցում

ՀՀ-ԱՊՀՄ-ի կամ ՀՀ-ՔԱԿ-ի պատասխանատվության փոխանցումը իրականացվում է, երբ ԱՊՄ-ն որոշում է նշանակել նոր ՀՀ-ԱՊՀՄ կամ ՀՀ-ՔԱԿ նախորդող մարմնի փոխարեն:

ԱՊՄ-ն պետք է ապահովի պատասխանատվությունների և ակտիվների կանոնավոր փոխանցման իրականացումը:

Հին ՀՀ-ԱՊՀՄ-ն պետք է փոխանցի բոլոր երթուղային բանալիները նոր ՀՀ-ԱՊՀՄ-ին այնպես, ինչպես կորոշի ԱՊՄ-ն:

Հին ՀՀ-ԱՊՀՄ-ն պետք է ոչնչացնի չփոխանցված բանալիների ցանկացած պատճե:

11.Աուդիտ

ԱՊՄ-ն պատասխանատվություն է կրում ՀՀ-ԱՊՀՄ-ի և ՀՀ-ՔԱԿ-ի աուդիտի իրականացումն ապահովելու համար:

11.1.Մարմնի համապատասխանության աուդիտի հաճախականություն

Սույն իրավասու մարմնի քաղաքականության շրջանակներում գործող ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ը պետք է ենթարկվի առնվազն ամենամյա քաղաքականությանը համապատասխանության աուդիտի:

11.2.Աուդիտի ներկայացվող հարցեր

Աուդիտ պետք է իրականացվի ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի փորձի համար:
Աուդիտ պետք է իրականացվի սույն իրավասու մարմնի քաղաքականությանը ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ-ի համապատասխանության համար:

Աուդիտ պետք է իրականացվի նաև Ծառայություններ մատուցող գործակալությունների գործունեության համար:

Աուդիտի արդյունքում պետք է պատրաստվի աուդիտի հաշվետվություն, որում նշված են ուղղիչ գործողությունները՝ դրանց իրականացման ժամանակացույցի հետ միասին, որոնք անհրաժեշտ են սույն քաղաքականության պահանջների կատարման համար:

11.3. Աուդիտ անցկացնող

ԱՊՄ-ն կարող է խորհրդակցել արտաքին հավաստագրման կամ հավատարմագրման կազմերպության հետ ՀՀ-ԱՊՀՄ/ՀՀ-ՔԱԿ Հ-ի հաստատման համար՝ իրականացման հարցում վստահվող կողմերի լիարժեք վստահությունն ապահովելու նպատակով: Այլապես ԱՊՄ-ն պետք է ստանձնի աուդիտի անցկացումը:

11.4. Թերությունների դեպքում նախաձեռնվող գործողություններ

Եթե աուդիտի արդյունքում անկանոնություններ հանդես գան, ԱՊՄ-ն պետք է խիստ գործողություններ իրականացնի:

11.5. Արդյունքների վերաբերյալ հայտարարություն

Ըստ պահանջի պետք է հասանելի լինեն անվտանգության կարգավիճակի մակարդակի մասին աուդիտի արդյունքները: Աուդիտի հաշվետվությունները չպետք է հասանելի լինեն՝ բացառությամբ տեղեկացված լինելու անհրաժեշտության դեպքից: Անգլերեն լեզվով հաշվետվությունն ուղարկվելու է ԵԵՀՄ: Հայտնաբերված թերությունների դեպքում այն պետք է պարունակի անհրաժեշտ փոփոխությունների ժամանակացույց:

12. Իրավասու մարմնի քաղաքականության փոփոխման ընթացակարգեր

12.1. Առանց ծանուցման փոփոխման ենթակա առարկաները

Միակ փոփոխությունները, որոնք կարող են կատարվել առանց ծանուցման, հետևյալն են.

1) Խմբագրական կամ տպագրական ուղղումներ,
2) Կոնտակտային տվյալների փոփոխություններ:

12.2.Ծանուցման ենթակա փոփոխություններ

12.2.1.Ծանուցում

Սույն հավաստագրման քաղաքականությունում ցանկացած կետ կարող է փոխվել 90 օր առաջ ծանուցման պայմանով:

Այն կետերի փոփոխությունները, որոնք ըստ քաղաքականության համար պատասխանատու կազմակերպության (ԱՊՄ-ն) նյութապես չի ազդելու սույն քաղաքականությունից օգտվողների և վստահվող կողմերի էական մեծամասնության վրա, կարող են փոփոխության ենթարկվել 30 օր առաջ ծանուցման պայմանով:

12.2.2. Մեկնաբանություններին տրվող ժամանակաշրջան

Ազդեցություն կրող օգտագործողները կարող են քաղաքականության կառավարման կազմակերպություն հղել իրենց մեկնաբանությունները ծանուցումից հետո 15 օրվա ընթացքում:

12.2.3.Տեղեկացում

Սույն քաղաքականությունում փոփոխությունների վերաբերյալ տեղեկատվությունը պետք է ուղարկվի

- Եվրոպական հանձնաժողովին,
- ԵԵՀՄ-ին,
- ՀՀ-ԱՊՀՄ-ին և ՀՀ-ՔԱԿ-ին՝ ներառյալ Ծառայություններ մատուցող գործակալությունները,
- Բոլոր մյուս ԱՊՄ-ներին:

12.2.4.Վերջնական փոփոխման ծանուցման համար տրվող ժամանակահատված

Եթե առաջարկվող փոփոխությունը լրամշակվում է մեկնաբանությունների արդյունքում, հարկավոր է ծանուցել լրամշակված առաջարկվող փոփոխության ուժի մեջ մտնելուց առնվազն 30 օր առաջ:

12.3. Իրավասու մարմնի նոր քաղաքականության հաստատմանը ենթակա փոփոխություններ

Եթե ԱՊՄ կազմակերպությունը մտադիր է քաղաքականության փոփոխություն կատարել, որը նյութական ազդեցություն կարող է ունենալ քաղաքականությունն օգտագործողների նշանակալի մեծամասնության վրա, ԱՊՄ-ն պետք է վերանայված ՀՀ-Մ քաղաքականությունը ներկայացնի Հանձնաժողովի հաստատմանը:

13.Հղումներ

[ԼՓՁ] Թվային տախոգրաֆ քարտերի տրամադրման լավագույն փորձի ձեռնարկ: Քարտերի տրամադրման խումբ, 2001թ. նոյեմբերի 16 (կառուցվող), պատկանում է Հանձնաժողովին:

[ԸՉ] Ընդհանուր չափանիշներ: ISO/IEC 15408 (1999): <<Տեղեկատվական տեխնոլոգիաներ – Անվտանգության տեխնիկաներ – Գնահատման չափանիշներ SS անվտանգության համար (մաս 1-ից 3)>>:

[CEN] CEN Աշխատանքային համաձայնագիր 14167-2: CSP ստորագրման գործողությունների համար կրիպտոգրաֆիկ մոդել – Պաշտպանության անձնագիր (ՍԳԿՄ-ՊԱ)

[ETSI 102 042]
ETSI TS 102 042. Քաղաքականության պահանջներ հավաստագրող մարմիններին, որոնք հանրային բանալիների հավաստագրեր են տրամադրում

[FIPS]
FIPS PUB 140-2 (2001թ. մայիսի 25): <<Կրիպտոգրաֆիկ մոդելներին ներկայացվող անվտանգության պահանջները>>: Տեղեկատվական տեխնոլոգիաների լաբորատորիա, Չափանիշների և տեխնոլոգիաների ազգային ինստիտուտ (ՉՏԱԻ)

[ISO 17799] BS ISO/IEC 17799: 2000. Տեղեկատվական տեխնոլոգիաներ – Տեղեկատվության անվտանգության կառավարման փորձի կանոնակարգ:

[ԱԸՈւ]
Անվտանգության ընդհանուր ուղեցույց, Քարտի տրամադրման նախագիծ: (կառուցվող), պատկանում է Հանձնաժողովին

[ԵԵՀՄ քաղաքականություն]
Թվային տախոգրաֆ համակարգի եվրոպական երթուղու քաղաքականություն, տարբերակ2.1:

14.Տերմիններ/սահմանումներ և հապավումներ

14.1.Տերմիններ/սահմանումներ

ՀՄ քաղաքականություն: Կանոնների անվանային խմբավորում, որը ցույց է տալիս բանալիների, հավաստագրերի և սարքավորումների կիրառելիության հատկանշումը հասարակությունում և/կամ ընդհանուր անվտանգության պահանջներով կիրառման դասը:

Քարտ/Տախոգրաֆ քարտեր: Ինտեգրված կաբելային սարքավորմամբ քարտ, սույն քաղաքականությունում սա համարժեք է <<ԻԿ-Քարտ>> և <<Խելացի քարտ>> տերմիններին:

Քարտատեր: Անձ կամ կազմակերպություն, ով ունի և օգտագործում է Տախոգրաֆ

քարտ: Ներառված են վարորդները, կազմակերպության ներկայացուցիչները, արհեստանոցի աշխատողները և վերահսկողություն իրականացնող մարմնի անձնակազմը:

Հավաստագիր: Ընդհանուր համատեքստում հավաստագիրը հաղորդագրությունների կառուցվածք է, որը ներառում է տրամադրողի կողմից պարտավորեցնող ստորագրությունը՝ հավաստող, որ հավաստագրում ներկայացված տեղեկատվությունը ճշգրիտ է, և որ հավաստագրվող հանրային բանալին կրողը կարող է ապացուցել ասոցացված մասնավոր բանալու պատկանելիությունը:

Հավաստագրող մարմնի համակարգ (ՀՄՀ): Համակարգչային համակարգ, որով հավաստագրերը տրամադրվում են ՀՄ մասնավոր ստորագրման բանալիով հավաստագրի տվյալների ստորագրմամբ (օգտագործող):

Հավաստագրման փորձի մասին վկայող Հայտարարություն (ՀՀ-ՀՀ): Փորձի ուղեցույց, որը հավաստագրող մարմինն օգտագործում է հավաստագրեր տրամադրելիս, և որն ուղղակիորեն կապված է սույն քաղաքականության հետ: ՀՀ-ՔՏՄ-ն սույն իրավասու մարմնի քաղաքականությունում փոխարինված է Փորձի մասին վկայող հայտարարությունով, քանի որ այն ունի առավել մեծ փորձ և կապ բանալիների, հավաստագրերի և սարքավորումների հետ:

Սարքավորումներ: Տախոգրաֆ համակարգում գոյություն ունեն հետևյալ սարքավորումները. Տախոգրաֆ քարտեր, ՓՄ (փոխադրամիջոցների միավորներ) և Արագության սենսորներ:

Արտադրող/Սարքավորում արտադրող: Տախոգրաֆ սարքավորումների արտադրողներ: Սույն քաղաքականությունում առավել հաճախ օգտագործվում է որպես ՓՄ և Արագության սենսորներ արտադրողներ, քանի որ սրանք նշանակալի պարտավորություն ունեն Համակարգում:

Արագության սենսորների բանալի: Համաչափ բանալի, որն օգտագործվում է Արագության սենսորների և ՓՄ-ի համար՝ փոխադարձ ճանաչումն ապահովելու նպատակով:

Փորձի մասին վկայող հայտարարություն (Հ): Տախոգրաֆի գործարկման անվտանգության ապահովման փորձի մասին վկայող ուղեցույց: Հ-ն համեմատելի է ստանդարտ ՀՀԵ փաստաթղթի՝ ՀՀ-ՀՈՒ-ի հետ:

Մասնավոր բանալի: Անհամաչափ բանալու զույգի մասնավոր հատվածը, որն օգտագործվում է հանրային բանալու գաղտնագրման տեխնիկայի համար: Մասնավոր բանալին սովորաբար օգտագործվում է թվային ստորագրություններ դնելիս կամ հաղորդագրություններն ապակոդավորելիս: Նաև կոչվում է Գաղտնի բանալի:

Հանրային բանալի: Անհամաչափ բանալու զույգի հանրային հատվածը, որն

օգտագործվում է հանրային բանալու գաղտնագրման տեխնիկայի համար: Հանրային բանալին սովորաբար օգտագործվում է թվային ստորագրությունների վավերականացման կամ մասնավոր բանալու տիրոջն ուղղված հաղորդագրությունների գաղտնագրման համար:

ՀՀԱ բանալիներ: ՀՀԱ-ն կրիպտոգրաֆիկ ալգորիթմ է, որն օգտագործվում է ***անհամաչափ*** (ՀՀԵ) բանալիների համար Տախոգրաֆ համակարգում:

Ծառայություններ մատուցող գործակալություն: Մարմին, որը ստանձնում է ՀՀ-ԱՊՀՄ-ի համար նախատեսված հանձնարարությունների կատարումը, ենթակապալառու:

Տախոգրաֆ քարտեր/Քարտեր: Տախոգրաֆ համակարգում կիրառվելիք քարտերի չորս տեսակներ՝ Վարորդական քարտ, Կազմակերպության քարտ, Արհեստանոցի քարտ, Վերահսկողության քարտ:

Օգտագործող: Օգտագործողները սարքավորումների օգտագործողներն են և կամ Քարտատերերն են կամ քարտի արտադրողներ Փոխադրամիջոցների միավորների/Արագության սենսորների համար: Բոլոր օգտագործողները պետք է ինքնատիպ նույնականացվող մարմիններ լինեն:

Սույն փաստաթղթում՝
Ստորագրված է: Որտեղ սույն քաղաքականությունը ստորագրություն է պահանջում, պահանջը պետք է կատարվի անվտանգ և վավերական էլեկտրոնային ստորագրության միջոցով:
Գրավոր: Որտեղ սույն քաղաքականությունը պահանջում է տեղեկատվությունը գրավոր տեսքով, պահանջը պետք է կատարվի տվյալների հաղորդագրության միջոցով, եթե դրանում տեղակայված տեղեկատվությունը հասանելի է և կարող է կիրառելի լինել շահագրգռված կողմերի համար:

14.2.Հապավումների ցանկ

ՀՄ	Հավաստագրման մարմին
ՀՄԱ/ԱԱ	Հավաստագրող մարմնի ադմինիստրատոր/Անհատականացնող ադմինիստրատոր
ՀՄՀ	Հավաստագրող մարմնի համակարգ
ՀՀ-ՔՏՄ	Հայաստանի Հանրապետության համար քարտ տրամադրող մարմին
ԸՉ	Ընդհանուր չափանիշներ
ՀՀ-ՔԱԿ	Հայաստանի Հանրապետության համար քարտի անհատականացման կազմակերպություն

ՀՀ-ՀՀ	Հավաստագրման փորձի մասին վկայող հայտարարություն
ԵԵՀՄ	Եվրոպական երթուղիների հավաստագրման մարմին
ՏՀԱԱ	Տեղեկատվական համակարգի անվտանգության աշխատակից
ՏՏԱԳՉ	Տեղեկատվական տեխնոլոգիաների անվտանգության գնահատման չափանիշներ
ԲԱ	Բանալիների արտադրություն
ԱՊ	Անդամ-պետություն
ԱՊՄ	Անդամ-պետության մարմին
ՀՀ-ԱՊՀՄ	Հայաստանի Հանրապետության համար անդամ-պետության հավաստագրման մարմին
ԱՆՀ	Անհատական նույնականացման համար
ՀԲԵ	Հանրային բանալու ենթակառուցվածք
ՀՀԲ	Հատուկ հանրային բանալիներ ալգորիթմ
ՀԱ	Համակարգի ադմինիստրատոր
ՈՒ	Փորձի մասին վկայող հայտարարություն
ՓՄ	Փոխադրամիջոցների միավոր
ՓՄԱ	ՓՄ անհատականացնող կազմակերպություն