ՀԱՍՏԱՏՎԱԾ ԵՆ

Եվրասիական տնտեսական հանձնաժողովի խորհրդի  
20 թվականի ի   
թիվ որոշմամբ

**ՊԱՀԱՆՋՆԵՐ**

վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող

I. Ընդհանուր դրույթներ

1. Սույն պահանջները մշակվել են «Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական հաղորդակցական տեխնոլոգիաների և տեղեկատվական փոխգործակցության մասին» արձանագրության («Եվրասիական տնտեսական միության մասին» 2014 թվականի մայիսի 29-ի պայմանագրի թիվ 3 հավելված) 18-րդ կետին համապատասխան և սահմանում են Եվրասիական տնտեսական միության (այսուհետ՝ Միություն) շրջանակներում վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջները:

2. Սույն պահանջների նպատակը Միության անդամ պետությունների (այսուհետ՝ անդամ պետություններ) պետական իշխանության մարմինների միջև՝ միմյանց և Եվրասիական տնտեսական հանձնաժողովի հետ (այսուհետ՝ Հանձնաժողով) տվյալների և էլեկտրոնային փաստաթղթերի միջպետական փոխանակման ժամանակ վստահության, ինչպես նաև Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտների կողմից տվյալ պահանջների կիրառման արդյունքում վստահության անդրսահմանային տարածքի գործունեության պաշտպանվածության և հուսալիության փոխընդունելի մակարդակի ապահովումն է:

3. Վստահության անդրսահմանային տարածքի տարրերի նկատմամբ պահանջները սահմանում են տվյալների և էլեկտրոնային փաստաթղթերի միջպետական փոխանակման ժամանակ վստահության ապահովման իրավական, կազմակերպչական և տեխնիկական պայմանները, այդ թվում ընդգրկում են տեղեկատվության պաշտպանության հարցերը:

4. Վստահության անդրսահմանային տարածքի տարրերի նկատմամբ պահանջները որոշվում են այդ տարրերի համար արդիական՝ տեղեկատվության անվտանգության սպառնալիքներին և խախտում կատարողի գործողություններին համապատասխան:

5. Սույն պահանջները չեն տարածվում որևէ ծառայության, տարրի և բաղադրիչի վրա, որն օգտագործվում է բացառապես տվյալների և էլեկտրոնային փաստաթղթերի ներպետական փոխանակման նպատակներով:

6. Սույն պահանջների նպատակների համար օգտագործվում են հասկացություններ, որոնք ունեն հետևյալ իմաստը՝

**հավատարմագրում**՝ կազմակերպչական-տեխնիկական միջոցառումների համալիր, որոնց արդյունքում փաստաթղթերով հաստատվում է դիմումատուի (լիազորված մարմնի կամ կազմակերպության) համապատասխանությունը հավատարմագրման պայմաններին, և միջպետական հանձնաժողովի և լիազորված մարմինների կողմից՝ սույն պահանջներին համապատասխան վստահության անդրսահմանային տարածքի շրջանակներում գործառույթներ իրականացնելու և ծառայություններ տրամադրելու նրա կարողությունների (իրավասությունների) պաշտոնական ճանաչում.

**կրիպտոգրաֆիկ ստանդարտ**՝ տեխնիկական այն մասնագրերի ամբողջությունը, որոնք սահմանում են կրիպտոգրաֆիկ բանալու օգտագործմամբ տեղեկատվության փոխակերպման (կրիպտոգրաֆիկ փոխակերպում), այդ թվում՝ ԷԹՍ-ի ձևավորման և ստուգման կանոնները և ալգորիթմները.

**միջպետական հանձնաժողով**՝ լիազորված մարմինների և Հանձնաժողովի ներկայացուցիչներից կազմված հանձնաժողով, որն իրականացնում է սույն պահանջներին էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների համապատասխանության ստուգում.

**էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածք**՝ Միության շրջանակներում օգտագործվող էլեկտրոնային փաստաթղթերին իրավաբանական ուժ տալու նպատակներով իրականացվող տեղեկատվական-տեխնոլոգիական և կազմակերպաիրավական միջոցառումների, կանոնների ու որոշումների ամբողջություն.

**էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորներ**՝ Հանձնաժողով կամ լիազորված մարմիններ կամ անդամ պետությունների օրենսդրությանը համապատասխան դրանց կողմից սահմանված կազմակերպություններ, որոնք միջպետական հանձնաժողովի կողմից հավատարմագրվել են սույն պահանջներին համապատասխան վստահության անդրսահմանային տարածքի շրջանակներում ծառայություններ տրամադրելու և գործառույթներ իրականացնելու համար.

**ԷԹՍ-ի ստուգման բանալու հավաստագիր**՝ հավաստագրման կենտրոնի կողմից թողարկված, ԷԹՍ բանալու օգտագործմամբ հավաստագրման կենտրոնի ԷԹՍ-ով ստորագրված և հավաստագրում նշված ԷԹՍ ստուգման բանալու՝ էլեկտրոնային փաստաթղթերի փոխանակման կոնկրետ մասնակցին պատկանելությունը հաստատող տեղեկատվություն և համապատասխան կրիպտոգրաֆիկ ստանդարտներով և սույն պահանջներով նախատեսված այլ տեղեկատվություն պարունակող էլեկտրոնային փաստաթուղթ.

**վստահված երրորդ կողմի ծառայություն**՝ վստահված երրորդ կողմի ծառայությունների ամբողջություն, որոնք գործում են Հանձնաժողովի ինտեգրացիոն հատվածի և Միության ինտեգրացված տեղեկատվական համակարգի ազգային հատվածների կազմում, որոնք ապահովում են ԷԹՍ վստահության անդրսահմանային միասնական տարածք՝ Միության ինտեգրացված տեղեկատվական համակարգերի միջոցներով սուբյեկտների էլեկտրոնային եղանակով փոխգործակցության դեպքում.

**վստահված երրորդ կողմի միջոցներ**՝ վստահված երրորդ կողմի գործառույթների իրականացման համար օգտագործվող ծրագրային և (կամ) ապարատային միջոցներ.

**հավաստագրման կենտրոնի միջոցներ**՝ հավաստագրման կենտրոնի գործառույթների իրականացման համար օգտագործվող ծրագրային և (կամ) ապարատային միջոցներ.

**ԷԹՍ միջոցներ**՝ կրիպտոգրաֆիկ միջոցներ, որոնք օգտագործվում են հետևյալ գործառույթներից առնվազն մեկի իրականացման համար՝ ԷԹՍ-ի ստեղծում, ԷԹՍ-ի ստուգում, ԷԹՍ բանալու ստեղծում և ԷԹՍ ստուգման բանալու ստեղծում.

**հավաստագրման կենտրոն**՝ լիազորված մարմին կամ կազմակերպություն, որը, Հանձնաժողովի ակտերին, անդամ պետությունների օրենսդրությանը համապատասխան, ապահովում է ԷԹՍ-ի ստուգման և հավաստագրերի վավերականության ստուգման բանալիների հավաստագրերի թողարկման, տարածման, պահպանման ծառայությունների տրամադրումը.

**Հանձնաժողովի հավաստագրման կենտրոն**՝ հավաստագրման կենտրոն, որը նախատեսված է Հանձնաժողովի կոլեգիայի անդամներին, Հանձնաժողովի պաշտոնատար անձանց և աշխատակիցներին ԷԹՍ-ի ստուգման բանալիների հավաստագրերով ապահովելու համար.

**վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոն**՝ հավաստագրման կենտրոն, որը նախատեսված է Միության ինտեգրացված տեղեկատվական համակարգի ինտեգրացիոն և ազգային հատվածների լիազորված վստահված երրորդ կողմերին ԷԹՍ-ի ստուգման բանալիների հավաստագրերով ապահովելու համար.

**լիազորված մարմին**՝ անդամ պետության պետական իշխանության մարմին կամ դրա կողմից սահմանված կազմակերպություն, որն օժտված է առանձին ոլորտներում պետական քաղաքականություն իրականացնելու լիազորություններով.

**ժամանակի դրոշմ**՝ էլեկտրոնային փաստաթղթի վավերապայման, որը հավաստում է էլեկտրոնային փաստաթղթի ստեղծման ամսաթիվը և ժամը.

**էլեկտրոնային թվային ստորագրություն (էլեկտրոնային ստորագրություն), «ԷԹՍ»**՝ էլեկտրոնային տեսքով տեղեկատվություն, որն էլեկտրոնային տեսքով կցված է այլ տեղեկատվության կամ այլ կերպ կապված է այդ տեղեկատվության հետ, ծառայում է այդ տեղեկատվության ամբողջականությունը և իսկությունը հսկելու համար, ապահովում է հեղինակությունից հրաժարվելու անհնարինությունը, մշակվում է տվյալ տեղեկատվության նկատմամբ փակ (անձնական) բանալու (ԷԹՍ բանալու) օգտագործմամբ կրիպտոգրաֆիկ փոխակերպում կիրառելու միջոցով և ստուգվում է բաց բանալու (ԷԹՍ-ի ստուգման բանալու) օգտագործմամբ:

II. Վստահության անդրսահմանային տարածքի ստեղծումը, զարգացումը և գործունեությունը

7. Վստահության անդրսահմանային տարածքի ստեղծումը, զարգացումը և գործունեությունն ապահովվում են Հանձնաժողովի և լիազորված մարմինների կողմից՝ Եվրասիական տնտեսական հանձնաժողովի խորհրդի 2014 թվականի սեպտեմբերի 18-ի թիվ 73 որոշմամբ հաստատված՝ «Միջպետական տեղեկատվական փոխգործակցության ժամանակ ծառայությունների և իրավաբանական ուժ ունեցող էլեկտրոնային փաստաթղթերի օգտագործման» հայեցակարգին, Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2016 թվականի սեպտեմբերի 27-ի թիվ 105 որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի զարգացման ռազմավարությանը, Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթին, ինչպես նաև Հանձնաժողովի՝ վստահության անդրսահմանային տարածքի ստեղծման, զարգացման և գործունեության հետ կապված հարցերի մասով այլ ակտերին համապատասխան:

8. Վստահության անդրսահմանային տարածքի ստեղծման, զարգացման և գործունեության նկատմամբ հսկողությունն իրականացվում է միջպետական հանձնաժողովի կողմից՝ այդ թվում էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների՝ սույն պահանջներին համապատասխանության ստուգման միջոցով:

9. Վստահության անդրսահմանային տարածքի զարգացման և գործունեության նկատմամբ հսկողության ապահովման նպատակով Միության ինտեգրացված տեղեկատվական համակարգի (այսուհետ՝ ինտեգրացված համակարգ) անդամ պետությունների ազգային հատվածների շրջանակներում անդամ պետությունների կողմից սահմանվում են լիազորված մարմիններ՝ վստահության անդրսահմանային տարածքի ապահովման իրավական, կազմակերպչական, տեխնիկական պայմաններին ներկայացվող, այդ թվում՝ էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների տեղեկատվության պաշտպանությանը վերաբերող պահանջների կատարման նկատմամբ հսկողություն իրականացնելու համար:

10. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքը բաղկացած է պետական բաղադրիչներից և ինտեգրացիոն բաղադրիչից։

11. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչի օպերատորը Հանձնաժողովն է։

12. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների օպերատորները լիազորված մարմիններն են:

13. Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտներ են պետական մարմինները, ֆիզիկական կամ իրավաբանական անձինք, որոնք փոխգործակցում են էլեկտրոնային փաստաթղթերը և էլեկտրոնային տեսքով տեղեկատվությունը կազմելու, ուղարկելու, փոխանցելու, ստանալու, պահպանելու և օգտագործելու ընթացքում ծագող հարաբերությունների շրջանակներում:

14. Միության շրջանակներում էլեկտրոնային փոխգործակցության դեպքում էլեկտրոնային փոխգործակցության սուբյեկտների միջև վստահությունն ապահովվում է էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների կողմից, որոնք իրականացնում են գործառույթներ և տրամադրում ծառայություններ սույն պահանջներին համապատասխան վստահության անդրսահմանային տարածքի շրջանակներում:

15. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների և ինտեգրացիոն բաղադրիչի կազմի մեջ մտնող՝ վստահության անդրսահմանային տարածքի տարրերը պետք է համապատասխանեն նկարագրությանը՝ համաձայն թիվ 1 հավելվածի:

16. Վստահության անդրսահմանային տարածքի տարրերը շահագործվում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի հավատարմագրված օպերատորների կողմից՝ սույն պահանջներին համապատասխան վստահության անդրսահմանային տարածքի շրջանակներում ծառայություններ տրամադրելու և գործառույթներ իրականացնելու համար:

17. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորը կարող է ապահովել վստահության անդրսահմանային տարածքի մի քանի տարրերի շահագործումը:

18. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորները պատասխանատու են էլեկտրոնային փոխգործակցության սուբյեկտներին հետևյալի արդյունքում պատճառված վնասի համար՝

ա) սույն պահանջներով նախատեսված պարտավորությունների չկատարում կամ ոչ պատշաճ կատարում.

բ) այն անդամ պետության օրենսդրությամբ նախատեսված չկատարում կամ ոչ պատշաճ կատարում, որի պետական բաղադրիչի մեջ դրանք մտնում են:

19. Հանձնաժողովը և անդամ պետությունները սահմանում են համաձայնեցված պահանջներ՝ սույն պահանջներն էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների գործունեության մասով խախտելու համար պատասխանատվության նկատմամբ:

20. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների հավատարմագրումն իրականացվում է Եվրասիական տնտեսական հանձնաժողովի խորհրդի  թվականի  -ի թիվ որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջներին էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների համապատասխանության ստուգման հարցերով հանձնաժողովի մասին հիմնադրույթին համապատասխան:

III. էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման   
ընդհանուր ենթակառուցվածքը

1. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնին ներկայացվող պահանջները

21. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնն իրականացնում է ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման մասով գործունեություն, որոնք նախատեսված են ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի կազմում գործող վստահված երրորդ կողմի (այսուհետ՝ Հանձնաժողովի վստահված երրորդ կողմ) և ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածներում գործող լիազորված վստահված երրորդ կողմերի (այսուհետ՝ անդամ պետությունների վստահված երրորդ կողմեր) էլեկտրոնային փոխգործակցության կազմակերպման համար:

22. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից տրամադրվող՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերի տիրապետողներ են՝

Հանձնաժողովի վստահված երրորդ կողմը.

անդամ պետությունների վստահված երրորդ կողմերը:

23. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնը պետք է գործի բաց բանալիների ենթակառուցվածքի (Public Key Infrastructure) ստեղծման վերաբերյալ միջազգային առաջարկություններին և լիազորված մարմինների հետ համաձայնեցված պահանջներին համապատասխան:

24. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնը ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման համար պետք է օգտագործի թիվ 2 հավելվածի համաձայն պահանջներին համապատասխանող՝ հավաստագրման կենտրոնի միջոցները: Նախքան նշված միջոցների օգտագործումը դրանց համապատասխանությունը նշված սահմանված պահանջներին պետք է հաստատվի Հանձնաժողովի գտնվելու երկրի լիազորված մարմինների կողմից՝ դրա օրենսդրությամբ սահմանված կարգով: Նախքան հավաստագրման կենտրոնի այն միջոցների օգտագործումը, որոնք մշակվել են վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի համար Միության տեղեկատվության կրիպտոգրաֆիկ պաշտպանության մասնագիտացված միջոցների համատեղ մշակման նախագծի շրջանակներում, դրանց համապատասխանությունը նշված սահմանված պահանջներին պետք է հաստատվի բոլոր անդամ պետությունների լիազորված մարմինների կողմից՝ դրանց օրենսդրությամբ սահմանված կարգով:

25. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի գործունեությանը ներկայացվող պահանջները սահմանվում են՝ հաշվի առնելով Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների մոդելները:

26. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնը պետք է ապահովի հետևյալ հիմնական գործառույթների կատարումը՝

ա) Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի գրանցում.

բ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծում և տրամադրում՝ ըստ Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի հարցումների.

գ) այն անձանց լիազորությունների սահմանում, որոնք հանդես են գալիս Հանձնաժողովի վստահված երրորդ կողմի անունից կամ անդամ պետությունների վստահված երրորդ կողմերի անունից ԷԹՍ-ի ստուգման բանալու հավաստագիր ստանալու համար դիմելիս, և նշված լիազորությունների մասին տեղեկատվության պահպանում՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի գործունեությունը կանոնակարգող՝ Հանձնաժողովի կողմից հաստատվող փաստաթղթերին համապատասխան.

դ) ԷԹՍ այն բանալու տիրապետման հաստատում, որը համապատասխանում է համապատասխան վստահված երրորդ կողմի կողմից՝ ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծման և ստացման հարցման մեջ նշված ԷԹՍ-ի ստուգման բանալուն, և նշված հավաստագրի ստեղծման մերժում՝ տվյալ բանալու տիրապետման հաստատման ժամանակ բացասական արդյունքի դեպքում.

ե) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի գործողության ժամկետների սահմանում: ԷԹՍ-ի ստուգման բանալու հավաստագիրը գործում է դրա տրման պահից, եթե այդ հավաստագրի գործողության սկզբի այլ ամսաթիվ նշված չէ անմիջապես հավաստագրում, ընդ որում, ԷԹՍ-ի ստուգման բանալու հավաստագրի մասին տեղեկատվությունը պետք է վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից ներառվի ԷԹՍ-ի ստուգման բանալիների տրված, գործողությունը դադարած և չեղյալ ճանաչված հավաստագրերի ռեեստրում (այսուհետ՝ հավաստագրերի ռեեստր) այդ հավաստագրում նշված՝ դրա գործողության սկզբի ամսաթվից ոչ ուշ.

զ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի գործողության դադարեցումը և չեղյալ ճանաչումը.

է) հավաստագրերի ռեեստրի վարում՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից տրված՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերում պարունակվող տեղեկատվության, ինչպես նաև այդ հավաստագրերի գործողության դադարեցման կամ չեղյալ ճանաչման ամսաթվերի և գործողության դադարեցման կամ չեղյալ ճանաչման հիմքերի մասին տեղեկատվության ներառմամբ.

ը) ԷԹՍ-ի ստուգման բանալիների՝ գործողությունը դադարած և չեղյալ ճանաչված հավաստագրերի ցանկի վարում (այսուհետ՝ հետ կանչված հավաստագրերի ցանկ).

թ) ԷԹՍ-ի ստուգման բանալու հավաստագրի տիրապետողին նրա հավաստագիրը չեղյալ ճանաչելու մասին տեղեկացում նախքան հավաստագրերի ռեեստրում և հետ կանչված հավաստագրերի ցանկում համապատասխան փոփոխություններ կատարելը.

ժ) հավաստագրերի ռեեստրում ԷԹՍ-ի ստուգման բանալիների եզակիության ստուգում և ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծման մերժում՝ Հանձնաժողովի վստահված երրորդ կողմի կամ անդամ պետության վստահված երրորդ կողմի հարցման մեջ նշված՝ ԷԹՍ-ի բանալու եզակիության ստուգման բացասական արդյունքի դեպքում.

ժա) հավաստագրերի ռեեստրում և հետ կանչված հավաստագրերի ցանկում պարունակվող տեղեկատվության արդիականացում, ինչպես նաև դրա պաշտպանությունն անօրինական հասանելիությունից, ոչնչացումից, ձևափոխումից, բլոկավորումից և անօրինական այլ գործողություններից.

ժբ) հավաստագրերի ռեեստրում ներառված տեղեկատվության պահպանում վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի գործունեության ամբողջ ընթացքում.

ժգ) Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի անհատույց հիմունքներով հասանելիություն հավաստագրերի ռեեստրին ինտեգրացված համակարգի միջոցների օգտագործմամբ ցանկացած ժամանակ.

ժդ) ԷԹՍ-ի ստուգումների իրականացում՝ ըստ Հանձնաժողովի վստահված երրորդ կողմի կամ անդամ պետությունների վստահված երրորդ կողմերի դիմումների, որոնք ստեղծվել են դրանց տրված՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերի օգտագործմամբ.

ժե) ժամանակի դրոշմների ստեղծում Հանձնաժողովի վստահված երրորդ կողմի անդորրագրերի և անդամ պետությունների վստահված երրորդ կողմերի անդորրագրերի վրա, որոնք պարունակում են ԷԹՍ-ի ստուգման արդյունքներ, որոնցով ստորագրված են էլեկտրոնային փաստաթղթերը, էլեկտրոնային փաստաթղթերի ստեղծման ժամանակի հաստատման և համապատասխան ԷԹՍ-ով դրանց ստորագրման նպատակով այդպիսի վստահված երրորդ կողմերի դիմելու դեպքում.

ժզ) ԷԹՍ-ի օգտագործման հետ կապված այլ գործառույթների իրականացում:

27. Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի գործունեության համար Հանձնաժողովը լիազորված մարմինների հետ փոխգործակցության միջոցով մշակում և հաստատում է տեխնիկական, տեխնոլոգիական, մեթոդական և կազմակերպչական փաստաթղթեր, որոնք նախատեսում են վստահված երրորդ կողմի ծառայության հավաստագրված կենտրոնի նկատմամբ պահանջների մանրամասնումը:

28. Սույն պահանջները և այն պահանջները, որոնք պարունակվում են վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի գործունեության ապահովման համար Հանձնաժողովի կողմից հաստատվող ակտերում, միջպետական հանձնաժողովի կողմից կիրառվում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչի ստուգման շրջանակներում վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնը ստուգելու համար:

2. Վստահված երրորդ կողմի ծառայությանը և դրա կազմի մեջ մտնող վստահված երրորդ կողմերին ներկայացվող պահանջները

29. Վստահված երրորդ կողմի ծառայությունն ինտեգրացված համակարգի գործառութային մասն է:

30. Վստահված երրորդ կողմի ծառայությունը պետք է ներառի Հանձնաժողովի վստահված երրորդ կողմի ծառայությունները և անդամ պետությունների վստահված երրորդ կողմերի ծառայությունները:

31. Վստահված այն երրորդ կողմերից յուրաքանչյուրը, որոնց ծառայություններն ընդգրկված են վստահված երրորդ կողմի ծառայության կազմի մեջ, «Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական հաղորդակցական տեխնոլոգիաների և տեղեկատվական փոխգործակցության մասին» արձանագրության 21-րդ կետին համապատասխան պետք է իրականացնի հետևյալ խնդիրները՝

ա) էլեկտրոնային փոխգործակցության սուբյեկտների էլեկտրոնային փաստաթղթերի և ԷԹՍ-ի օրինականացման իրականացում (իսկության հաստատում)՝ ժամանակի ֆիքսված պահին.

բ) էլեկտրոնային փաստաթղթերի միջպետական (անդրսահմանային) փոխանակման գործում վստահության երաշխիքների ապահովում.

գ) ելից և (կամ) մտից փաստաթղթերում ԷԹՍ-ի կիրառման իրավաչափության ապահովում անդամ պետությունների օրենսդրությանը և Հանձնաժողովի ակտերին համապատասխան:

32. Հանձնաժողովի վստահված երրորդ կողմը և անդամ պետությունների վստահված երրորդ կողմերը պետք է ապահովեն վստահված երրորդ կողմերի միջոցների օգտագործմամբ իրականացվող ծառայությունների հետևյալ ամբողջության գործելն իր կազմում՝

ա) իսկության հաստատման ծառայություն (ԷԹՍ-ի, ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության և սահմանված պահանջներին դրա համապատասխանության ստուգում, լիազորությունների ստուգման ծառայությունից արդյունքի ստացում և էլեկտրոնային փաստաթղթի իսկության ստուգման արդյունքով անդորրագրերի ստեղծում).

բ) լիազորությունների ստուգման ծառայություն (էլեկտրոնային փոխգործակցության այն սուբյեկտի լիազորությունների ստուգում, որը ստեղծել և ստորագրել է էլեկտրոնային փաստաթուղթն ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածում կամ Հանձնաժողովի ինտեգրացիոն հատվածում).

գ) ժամանակի դրոշմի ծառայություն (ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածի կամ Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթերի համար ժամանակի դրոշմների և էլեկտրոնային փաստաթղթի իսկության ստուգման արդյունքով անդորրագրերի ստեղծում).

դ) տվյալների պահպանման ծառայություն (վստահված երրորդ կողմի կողմից կատարվող գործառնությունների փաստաթղթավորում).

ե) տեղեկատվության տրամադրման ծառայություն (վստահված երրորդ կողմի գործառնությունների մասին՝ ըստ լիազորված մարմինների և Հանձնաժողովի հարցումների):

33. Հանձնաժողովի վստահված երրորդ կողմի միջոցներով կամ անդամ պետությունների վստահված երրորդ կողմերի միջոցներով իրականացվող ծառայությունները պետք է համապատասխանեն սույն պահանջներին, «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթին, ինչպես նաև Հանձնաժողովի՝ վստահված երրորդ կողմերի գործունեության հարցերին վերաբերող ակտերին:

34. Հանձնաժողովի վստահված երրորդ կողմը և անդամ պետությունների վստահված երրորդ կողմերն իրենց գործառույթներն իրականացնելիս պետք է ապահովեն հետևյալ հիմնական պայմանների պահպանումը՝ իրենց համակցությամբ՝

ա) այն ԷԹՍ-ի բանալու գաղտնիության ապահովում, որի ստուգման բանալին պարունակվում է վստահված երրորդ կողմի կողմից տրված՝ ԷԹՍ-ի ստուգման բանալու հավաստագրում.

բ) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի, Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի ծանուցում՝ Միության շրջանակներում էլեկտրոնային փոխգործակցության համար նախատեսված ԷԹՍ-ի բանալու գաղտնիության խախտման մասին՝ ոչ ավելի, քան այդպիսի խախտման վերաբերյալ տեղեկատվություն ստանալու պահից 12 ժամվա ընթացքում.

գ) Միության շրջանակներում փոխգործակցության համար նախատեսված ԷԹՍ-ի բանալու օգտագործման դադարեցում, եթե առկա են հիմքեր՝ ենթադրելու համար, որ տվյալ բանալու գաղտնիությունը խախտվել է.

դ) Միության շրջանակներում փոխգործակցության համար նախատեսված ԷԹՍ-ի բանալու օգտագործում՝ բացառապես էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքներով անդորրագրերի ստորագրման համար.

ե) Միության շրջանակներում էլեկտրոնային փոխգործակցության համար նախատեսված ԷԹՍ-ի ստեղծման և ստուգման, ԷԹՍ-ի բանալիների և ԷԹՍ-ի ստուգման բանալիների ստեղծման համար տեղեկատվության կրիպտոգրաֆիկ պաշտպանության այն միջոցների օգտագործում, որոնք իրականացնում են կրիպտոգրաֆիկ ալգորիթմներ, որոնք սահմանված են Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2016 թվականի հունիսի 2-ի թիվ 49 որոշմամբ (ԾՕՀ), նախքան Միության՝ տեղեկատվության կրիպտոգրաֆիկ պաշտպանության մասնագիտացված միջոցների համատեղ մշակման նախագծի իրականացումը.

զ) էլեկտրոնային փաստաթղթերում ԷԹՍ-ի ստուգման ժամանակ հետևյալ պայմանների՝ դրանց համակցությամբ պահպանման ստուգում՝

ԷԹՍ-ով ստորագրվող տվյալների ամբողջականությունը խախտված չէ.

ԷԹՍ-ն մշակված է ԷԹՍ-ի բանալու օգտագործմամբ, ԷԹՍ-ի ստուգման բանալու համապատասխան հավաստագիրը վստահված երրորդ կողմի տրամադրության տակ է ստուգումը սկսելու պահին կամ վստահված երրորդ կողմի կողմից ստացվել է ստուգման ընթացակարգերի իրականացման ընթացքում.

ԷԹՍ-ի ստուգման բանալու հավաստագիրը էլեկտրոնային փաստաթղթի ստորագրման պահին վավեր է.

հավաստագրման կենտրոնների ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից ԷԹՍ-ի ստուգման բանալու յուրաքանչյուր հավաստագիր վավեր է ստորագրման պահին.

է) Հանձնաժողովի ակտերով կամ անդամ պետությունների օրենսդրությամբ սահմանված ժամանակահատվածի ընթացքում էլեկտրոնային փաստաթղթերում ԷԹՍ-ի անցկացվող բոլոր ստուգումներին վերաբերող անհրաժեշտ ամբողջ տեղեկատվության փաստաթղթավորում և պահպանում՝ ծառայությունների տրամադրման անընդհատությունն ապահովելու և (անհրաժեշտության դեպքում) դատարանում ապացույցներ ներկայացնելու համար: Նշված տեղեկատվության պահպանումը կարող է իրականացվել էլեկտրոնային եղանակով:

35. Հանձնաժողովի վստահված երրորդ կողմը պետք է օգտագործի վստահված երրորդ կողմի միջոցներ և ԷԹՍ-ի միջոցներ դրանց կազմում, որոնք համապատասխանում են պահանջներին՝ համաձայն թիվ 3 հավելվածի:

36. Հանձնաժողովը Հանձնաժողովի վստահված երրորդ կողմի գործունեության ապահովման համար լիազորված մարմինների հետ փոխգործակցության միջոցով մշակում և հաստատում է տեխնիկական, տեխնոլոգիական, մեթոդական և կազմակերպչական փաստաթղթեր, որոնք նախատեսում են բաղադրիչների և ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի վստահված երրորդ կողմին ներկայացվող պահանջների մանրամասնում:

37. Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի՝ միմյանց միջև և վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի հետ փոխգործակցությանը ներկայացվող պահանջները սահմանվում են՝ հաշվի առնելով Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների համապատասխան մոդելները:

38. Անդամ պետությունների վստահված երրորդ կողմերի գործունեության ապահովման համար լիազորված մարմինները, անդամ պետությունների օրենսդրությանը և Հանձնաժողովի ակտերին համապատասխան, մշակում և հաստատում են տեխնիկական, տեխնոլոգիական, մեթոդական և կազմակերպչական փաստաթղթեր, որոնք նախատեսում են բաղադրիչների և անդամ պետությունների վստահված երրորդ կողմերին ներկայացվող պահանջների մանրամասնում:

39. Հանձնաժողովն իրականացնում է ինտեգրացված համակարգի ստեղծման և զարգացման աշխատանքների շրջանակներում մշակված և վստահված երրորդ կողմերի գործունեության համար նախատեսված՝ տեղեկատվության կրիպտոգրաֆիկ պաշտպանության ծրագրային և ապարատային միջոցների փոխանցումը շահագրգիռ անդամ պետությունների լիազորված մարմիններին՝ Հանձնաժողովի կողմից հաստատվող կարգով ազգային հատվածների կազմում օգտագործելու համար:

40. Սույն պահանջները և այն պահանջները, որոնք պարունակվում են վստահված երրորդ կողմերի գործունեությունն ապահովելու համար անդամ պետությունների և Հանձնաժողովի կողմից հաստատվող փաստաթղթերում, միջպետական հանձնաժողովի կողմից օգտագործվում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչի ստուգման շրջանակներում վստահված երրորդ կողմի ծառայությունը և դրա կազմի մեջ մտնող վստահված երրորդ կողմերին ստուգելու համար:

3. Պահանջներ, որոնք ներկայացվում են Հանձնաժողովի հավաստագրման կենտրոնին և անդամ պետությունների հավաստագրման կենտրոններին, որոնք Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտներին ապահովում են ԷԹՍ-ի ստուգման բանալիների հավաստագրերով

41. Հանձնաժողովի հավաստագրման կենտրոնը և անդամ պետությունների հավաստագրման կենտրոնները, որոնք էլեկտրոնային փոխգործակցության սուբյեկտներին ապահովում են ԷԹՍ բանալիների հավաստագրերով՝ Միության շրջանակներում էլեկտրոնային փոխգործակցության համար, Վստահության անդրսահմանային տարածքի զարգացման ռազմավարությանը համապատասխան՝ վստահության անդրսահմանային տարածքի տարրեր են և մտնում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների կազմի մեջ:

42. Միության շրջանակներում էլեկտրոնային փոխգործակցության համար թույլատրվում են միայն հավաստագրման այն կենտրոնները, որոնք լիազորված (հավատարմագրված են) անդամ պետությունների օրենսդրությանը կամ Հանձնաժողովի ակտերին համապատասխան:

43. Հանձնաժողովի հավաստագրման կենտրոնը և անդամ պետությունների հավաստագրման կենտրոնները պետք է գործեն բաց բանալիների ենթակառուցվածքի (Public Key Infrastructure) ստեղծման վերաբերյալ միջազգային առաջարկություններին համապատասխան և կատարեն սույն պահանջների 49-րդ կետում նշված նվազագույն անհրաժեշտ պահանջները:

44. Անդամ պետությունների հավաստագրման կենտրոնների գործունեությանը ներկայացվող պահանջները, այդ թվում՝ տեղեկատվության պաշտպանության մասով, սահմանվում են՝ հաշվի առնելով տեղեկատվության անվտանգության արդիական սպառնալիքները և խախտում կատարողի գործողությունները՝ անդամ պետությունների՝ տեղեկատվության պաշտպանության ոլորտում օրենսդրությանը համապատասխան:

45. Հանձնաժողովի հավաստագրման կենտրոնի գործունեությանը ներկայացվող պահանջները սահմանվում են՝ հաշվի առնելով Հանձնաժողովի հավաստագրման կենտրոնում տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների մոդելները:

Հանձնաժողովի հավաստագրման կենտրոնը ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման համար պետք է օգտագործի ԷԹՍ-ի միջոցներ և հավաստագրման կենտրոնի միջոցներ, որոնք համապատասխանում են պահանջներին՝ համաձայն թիվ 4 հավելվածի: Նախքան նշված միջոցների օգտագործումը դրանց համապատասխանությունը նշված պահանջներին պետք է հաստատվի Հանձնաժողովի գտնվելու երկրի լիազորված մարմինների կողմից՝ դրա օրենսդրությամբ սահմանված կարգով:

46. Անդամ պետությունների հավաստագրման կենտրոնները ստեղծում են ԷԹՍ-ի ստուգման բանալիների հավաստագրեր՝ համապատասխան անդամ պետության օրենսդրությանը համապատասխան:

47. Հանձնաժողովի հավաստագրման կենտրոնը ստեղծում է ԷԹՍ-ի ստուգման բանալիների հավաստագրեր՝ սույն պահանջներին համապատասխան:

48. ԷԹՍ-ի ստեղծման և ստուգման համար անդամ պետություններում պետք է օգտագործվեն դրանց օրենսդրությանը համապատասխան հավաստագրված (սահմանված պահանջներին համապատասխանության հաստատում ստացած) ԷԹՍ միջոցներ:

49. Հավաստագրման կենտրոնների գործունեության համար անդամ պետությունների օրենսդրությանը համապատասխան սահմանվում են հետևյալ նվազագույն անհրաժեշտ պահանջները՝

ա) էլեկտրոնային փոխգործակցության սուբյեկտների ինքնության ստուգման ապահովում՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերի տրամադրման ժամանակ: Հավաստագիրը ստացողի ինքնության ստուգումն իրականացվում է կա՛մ անմիջապես հավաստագրման կենտրոնի կողմից, կա՛մ երրորդ անձի (գրանցման կենտրոնի և այլն) ներգրավմամբ, եթե դա նախատեսված է անդամ պետությունների օրենսդրությամբ.

բ) հավաստագրման կենտրոնի ծառայություններից օգտվելու պայմանների, այդ թվում՝ դրանցից օգտվելու ցանկացած սահմանափակման մասին տեղեկատվության հրապարակում «Ինտերնետ» տեղեկատվական-հեռահաղորդակցական ցանցում՝ ընդհանուր հասանելիության ռեժիմով.

գ) էլեկտրոնային փոխգործակցության սուբյեկտներին, անդամ պետությունների օրենսդրությանը կամ Հանձնաժողովի ակտերին համապատասխան՝ Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխանող ԷԹՍ-ի ստուգման բանալիների հավաստագրերի տրամադրում.

դ) էլեկտրոնային փոխգործակցության բոլոր սուբյեկտներին ԷԹՍ-ի ստուգման բանալիների տրամադրված բոլոր հավաստագրերի կարգավիճակի (արդիականության) մասին տեղեկատվության ժամանակին տրամադրում: Այդ տեղեկատվությունը պետք է հասանելի լինի ցանկացած ժամանակ, այդ թվում՝ նաև ԷԹՍ-ի ստուգման բանալու հավաստագրի գործողության դադարեցումից հետո, և տրամադրվի ավտոմատացված եղանակով.

ե) հավաստագրերը հետ կանչելու դեպքում տեղեկատվության օպերատիվ (հարցումը ստանալու օրը՝ հավաստագրման կենտրոնի աշխատանքային ռեժիմին համապատասխան) ներառում հավաստագրերի ռեեստրում և հետ կանչված հավաստագրերի ցանկում: Հավաստագիրը համարվում է հետ կանչված այդ հավաստագրի համապատասխան կարգավիճակի (արդիականության) մասին տեղեկատվություն պարունակող և էլեկտրոնային փոխգործակցության սուբյեկտներին ցանկացած ժամանակ հասանելի՝ հետ կանչված հավաստագրերի ցանկի հրապարակման պահից.

զ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի տրմանը, ստացմանը և դրանց կարգավիճակների (արդիականության) փոփոխմանը վերաբերող անհրաժեշտ ամբողջ տեղեկատվության փաստաթղթավորում և պահում առնվազն 15 տարի (այդ թվում՝ Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտներին ԷԹՍ-ի բանալիների հավաստագրերով ապահովելու գործունեության դադարեցումից հետո)՝ ծառայությունների տրամադրման անընդհատությունն ապահովելու և (անհրաժեշտության դեպքում) դատարանում ապացույցներ ներկայացնելու համար: Նշված տեղեկատվության պահպանումը կարող է իրականացվել էլեկտրոնային եղանակով.

է) հավաստագրման կենտրոնի կողմից ստեղծված և պահվող կրիպտոգրաֆիկ բանալիների գաղտնիության, ամբողջականության ապահովում.

ը) Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտներին ԷԹՍ-ի բանալիների հավաստագրերով ապահովելու գործունեությունը դադարեցնելու մտադրության կամ գործունեության դադարեցման այլ դեպքերի մասին լիազորված մարմիններին տեղեկացում:

50. Անդամ պետությունների հավաստագրման կենտրոնների գործունեության համար լիազորված մարմինները մշակում և հաստատում են տեխնիկական, տեխնոլոգիական, մեթոդական և կազմակերպչական փաստաթղթեր՝ իրենց անդամ պետությունների օրենսդրությանը համապատասխան:

51. Հանձնաժողովի հավաստագրման կենտրոնի գործունեությունն ապահովելու համար Հանձնաժողովը լիազորված մարմինների հետ փոխգործակցության միջոցով մշակում և հաստատում է տեխնիկական, տեխնոլոգիական, մեթոդական և կազմակերպչական փաստաթղթեր:

52. Սույն պահանջները և այն պահանջները, որոնք պարունակվում են հավաստագրման կենտրոնների գործունեությունն ապահովելու համար անդամ պետությունների և Հանձնաժողովի կողմից հաստատվող փաստաթղթերում, միջպետական հանձնաժողովի կողմից օգտագործվում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչի ստուգման շրջանակներում վստահված երրորդ կողմի ծառայությունը ստուգելու համար:

4. Տվյալների և էլեկտրոնային փաստաթղթերի միջպետական փոխանակման ժամանակ անդամ պետությունների և Հանձնաժողովի տեղեկատվական համակարգերի և ռեսուրսների փոխգործակցության ապահովման ենթակառուցվածքին ներկայացվող պահանջներ

53. Տվյալների և էլեկտրոնային փաստաթղթերի միջպետական փոխանակման ժամանակ անդամ պետությունների և Հանձնաժողովի տեղեկատվական համակարգերի և ռեսուրսների փոխգործակցության ապահովման ենթակառուցվածքը կազմված է ինտեգրացված համակարգի ինտեգրացիոն հարթակից և անդամ պետությունների միջգերատեսչական տեղեկատվական փոխգործակցության համակարգերից:

54. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը կազմված է ինտեգրացիոն անցուղիներից, տվյալների սինքրոնացման ենթահամակարգից, տրանսպորտային ենթահամակարգից, արտաքին տեղեկատվական համակարգերի հետ փոխգործակցության ենթահամակարգից և փոխկապակցման ենթահամակարգից:

55. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը ներառում է անդամ պետությունների ինտեգրացիոն անցուղիները, որոնք գործում են ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածների կազմում, և Հանձնաժողովի ինտեգրված անցուղին, որը գործում է ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի կազմում:

56. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը տվյալների սինքրոնացման ենթահամակարգի շրջանակներում պետք է ապահովի Հանձնաժողովի ինտեգրացիոն հատվածի շրջանակներում ինտեգրացված համակարգի ենթահամակարգերի տեղեկատվական փոխգործակցությունը:

57. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը տրանսպորտային ենթահամակարգի շրջանակներում պետք է ապահովի ինտեգրացիոն հարթակի բաղադրիչների միջև էլեկտրոնային հաղորդագրությունների երաշխավորված առաքումը հաղորդագրությունների հերթերի օգտագործմամբ:

58. Ինտեգրացված համակարգի ինտեգրացիոն հարթակն արտաքին տեղեկատվական համակարգերի հետ փոխգործակցության ենթահամակարգի շրջանակներում պետք է ապահովի ինտեգրացիոն հարթակին միանալու միասնական կետ՝ Միության անդամ չհանդիսացող ինտեգրացիոն միավորումների, միջազգային կազմակերպությունների և պետությունների տեղեկատվական համակարգերի (այսուհետ՝ արտաքին տեղեկատվական համակարգեր) հետ տեղեկատվական փոխգործակցություն կազմակերպելիս:

59. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը փոխկապակցման ենթահամակարգի շրջանակներում պետք է ապահովի փոխգործակցությունն ինտեգրացիոն հարթակի ինտեգրացիոն անցուղու և անդամ պետություններում կիրառվող միջպետական տեղեկատվական փոխգործակցության համակարգերի (տիպային ինտեգրացիոն անցուղու հիման վրա իրականացված՝ անդամ պետությունների ազգային հատվածների ինտեգրացիոն անցուղիների համար), ինչպես նաև արտաքին տեղեկատվական համակարգերի հետ փոխգործակցության ենթահամակարգի միջև:

60. Տեղեկատվության փոխանակումը ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի ինտեգրացիոն անցուղու և տվյալների սինքրոնացման ենթահամակարգի միջև, ինչպես նաև տեղեկատվության փոխանակումը ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածների ինտեգրացիոն անցուղիների միջև, ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացված հատվածի ինտեգրացիոն անցուղու և ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածների ինտեգրացիոն անցուղիների միջև պետք է իրականացվի Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի հունվարի 27-ի թիվ 5 որոշմամբ հաստատված՝ Արտաքին և փոխադարձ առևտրի ինտեգրացված տեղեկատվական համակարգում տվյալների էլեկտրոնային փոխանակման կանոններին համապատասխան:

61. Անդամ պետությունների ազգային հատվածների ինտեգրացիոն անցուղիների և Հանձնաժողովի ինտեգրացիոն անցուղիների հաշվիչ ռեսուրսները պետք է ապահովեն դրանց հասանելիության մակարդակն օրը 24 ժամ, շաբաթը՝ 7 օր, տարին՝ 365 օր՝ բացառությամբ տեխնիկական սպասարկման ժամանակահատվածների:

62. Ինտեգրացված համակարգի ինտեգրացիոն հարթակը պետք է ապահովի վթարային այն իրավիճակների ճշգրիտ մշակումը, որոնք առաջացել են մուտքային տվյալների ոչ ճիշտ ձևաչափի կամ անթույլատրելի արժեքների արդյունքում: Նշված դեպքերում ինտեգրացված համակարգի ինտեգրացիոն հարթակը պետք է ապահովի համապատասխան մատյաններում վթարային իրավիճակների վերաբերյալ տեղեկատվության պահպանումը, ինչից հետո վերադառնա ոչ ճիշտ մուտքային տվյալների ստացմանը նախորդող աշխատանքային վիճակին:

63. Անդամ պետությունների ինտեգրացիոն անցուղիները և միջգերատեսչական տեղեկատվական փոխգործակցության համակարգերը պետք է ապահովեն փոխանցվող տվյալների պաշտպանությունը:

64. Ինտեգրացիոն անցուղիների օպերատորները պետք է սահմանափակեն այն աշխատակիցների շրջանակը, որոնք հասանելիություն ունեն փոխանցվող տվյալներին, ընդ որում, տվյալներին հասանելիությունը պետք է տրամադրվի այդ աշխատակիցներին միայն արտակարգ (կոնֆլիկտային) իրավիճակների քննության համար:

65. Անդամ պետությունների ինտեգրացիոն անցուղիները և միջգերատեսչական տեղեկատվական փոխգործակցության համակարգերը պետք է ապահովեն փոխանցվող տվյալներն ուղարկողների և ստացողների նույնականացումը և իսկորոշումը:

66. Ինտեգրացիոն անցուղիները պետք է ապահովեն փոխանցվող և ստացվող տվյալներով, այդ թվում՝ էլեկտրոնային փաստաթղթերով իրականացված գործառնությունների վերաբերյալ տեղեկատվության փաստաթղթավորումը և դրա պահպանումն անդամ պետությունների օրենսդրությամբ կամ Հանձնաժողովի ակտերով սահմանված ժամանակահատվածում, այդ թվում՝ դատարանում ապացույցներ ներկայացնելու հնարավորության համար:

67. Ինտեգրացիոն անցուղիների ծառայությունները, որոնք օգտագործվում են անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակումն իրականացնելու համար, պետք է համապատասխանեն սույն պահանջներին, «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթի պահանջներին և Հանձնաժողովի՝ ինտեգրացիոն անցուղիների գործունեության հարցերի վերաբերյալ այլ ակտերի:

5. Տեղեկատվության պաշտպանության ապահովման ենթակառուցվածքին և համակարգերին ներկայացվող պահանջները

68. Ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի պաշտպանության համար Հանձնաժողովի կողմից օգտագործվում է տեղեկատվական անվտանգության ենթահամակարգ, որը, Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի հոկտեմբերի 12-ի թիվ 137 որոշմամբ հաստատված՝ Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգ ստեղծելու տեխնիկական խնդրին համապատասխան, նախատեսված է ապահովելու տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը Հանձնաժողովի ինտեգրացիոն հատվածում դրանց մշակման և պահպանման ժամանակ, ինչպես նաև ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածների հետ փոխգործակցության ժամանակ կապի ուղիներով դրանց փոխանցման ժամանակ:

69. Ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածների պաշտպանության համար լիազորված մարմինները պետք է ապահովեն անդամ պետություններում անդամ պետությունների ազգային հատվածների տեղեկատվության պաշտպանության այնպիսի ենթահամակարգերի ստեղծումը և ներդրումը, որոնք, ինտեգրացված համակարգ ստեղծելու տեխնիկական խնդրին համապատասխան, նախատեսված են ապահովելու տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունն անդամ պետության ազգային հատվածում դրանց ստեղծման, մշակման և պահպանման ժամանակ, ինչպես նաև Հանձնաժողովի ինտեգրացիոն հատվածի և ինտեգրացված համակարգի՝ մյուս անդամ պետությունների ազգային հատվածների հետ փոխգործակցելիս կապի ուղիներով դրանց փոխանցման ժամանակ: Ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածում տեղեկատվության գաղտնիության, ամբողջականության, հասանելիության և պահպանվածության ապահովման համար ընդունվում և իրականացվում է տեղեկատվության պաշտպանության իրավական, կազմակերպչական և տեխնիկական միջոցների համալիր՝ համապատասխան անդամ պետության օրենսդրությանը համապատասխան:

70. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների օպերատորները պետք է ձեռնարկեն տեխնիկական և կազմակերպչական միջոցներ, որոնք ուղղված են դրանց կողմից իրականացվող գործառույթների համար սպառնալիքների չեզոքացմանը: Նշված միջոցները պետք է իրականացվեն տեղեկատվության անվտանգության սպառնալիքները և խախտում կատարողի գործողությունները սահմանելու հիման վրա, որոնք արտացոլվում են անդամ պետությունների օրենսդրությանը համապատասխան մշակվող փաստաթղթերում (անվտանգության մասով խնդիրներում, սպառնալիքների մոդելներում և այլն):

71. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների օպերատորները պետք է ապահովեն իրենց աշխատակիցների անհրաժեշտ գիտելիքների, հուսալիության, լոյալության, փորձի և որակավորման առկայությունը, ինչպես նաև նրանց՝ համապատասխան անդամ պետության օրենսդրությանը համապատասխան՝ տեղեկատվության պաշտպանության ոլորտում բավարար պատրաստվածությունը:

72. Վստահության անդրսահմանային տարածքի տարրերի տեղեկատվության գաղտնիության, ամբողջականության և հասանելիության խախտման ցանկացած փաստի հայտնաբերման դեպքում էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների օպերատորները պետք է առավելագույնս օպերատիվ կերպով տեղեկացնեն այդ մասին իրենց լիազորված մարմնին:

Եթե տեղեկատվության պաշտպանության խախտումը վերաբերում է 2 կամ ավելի անդամ պետությունների, ապա այդպիսի ծանուցում ստացած լիազորված մարմինը տեղեկացնում է այդ մասին մյուս անդամ պետությունների լիազորված մարմիններին և միջպետական հանձնաժողովին:

73. Տեղեկատվության պաշտպանության ապահովման միջոցները և եղանակները, որոնք էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների օպերատորների կողմից իրականացվում են վստահության անդրսահմանային տարածքի տարրերի և դրանց կողմից տրամադրվող ծառայությունների նկատմամբ, պետք է համապատասխանեն պահանջներին՝ համաձայն թիվ 5 հավելվածի:

ՀԱՎԵԼՎԱԾ ԹԻՎ 1

Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների

**Վստահության անդրսահմանային տարածքի**

ԿԱՌՈՒՑՎԱԾՔԸ

1. Սույն փաստաթուղթը սահմանում է վստահության անդրսահմանային տարածքի տարրերը՝ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2016 թվականի սեպտեմբերի 27-ի թիվ 105 որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի զարգացման ռազմավարության առաջին փուլի իրագործման շրջանակներում Եվրասիական տնտեսական միության անդամ պետությունների (այսուհետ համապատասխանաբար՝ Միություն, անդամ պետություններ) պետական իշխանության մարմինների միջև՝ միմյանց և Եվրասիական տնտեսական հանձնաժողովի հետ (այսուհետ՝ Հանձնաժողով) տվյալների և էլեկտրոնային փաստաթղթերի միջպետական փոխանակման ապահովման համար:

2. Իրավաբանական ուժ ունեցող էլեկտրոնային փաստաթղթերի օգտագործմամբ միջպետական տեղեկատվական փոխգործակցություն իրականացնելիս վստահությունն ապահովելու համար Միության շրջանակներում ստեղծվում են վստահության անդրսահմանային տարածքի տարրեր, որոնք մտնում են էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի մեջ, որը երաշխավորում է՝

էլեկտրոնային փաստաթղթերի ժամանակին և ճշգրիտ փոխանցումն էլեկտրոնային փոխգործակցության սուբյեկտների միջև՝ դրանց իրավաբանական ուժի ապահովմամբ (պահպանմամբ), ինչպես նաև տեղեկատվության պաշտպանության փոխընդունելի մակարդակի ապահովմամբ.

պահանջվող այն վկայությունների նախապատրաստման և ներկայացման համապատասխան մեթոդների առկայությունը ցանկացած տարաձայնության առաջացման դեպքում, որոնք թույլ են տալիս վերականգնել իրադարձությունների ընթացքը և որոշել դրանց պատճառը:

3. Վստահության անդրսահմանային տարածքի շրջանակներում յուրաքանչյուր անդամ պետությունում ստեղծվում է էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչ, Հանձնաժողովում ստեղծվում է էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչ:

4. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչը ներառում է վստահության անդրսահմանային տարածքի հետևյալ տարրերը՝

Միության ինտեգրացված տեղեկատվական համակարգի վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոն (այսուհետ համապատասխանաբար՝ ինտեգրացված համակարգ, վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոն), որը նախատեսված է ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի և անդամ պետությունների ազգային հատվածների լիազորված վստահված երրորդ կողմերի ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման և արդիականության ստուգման համար: Վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ծառայությունների կազմի մեջ է մտնում ժամանակի դրոշմի ծառայությունը, որն օգտագործվում է ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի և անդամ պետությունների ազգային հատվածների վստահված երրորդ կողմերի կողմից՝ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթին համապատասխան.

վստահված երրորդ կողմ, որը գործում է ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածում (այսուհետ՝ Հանձնաժողովի վստահված երրորդ կողմ), որը նախատեսված է էլեկտրոնային փաստաթուղթը ստորագրած անձի առնչությամբ ժամանակի ֆիքսված պահին էլեկտրոնային փաստաթղթերում ԷԹՍ-ի ստուգման և Հանձնաժողովի վստահված երրորդ կողմի հիմնական խնդիրների կատարման համար՝ «Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական հաղորդակցական տեխնոլոգիաների և տեղեկատվական փոխգործակցության մասին» արձանագրությանը («Եվրասիական տնտեսական միության մասին» 2014 թվականի մայիսի 29-ի պայմանագրի թիվ 3 հավելված) համապատասխան: Հանձնաժողովի վստահված երրորդ կողմի ծառայությունների կազմի մեջ է մտնում ժամանակի դրոշմի ծառայությունը, որն օգտագործվում է Հանձնաժողովի վստահված երրորդ կողմի և ինտեգրացված համակարգի՝ անդամ պետությունների ազգային հատվածներում գործող լիազորված վստահված երրորդ կողմերի (այսուհետ՝ անդամ պետությունների վստահված երրորդ կողմեր) կողմից՝ Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթին համապատասխան.

Հանձնաժողովի հավաստագրման կենտրոն, որը նախատեսված է Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտ հանդիսացող՝ Հանձնաժողովի կոլեգիայի անդամներին, պաշտոնատար անձանց և Հանձնաժողովի աշխատակիցներին ԷԹՍ-ի ստուգման բանալիների հավաստագրերով ապահովելու և ԷԹՍ-ի ստուգման բանալիների տրված հավաստագրերի արդիականությունը ստուգելու համար.

ինտեգրացված համակարգի ինտեգրացիոն հարթակ, որն ապահովում է էլեկտրոնային փաստաթղթերի և տվյալների երթուղումը և երաշխավորված առաքումն ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի և անդամ պետությունների ազգային հատվածների միջև էլեկտրոնային փոխգործակցության ժամանակ.

ինտեգրացված համակարգի ինտեգրացիոն անցուղի, որն ապահովում է ինտեգրացված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի ենթահամակարգերի փոխգործակցությունը ինտեգրացված համակարգի ինտեգրացիոն հարթակի հետ.

ինտեգրացված համակարգի տեղեկատվական անվտանգության ենթահամակարգ, որը նախատեսված է ապահովելու համար տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը Հանձնաժողովի ինտեգրացիոն հատվածում դրանց մշակման և պահպանման ժամանակ, ինչպես նաև դրանց՝ կապի այն ուղիներով փոխանցման ժամանակ, որոնք միավորում են ինտեգրված համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի ինտեգրացիոն անցուղիները և անդամ պետությունների ազգային հատվածների ինտեգրացիոն անցուղիները:

5. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի յուրաքանչյուր պետական բաղադրիչ ներառում է վստահության անդրսահմանային տարածքի հետևյալ տարրերը՝

անդամ պետության վստահված երրորդ կողմ, որը նախատեսված է էլեկտրոնային փաստաթուղթը ստորագրած անձի առնչությամբ ժամանակի ֆիքսված պահին էլեկտրոնային փաստաթղթերում ԷԹՍ-ի ստուգման և անդամ պետության վստահված երրորդ կողմի հիմնական խնդիրների կատարման համար՝ «Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական հաղորդակցական տեխնոլոգիաների և տեղեկատվական փոխգործակցության մասին» արձանագրությանը համապատասխան: Անդամ պետության վստահված երրորդ կողմի ծառայությունների կազմի մեջ է մտնում ժամանակի դրոշմի ծառայությունը, որն օգտագործվում է վստահված երրորդ կողմի կողմից՝ Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթին համապատասխան.

անդամ պետության հավաստագրման կենտրոններ, ինչպես նաև այլ ենթակառուցվածք, որը նախատեսված է Միության շրջանակներում էլեկտրոնային փոխգործակցության սուբյեկտներին ԷԹՍ-ի ստուգման բանալիների հավաստագրերով ապահովելու և ԷԹՍ-ի ստուգման բանալիների տրված հավաստագրերի արդիականությունը ստուգելու համար.

ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածի ինտեգրացիոն անցուղի, որն ապահովում է անդամ պետության միջգերատեսչական տեղեկատվական փոխգործակցության համակարգի միացումն ինտեգրացված համակարգի ինտեգրացիոն հարթակին.

ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածի պաշտպանության ենթահամակարգ, որը նախատեսված է ապահովելու համար տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունն ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածում դրանց մշակման և պահպանման ժամանակ. ինտեգրացված համակարգի՝ անդամ պետության ազգային հատվածում տեղեկատվության գաղտնիության, ամբողջականության, հասանելիության և պահպանվածության ապահովման համար ընդունվում և իրականացվում է տեղեկատվության պաշտպանության իրավական, կազմակերպչական և տեխնիկական միջոցների համալիր՝ համապատասխան անդամ պետության օրենսդրության համաձայն:

ՀԱՎԵԼՎԱԾ ԹԻՎ 2

Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների

**ՊԱՀԱՆՋՆԵՐ**

Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգի վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի միջոցներին ներկայացվող

I. Ընդհանուր դրույթներ

1. Սույն պահանջները սահմանում են պահանջներ, որոնք ներկայացվում են Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգի վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի միջոցներին (այսուհետ համապատասխանաբար՝ Միություն, հավաստագրման կենտրոն):

II. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովմանը ներկայացվող պահանջներ

2. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովումը չպետք է պարունակի միջոցներ, որոնք թույլ են տալիս ձևափոխել կամ խեղաթյուրել հավաստագրման կենտրոնի միջոցների ծրագրային ապահովման աշխատանքի ալգորիթմը:

3. Հավաստագրման կենտրոնի միջոցների կիրառական ծրագրային ապահովումը և հավաստագրման կենտրոնի կողմից օգտագործվող՝ տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների ծրագրային ապահովումը պետք է օգտագործեն համակարգային ծրագրային ապահովման միայն փաստաթղթավորված գործառույթներ:

4. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովումը պետք է ապահովի հավաստագրման կենտրոնի միջոցների համակարգային ադմինիստրատորի, հավաստագրման կենտրոնի միջոցների հավաստագրման ադմինիստրատորի, հավաստագրման կենտրոնի միջոցների օպերատորների և հավաստագրման կենտրոնի օգտագործողների՝ հավաստագրման կենտրոնի միջոցներով մշակվող տեղեկատվությանը հասանելիության սահմանազատումը՝ հավաստագրման կենտրոնի միջոցների համակարգային ադմինիստրատորի կողմից սահմանված՝ հասանելիության սահմանազատման կանոններին համապատասխան:

5. Հավաստագրման կենտրոնի միջոցների համակարգային և (կամ) կիրառական ծրագրային ապահովման կազմի մեջ պետք է մտնի մեխանիզմ, որն ապահովում է սահմանափակ հասանելիության տեղեկատվության պահպանման համար օգտագործվող՝ օպերատիվ և արտաքին հիշողության մաքրումը:

6. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովման ելակետային տեքստերը պետք է անցնեն տեղեկատվությունը հարձակումներից պաշտպանելու այն մեթոդների և եղանակների իրագործման մասով ստուգում, որոնց նախապատրաստման և անցկացման համար օգտագործվում են տեղեկատվության անվտանգությունը խախտողի հնարավորությունները, որոնք նշված են Եվրասիական տնտեսական հանձնաժողովի (այսուհետ՝ Հանձնաժողով) կողմից հաստատվող՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնում տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների մոդելներում:

7. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովման կազմի մեջ պետք է ընդգրկվի մեխանիզմ, որն ապահովում է կայունությունն արտաքին ցանցերից համակարգչային հարձակումների նկատմամբ:

8. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովման ելակետային տեքստերը պետք է անցնեն չհայտարարագրված հնարավորությունների բացակայության ֆորմալ վերիֆիկացում, ինչպես նաև հարձակումներին դիմակայելու տեղեկատվության պաշտպանության մեթոդների և եղանակների իրագործման ֆորմալ վերիֆիկացում, որոնց նախապատրաստման և անցկացման համար օգտագործվում են տեղեկատվության անվտանգությունը խախտողի հնարավորությունները, որոնք նշված են Հանձնաժողովի կողմից հաստատվող՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնում տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների մոդելում:

III. Հավաստագրման կենտրոնի ապարատային միջոցներին   
ներկայացվող պահանջները

9. Հավաստագրման կենտրոնի ապարատային միջոցներին ներկայացվում են հետևյալ պահանջները՝

ա) հավաստագրման կենտրոնի նպատակային գործառույթների իրագործման՝ Հանձնաժողովի կողմից սահմանվող՝ հավաստագրման կենտրոնի ապարատային միջոցների փորձարկումների համակարգի հետ համապատասխանության ստուգման անցկացում.

բ) հավաստագրման կենտրոնի՝ երրորդ երկրներում արտադրված ապարատային միջոցների հատուկ ստուգման անցկացում՝ տեղեկատվությունը գաղտնի կերպով ստանալու համար նախատեսված սարքերի հայտնաբերման նպատակով.

գ) հավաստագրման կենտրոնի ապարատային միջոցների ուսումնասիրությունների և BIOS ծրագրային ծածկագրի վերլուծության անցկացում՝ չհայտարարագրված հնարավորությունների առկայությունը բացառելու նպատակով, ինչպես նաև Միության անդամ պետությունների (այսուհետ՝ անդամ պետություններ) օրենսդրությանը համապատասխան սահմանված՝ կողմնակի էլեկտրամագնիսական ճառագայթումների և մակածումների ուղիներով տեղեկատվության արտահոսքից պաշտպանությանը ներկայացվող պահանջներին համապատասխանության մասով ուսումնասիրությունների անցկացում:

IV. Դերերի սահմանազատմանը ներկայացվող պահանջները

10. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվեն հետևյալ պարտադիր դերերը՝

ա) համակարգային ադմինիստրատոր, որի լիազորությունները ներառում են հավաստագրման կենտրոնի միջոցների տեղադրումը, փոխդասավորության և գործունեության ապահովումը, հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների պրոֆիլների ստեղծումը և պահպանումը, աուդիտի մատյանի պրոֆիլի և պարամետրերի փոխդասավորության ապահովումը.

բ) հավաստագրման ադմինիստրատոր, որի լիազորությունները ներառում են էլեկտրոնային թվային ստորագրության (էլեկտրոնային ստորագրության) (այսուհետ՝ ԷԹՍ) ստուգման բանալիների հավաստագրերի ստեղծումը և չեղարկումը.

գ) աուդիտի ադմինիստրատոր, որի լիազորությունները ներառում են աուդիտի մատյանի վերանայումը, պատճենումը և ամբողջական մաքրումը.

դ) օպերատոր, որի լիազորությունները ներառում են հավաստագրման կենտրոնի միջոցներում պահվող տեղեկատվության պատճենումը և վերականգնումը:

11. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվի մեխանիզմ, որը բացառում է տարբեր դերերի լիազորությունների օգտագործման նպատակով հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի մեկ անդամի ավտորիզացման հնարավորությունը:

12. Համակարգային ադմինիստրատորը չպետք է աուդիտի մատյանում փոփոխություններ կատարելու հնարավորություն ունենա:

V. Հավաստագրման կենտրոնի միջոցների ամբողջականությանը   
ներկայացվող պահանջները

13. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվի մեխանիզմ, որը բացառում է տեղեկատվության, հավաստագրման կենտրոնի համակարգային և (կամ) ապարատային միջոցների չարտոնված պատահական և (կամ) կանխամտածված խեղաթյուրման (փոփոխության, ձևափոխման) և (կամ) ոչնչացման հնարավորությունը (այսուհետ՝ ամբողջականության հսկողություն): Ամբողջականության հսկողության մեխանիզմին ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

14. Ամբողջականության հսկողությունը պետք է իրականացվի օպերացիոն համակարգի յուրաքանչյուր վերագործարկումից հետո մինչև դրա ներբեռնումը, ինչպես նաև հավաստագրման կենտրոնի միջոցների գործունեության ընթացքում դինամիկ կերպով (ամբողջականության դինամիկ հսկողություն):

15. Ամբողջականության դինամիկ հսկողությունը պետք է իրականացվի օրն առնվազն 1 անգամ:

16. Հավաստագրման կենտրոնի ծրագրային և (կամ) ապարատային միջոցների կազմում պետք է առկա լինեն հավաստագրման կենտրոնի ծրագրային միջոցների ամբողջականության վերականգնման միջոցներ:

VI. Հասանելիության կառավարմանը ներկայացվող պահանջները

17. Հավաստագրման կենտրոնի միջոցները պետք է ապահովեն հասանելիության կառավարման կամավոր և պարտադիր սկզբունքների իրագործումը, ինչպես նաև փակ աշխատանքային միջավայրի (ծրագրային այն միջավայրի, որը թույլ է տալիս դրանում ունենալ ծրագրերի և գործընթացների միայն ֆիքսված լրակազմ) ստեղծումը: Հասանելիության կառավարմանը ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

VII. Նույնականացմանը և իսկորոշմանը ներկայացվող պահանջները

18. Նույնականացումը և իսկորոշումը ներառում են հավաստագրման կենտրոնի միջոցների օգտագործողի, հավաստագրման կենտրոնի միջոցների կամ գործընթացի ադմինիստրատորների խմբի անդամի ճանաչում, ինչպես նաև դրանց իսկության ստուգում: Իսկորոշման բացասական արդյունքի դեպքում իսկորոշման մեխանիզմը պետք է արգելափակի այդ սուբյեկտների հասանելիությունը հավաստագրման կենտրոնի գործառույթներին:

19. Հավաստագրման կենտրոնի միջոցներում իսկորոշման ցանկացած իրականացված ընթացակարգի համար պետք է կիրառվի հասանելիության մեկ սուբյեկտի իսկորոշման՝ անընդմեջ հաջորդող փորձերի քանակի սահմանափակման մեխանիզմը, որոնց թիվը չպետք է գերազանցի 20-ը։ Հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի թիվը գերազանցելու դեպքում հասանելիության այդ սուբյեկտի համար հավաստագրման կենտրոնի միջոցների հասանելիությունը պետք է արգելափակվի 15 րոպեով:

20. Հավաստագրման կենտրոնի միջոցների օգտագործողների գրանցման ընթացակարգի (հավաստագրման կենտրոնի միջոցների օգտագործողների ռեեստրում տվյալների մուտքագրման) նկարագրությունը, այդ թվում՝ գրանցման ժամանակ հավաստագրման կենտրոնի միջոցների օգտագործողի կողմից անձը հաստատող փաստաթղթերի ներկայացման անհրաժեշտության մասին պահանջը պետք է պարունակվեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

21. Հավաստագրման կենտրոնի միջոցներին հասանելիություն ձեռք բերող բոլոր անձանց համար պետք է անցկացվի երկգործոն իսկորոշում։

22. Հավաստագրման կենտրոնի միջոցների օգտագործողների և հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների համար թույլատրվում է իրագործել հեռավար իսկորոշման մեխանիզմներ՝ իսկորոշման հավաստագրերի օգտագործմամբ՝ թույլատրված կրիպտոգրաֆիկ ալգորիթմների հիման վրա:

23. Հավաստագրման կենտրոնի միջոցների լոկալ հասանելիությունը ձեռք բերելիս հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների իսկորոշումը պետք է կատարվի նախքան այդ միջոցների՝ աշխատանքային վիճակի անցնելը (օրինակ՝ մինչև բազային օպերացիոն համակարգի ներբեռնումը)։

24. Լոկալ իսկորոշման համար պայմանանշանային, պարբերաբար փոփոխվող գաղտնաբառ օգտագործելու դեպքում այն պետք է կազմված լինի առնվազն 8 պայմանանշանից (այն դեպքում, երբ այբուբենի պայմանանշանների ընդհանուր թիվը կազմում է առնվազն 36): Գաղտնաբառի փոփոխման ժամանակահատվածը չպետք է գերազանցի 6 ամիսը։

VIII. Հավաստագրման կենտրոնի կողմից ստացվող կամ փոխանցվող տվյալների պաշտպանությանը ներկայացվող պահանջները

25. Հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու ինքնաստորագրված հավաստագիրը պետք է պահվի դրա ձևափոխումը կամ խեղաթյուրումը բացառող եղանակով:

26. Հավաստագրման կենտրոնի միջոցները պետք է ապահովեն սահմանափակ հասանելիության տեղեկատվություն պարունակող այն տվյալների փոխանցումը, որոնք ստացվել են հավաստագրման կենտրոնի կողմից կամ փոխանցվում են հավաստագրման կենտրոնից՝ տեղեկատվության չարտոնված հասանելիությունը բացառող եղանակով:

27. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն կեղծ հաղորդագրություններ (գործողություններ, որոնք էլեկտրոնային փոխգործակցության սուբյեկտների կամ հավաստագրման կենտրոնի միջոցների կողմից ընկալվում են որպես իրական հաղորդագրության փոխանցում՝ չարտոնված հասանելիությունից պաշտպանված եղանակով) պարտադրելուց պաշտպանությունը ԷԹՍ-ի ստուգման բանալիի հավաստագրերի օգտագործմամբ՝ թույլատրված կրիպտոգրաֆիկ ալգորիթմների կիրառման միջոցով: Կեղծ հաղորդագրություններ պարտադրելուց պաշտպանությանը ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

28. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն հավաստագրման կենտրոնի միջոցների օգտագործողի կողմից նրա համար ԷԹՍ-ի ստուգման բանալիի հավաստագրի ստեղծման նախնական հարցման պաշտպանված փոխանցման ընթացակարգը:

29. Հավաստագրման կենտրոնի միջոցները պետք է ընդունեն հավաստագրման կենտրոնի գործունեության համար կրիտիկական տեղեկատվությունն այն դեպքում, երբ այն ստորագրված է ԷԹՍ-ով:

30. Հավաստագրման կենտրոնի միջոցների բոլոր բաղադրիչները պետք է տեղադրվեն հսկվող մեկ գոտում:

IX. Իրադարձությունների գրանցմանը ներկայացվող պահանջները

31. Հավաստագրման կենտրոնի միջոցների օպերացիոն համակարգը պետք է ապահովի աուդիտի այն մատյանի վարումը, որը պարունակում է տեղեկատվություն համակարգային իրադարձությունների և այն իրադարձությունների մասին, որոնք կապված են հավաստագրման կենտրոնի կողմից դրա գործառույթների կատարման հետ:

32. Աուդիտի մատյանում գրանցվող իրադարձությունների ցանկը պետք է պարունակվի հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

33. Աուդիտի մատյանը պետք է հասանելի լինի միայն աուդիտի ադմինիստրատորի համար:

34. Աուդիտի մատյանի ամբողջական մաքրումն անցկացվում է միայն մաքրման ենթակա ամբողջ տեղեկատվությունը պատճենելուց հետո։ Այդպիսի մաքրումից հետո աուդիտի մատյանում որպես առաջին գրառում պետք է ավտոմատ գրանցվի մաքրում անցկացնելու փաստը (նշված մաքրումն անցկացնելու ամսաթվի, ժամի և այն անցկացրած անձի մասին տեղեկատվության նշմամբ)։

X. Հավաստագրման կենտրոնի միջոցների հուսալիությանը և գործունեության կայունությանը ներկայացվող պահանջները

35. Իրականացվում է հավաստագրման կենտրոնի ապարատային միջոցների այնպիսի խափանումների և անսարքությունների առաջացման հավանականության հաշվարկ, որոնք հանգեցնում են հավաստագրման կենտրոնի կողմից դրա գործառույթները չկատարելուն:

36. Հավաստագրման կենտրոնի ապարատային միջոցների այնպիսի խափանումների և անսարքությունների առաջացման հավանականությունն օրվա ընթացքում, որոնք հանգեցնում են հավաստագրման կենտրոնի կողմից դրա գործառույթները չկատարելուն, չպետք է գերազանցի հավաստագրման կենտրոնի կազմում օգտագործվող կրիպտոգրաֆիկ միջոցների խափանումների և անսարքությունների առաջացման նույնանման հավանականությունը։

37. Հավաստագրման կենտրոնի միջոցների (համալիր) հրաժարման միջին աշխատատևությունը կազմում է առնվազն 18 000 ժամ։

38. Պետք է իրականացվի հավաստագրման կենտրոնի միջոցների գործունեության կայունության փորձարկում։

39. Հավաստագրման կենտրոնի միջոցների վերականգնման ժամանակը կազմում է ոչ ավելի, քան 4 ժամ։

40. Հավաստագրման կենտրոնի միջոցների հուսալիության և դրանց գործունեության կայունության բարձրացման միջոցառումներն ու միջոցները պետք է նախատեսեն հավաստագրման կենտրոնի միջոցների ռեսուրսների քվոտավորում։

XI. Առանցքային տեղեկատվության ստեղծմանը, օգտագործմանը,   
պահպանմանը և ոչնչացմանը ներկայացվող պահանջները

41. Առանցքային տեղեկատվության ստեղծման, օգտագործման, պահպանման և ոչնչացման կարգը և դրա գործողության ժամկետները որոշվում են ԷԹՍ միջոցների և հավաստագրման կենտրոնի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ այլ միջոցների շահագործման փաստաթղթերում սահմանված պահանջներին համապատասխան, ինչպես նաև Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության պաշտպանության ծածկագրման (կրիպտոգրաֆիկ) միջոցների մշակման և արդիականացման սկզբունքներին համապատասխան:

42. Առանցքային տեղեկատվության պատճենումը պետք է իրականացվի հավաստագրման կենտրոնում օգտագործվող կրիպտոգրաֆիկ միջոցների շահագործման փաստաթղթերին համապատասխան։

43. ԷԹՍ-ի այն բանալիները, որոնք օգտագործվում են հավաստագրման կենտրոնի միջոցներով ստեղծվող ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստորագրման և վստահված ժամանակի ծառայության և հավաստագրերի կարգավիճակների հաստատման ծառայության հաղորդագրությունների ստորագրման համար, պետք է գեներացվեն, պահպանվեն, օգտագործվեն և ոչնչացվեն առանձին կրիպտոգրաֆիկ մոդուլներում (վստահված հաշվիչ սարքերում):

44. ԷԹՍ-ի այն բանալին, որն օգտագործվում է ԷԹՍ-ի ստուգման բանալիների ստեղծվող հավաստագրերի ստորագրման և ԷԹՍ-ի ստուգման բանալիների հավաստագրերի եզակի համարների ցանկի ստորագրման համար, որոնց գործողությունը ժամանակի որոշակի պահին դադարեցվել է հավաստագրման կենտրոնի կողմից մինչև դրանց գործողության ժամկետը լրանալը (այսուհետ՝ հետ կանչված հավաստագրերի ցանկ), չպետք է օգտագործվի այլ նպատակներով:

XI. Տեղեկատվության պահուստային պատճենմանը և հավաստագրման կենտրոնի միջոցների աշխատունակության վերականգնմանը   
ներկայացվող պահանջները

45. Հավաստագրման կենտրոնի միջոցները պետք է իրականացնեն հավաստագրման կենտրոնի միջոցներով մշակվող տեղեկատվության պահուստային պատճենման և այդպիսի տեղեկատվության ու այդպիսի միջոցների վնասման դեպքում հավաստագրման կենտրոնի ապարատային միջոցների աշխատունակության վերականգնման գործառույթներ: Պահուստային պատճենման ընթացքում պետք է բացառվի կրիպտոգրաֆիկ բանալիների պատճենման հնարավորությունը:

46. Պահուստային պատճենման ժամանակ պահպանված տվյալները պետք է բավարար լինեն հավաստագրման կենտրոնի միջոցների գործունեության՝ մինչև տվյալների պատճենման պահի դրությամբ գրանցված վիճակը վերականգնելու համար:

47. Պետք է ձեռնարկվեն պահպանված տվյալների չարտոնված փոփոխությունների հայտնաբերմանն ուղղված միջոցներ:

48. Հավաստագրման կենտրոնի միջոցների աշխատունակության վերականգնման ժամանակին ներկայացվող պահանջները պետք է սահմանված լինեն հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում, ինչպես նաև հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

49. Պահուստային պատճենման ժամանակ պահպանվող՝ պաշտպանվող տեղեկատվությունը պետք է պահպանվի միայն ծածկագրված ձևով:

XIII. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծմանը և   
չեղյալ ճանաչմանը ներկայացվող պահանջները

50. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման և չեղյալ ճանաչման արձանագրությունները պետք է նկարագրված լինեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

51. Հավաստագրման կենտրոնի կողմից ստեղծվող՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերը և հետ կանչված հավաստագրերի ցանկերը պետք է համապատասխանեն Հանձնաժողովի կողմից հաստատվող պահանջներին:

52. Հավաստագրման կենտրոնի միջոցները պետք է իրականացնեն ԷԹՍ-ի ստուգման բանալիների ստեղծվող հավաստագրերի՝ Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխանության հսկողության մեխանիզմ:

53. Հավաստագրման կենտրոնի միջոցները պետք է հետ կանչված հավաստագրերի ցանկերի և OCSP արձանագրության օգտագործմամբ իրականացնեն ԷԹՍ-ի ստուգման բանալու հավաստագրի հետկանչ՝ դրա գործողության դադարեցման կամ չեղյալ ճանաչման դեպքում: Այդպիսի հետկանչի կարգը հաստատվում է Հանձնաժողովի կողմից:

54. Հավաստագրման կենտրոնի միջոցները ԷԹՍ-ի ստուգման բանալու հավաստագրի տիրապետողի նկատմամբ պետք է իրականացնեն ԷԹՍ-ի ստուգման բանալու եզակիության ստուգում և ԷԹՍ-ի համապատասխան բանալուն տիրապետելու ստուգում:

XIV. ԷԹՍ-ի ստուգման բանալիների տրված, գործողությունը դադարած և   
չեղյալ ճանաչված հավաստագրերի ռեեստրին և դրան հասանելիություն տրամադրելուն ներկայացվող պահանջները

55. Հավաստագրման կենտրոնի միջոցներում պետք է իրականացվեն ԷԹՍ-ի ստուգման բանալիների տրված, գործողությունը դադարած և չեղյալ ճանաչված հավաստագրերի ռեեստրում (այսուհետ՝ հավաստագրերի ռեեստր) ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրված, գործողությունը դադարած և չեղյալ ճանաչված հավաստագրերը պահպանելու և ատրիբուտներով փնտրելու մեխանիզմներ, ինչպես նաև հավաստագրերի ռեեստրին ցանցային հասանելիություն տրամադրելու մեխանիզմներ:

56. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ռեեստրում կատարվող բոլոր փոփոխությունները պետք է գրանցվեն աուդիտի մատյանում:

XV. Կրիպտոգրաֆիկ միջոցներին ներկայացվող պահանջները

57. Հավաստագրման կենտրոնի միջոցները պետք է օգտագործեն ԷԹՍ-ի միջոցներ և կրիպտոգրաֆիկ այլ միջոցներ, որոնք ունեն Հանձնաժողովի գտնվելու պետության լիազորված մարմինների՝ այդ պետության օրենսդրությամբ ԿԱ դասի կրիպտոգրաֆիկ միջոցների նկատմամբ սահմանված պահանջներին համապատասխանության մասին եզրակացություն, և որոնք համապատասխանում են Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության պաշտպանության ծածկագրման (կրիպտոգրաֆիկ) միջոցների մշակման և արդիականացման սկզբունքներին:

58. ԷԹՍ-ի ստեղծման և ստուգման համար հավաստագրման կենտրոնի միջոցները պետք է օգտագործեն ԷԹՍ-ի միջոցներ, որոնք իրականացվում են կրիպտոգրաֆիկ այն մոդուլի հիման վրա, որն իր կազմում ունի ԷԹՍ-ի ստեղծման (ստուգման) արդյունքների արտացոլման միջոցներ:

XVI. Կրիպտոգրաֆիկ ստանդարտներին ներկայացվող պահանջները

59. Հավաստագրման կենտրոնի միջոցները պետք է օգտագործեն ԷԹՍ-ի այն միջոցները և կրիպտոգրաֆիկ այլ միջոցներ, որոնք իրագործում են կրիպտոգրաֆիկ այն ալգորիթմները, որոնց նույնացուցիչները նշված են Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթի թիվ 8 հավելվածում։

XVII. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգմանը ներկայացվող պահանջները

60. ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրվող հավաստագրերում ԷԹՍ-ի ստուգման՝ հավաստագրման կենտրոնի միջոցներում իրագործված մեխանիզմը պետք է նշված լինի հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում: Այդ մեխանիզմը պետք է ապահովի ԷԹՍ-ի ստուգումը ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրվող հավաստագրերում՝ ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծումից հետո և մինչև դրա տրամադրումը:

61. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականությունը ստուգելիս հավաստագրման կենտրոնի միջոցները ստուգում են ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից յուրաքանչյուր հավաստագրի վավերականությունը, այդ թվում՝ այն ԷԹՍ-ի վավերականությունը, որով ստորագրված են այդ հավաստագրերը: Տվյալ շղթան կազմված է հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական ինքնաստորագրված հավաստագրից և ԷԹՍ-ի ստուգման բանալու ստուգվող հավաստագրից:

XVIII. Լրացուցիչ պահանջներ

62. Կապի ուղիների օգտագործմամբ հավաստագրման կենտրոնի միջոցների վրա հարձակումների կազմակերպման հնարավորությունների սահմանափակման նպատակով պետք է կիրառվեն միջցանցային էկրանավորման միջոցներ, որոնք կիրառվում են կայքերը, վեբ-ծառայությունները և վեբ-հավելվածները սպասարկող սպասարկիչների կողմից: Միջցանցային էկրանավորման միջոցները պետք է ապահովեն տեղեկատվական այն հոսքերի հսկողությունն ու զտումն ըստ հիպերտեքստի փոխանցման արձանագրության, որոնք անցնում են դեպի վեբ-սպասարկիչ և վեբ-սպասարկչից։

63. Պետք է կիրառվեն համակարգչային վիրուսներից պաշտպանության միջոցներ, որոնք ապահովում են պաշտպանվող տեղեկատվության չարտոնված ոչնչացման, արգելափակման, ձևափոխման, պատճենման կամ տեղեկատվության պաշտպանության միջոցների չեզոքացման համար նախատեսված համակարգչային ծրագրերի կամ այլ համակարգչային տեղեկատվության հայտնաբերումը, ինչպես նաև պետք է ապահովվի այդպիսի ծրագրերի և տեղեկատվության հայտնաբերման առնչությամբ արձագանքումը։

64. Պետք է կիրառվեն համակարգչային հարձակումներից պաշտպանության միջոցներ, որոնք ապահովում են այնպիսի գործողությունների հայտնաբերումը, որոնք ուղղված են տեղեկատվության չարտոնված հասանելիություն ստանալուն, հավաստագրման կենտրոնի միջոցների վրա հատուկ ներգործություններ թողնելուն՝ պաշտպանվող տեղեկատվության ստացման, ոչնչացման, խեղաթյուրման և (կամ) դրա հասանելիության արգելափակման նպատակով, ինչպես նաև պետք է ապահովվի այդպիսի գործողությունների առնչությամբ արձագանքումը (այդպիսի գործողությունների կանխումը)։

65. Միջցանցային էկրանավորման միջոցները, համակարգչային վիրուսներից պաշտպանության միջոցները և համակարգչային հարձակումներից պաշտպանության միջոցները պետք է համապատասխանեն անդամ պետությունների լիազորված մարմինների կողմից սահմանվող պահանջներին:

66. Հավաստագրման կենտրոնի միջոցների ուսումնասիրությունները սույն պահանջներին դրանց համապատասխանությունը հաստատելու նպատակով պետք է իրականացվեն անդամ պետությունների լիազորված մարմինների կողմից սահմանվող՝ հավաստագրման կենտրոնի միջոցներում իրագործվող՝ տեղեկատվության պաշտպանության մեխանիզմների պարամետրերի և բնութագրերի թվային արժեքների օգտագործմամբ:

67. Հավաստագրման կենտրոնի միջոցները պետք է շահագործվեն դրանց շահագործման փաստաթղթերին համապատասխան: Հավաստագրման կենտրոնի միջոցների անվտանգ գործունեությունն ապահովելու համար անհրաժեշտ կազմակերպատեխնիկական միջոցառումները պետք է նշվեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

ՀԱՎԵԼՎԱԾ ԹԻՎ 3

Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների

**ՊԱՀԱՆՋՆԵՐ**

Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգի՝ Եվրասիական տնտեսական հանձնաժողովի ինտեգրացիոն հատվածի վստահված երրորդ կողմի միջոցներին և դրանց կազմում էլեկտրոնային թվային ստորագրության (էլեկտրոնային ստորագրության)   
միջոցին ներկայացվող

I. Ընդհանուր դրույթներ

1. Սույն պահանջներով սահմանվում են Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգի՝ Եվրասիական տնտեսական հանձնաժողովի ինտեգրացիոն հատվածի վստահված երրորդ կողմի միջոցներին (այսուհետ համապատասխանաբար՝ Միություն, ինտեգրացված համակարգ, Հանձնաժողով, ինտեգրացիոն հատված, վստահված երրորդ կողմի միջոցներ), ինչպես նաև դրանց կազմում էլեկտրոնային թվային ստորագրության (էլեկտրոնային ստորագրության) (այսուհետ՝ ԷԹՍ) միջոցին ներկայացվող պահանջները:

II. Վստահված երրորդ կողմի միջոցներին ներկայացվող պահանջները

1. Վստահված երրորդ կողմի միջոցների բաղադրիչների կազմին և գործառույթներին ներկայացվող պահանջները

2. Վստահված երրորդ կողմի միջոցների կազմի մեջ պետք է ընդգրկվեն հետևյալ բաղադրիչները՝

ա) ԷԹՍ-ի ստուգման բաղադրիչ.

բ) ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգման բաղադրիչ.

գ) ԷԹՍ-ի ստուգման բանալու հավաստագրի՝ սահմանված պահանջներին համապատասխանության ստուգման բաղադրիչ.

դ) այն ուղարկողի լիազորությունների ստուգման բաղադրիչ, որը ձևավորել և ստորագրել է էլեկտրոնային փաստաթուղթը Հանձնաժողովի ինտեգրացիոն հատվածում.

ե) ԷԹՍ-ի ստուգման արդյունքով անդորրագրերի ձևավորման և Հանձնաժողովի ինտեգրացիոն հատվածի կազմում գործող վստահված երրորդ կողմի (այսուհետ՝ Հանձնաժողովի վստահված երրորդ կողմ) համապատասխան ԷԹՍ-ներով դրանց ստորագրման բաղադրիչ.

զ) Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթերի համար ժամանակի գրանցման բաղադրիչ.

է) վստահված երրորդ կողմի միջոցներով կատարվող գործառնությունների փաստաթղթավորման բաղադրիչ.

ը) Միության իրավունքով նախատեսված հարցումներով Հանձնաժողովի վստահված երրորդ կողմի կողմից կատարվող գործառնությունների մասին տեղեկատվության տրամադրման բաղադրիչ:

3. ԷԹՍ-ի ստուգման բաղադրիչը պետք է իրականացնի՝

ա) էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգում այն ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագրի կիրառմամբ, որը ձևավորել և ստորագրել է այդ էլեկտրոնային փաստաթուղթը Հանձնաժողովի ինտեգրացիոն հատվածում կամ Հանձնաժողովի տեղեկատվական համակարգում.

բ) Միության անդամ պետության այն վստահված երրորդ կողմի անդորրագրի ԷԹՍ-ի ստուգում, որը գործում է Միության ինտեգրացված տեղեկատվական համակարգի ազգային հատվածի կազմում (այսուհետ համապատասխանաբար՝ անդամ պետության վստահված երրորդ կողմ, անդամ պետություն), որով ստորագրվել է Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքը.

գ) անդամ պետության վստահված երրորդ կողմի անդորրագրի ժամանակի դրոշմի այն ԷԹՍ-ի ստուգում, որով ստորագրվել է Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքը.

դ) հետևյալի ԷԹՍ-ի ստուգում՝

ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագիր.

Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որով ստորագրվել է ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագիրը.

Հանձնաժողովի վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու հավաստագիր, որը տրվել է Միության ինտեգրացված համակարգի՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից (այսուհետ՝ վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոն).

վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որով ստորագրվել է Հանձնաժողովի վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու հավաստագիրը.

վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է ժամանակի դրոշմի այն ԷԹՍ-ն, որը ձևավորվել է այն անդորրագրերի համար, որոնք օգտագործվում են Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի փոխգործակցության ժամանակ:

4. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգման բաղադրիչը պետք է իրականացնի՝

ա) էլեկտրոնային փաստաթուղթն ուղարկողի կողմից ստորագրելու պահին նրա ԷԹՍ-ի ստուգման բանալու հավաստագրի և Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական այն հավաստագրի վավերականության ստուգում, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որով ստորագրվել է ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագիրը.

բ) հետևյալի վավերականության ստուգում՝

վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից տրված՝ անդամ պետության վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու հավաստագիր՝ Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքով անդորրագիրը նրա կողմից ստորագրելու պահին.

վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի հիմնական հավաստագիր՝ անդամ պետության վստահված երրորդ կողմի հավաստագիրը ստորագրելու պահին.

գ) ԷԹՍ-ի ստուգման բանալիների այն հավաստագրերի վավերականության ստուգում, որոնց համապատասխան ԷԹՍ-ի բանալիների վրա հիմնած են այն ԷԹՍ-ները, որոնք օգտագործվում են Հանձնաժողովի վստահված երրորդ կողմի միջոցների կողմից՝ հետևյալը ստորագրելու համար՝

ելից էլեկտրոնային փաստաթղթերի ԷԹՍ-ների ստուգումների արդյունքներ.

մտից էլեկտրոնային փաստաթղթերի ստորագրման պահին դրանց ԷԹՍ-ների ստուգումների արդյունքներով անդորրագրերի ԷԹՍ-ների ստուգումների արդյունքներ.

դ) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու այն հավաստագրի վավերականության ստուգում, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն անդորրագրերի համար նախատեսված ժամանակի դրոշմի ԷԹՍ-ն, որոնք օգտագործվում են Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի փոխգործակցության ժամանակ:

5. ԷԹՍ-ի ստուգման բանալու հավաստագրի՝ սահմանված պահանջներին համապատասխանության ստուգման բաղադրիչը պետք է իրականացնի հետևյալի՝ Միության իրավունքի այն պահանջներին համապատասխանության ստուգում, որոնք ներկայացվում են ԷԹՍ-ի ստուգման բանալիների հավաստագրերին, ներառյալ՝ դրանց ձևին, բովանդակությանը, հավաստագրման կենտրոնի այն միջոցներին ներկայացվող պահանջները, որոնց օգտագործմամբ դրանք ստեղծվել են, և ԷԹՍ-ի այն միջոցներին ներկայացվող պահանջները, որոնց օգտագործմամբ դրանք ստորագրվել են՝

ա) ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագիր.

բ) Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որով ստորագրվել է ուղարկողի ԷԹՍ-ի ստուգման բանալու հավաստագիրը.

գ) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որով ստորագրվել է անդամ պետության վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու հավաստագիրը.

դ) ԷԹՍ-ի ստուգման բանալու հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որն օգտագործվում է Հանձնաժողովի վստահված երրորդ կողմի միջոցների կողմից՝ մտից էլեկտրոնային փաստաթղթերի ԷԹՍ-ների ստուգումների արդյունքներով անդորրագրերի ԷԹՍ-ների ստուգումների արդյունքները ստորագրելու համար.

ե) ԷԹՍ-ի ստուգման բանալու հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է այն ԷԹՍ-ն, որն օգտագործվում է Հանձնաժողովի վստահված երրորդ կողմի միջոցների կողմից՝ ելից էլեկտրոնային փաստաթղթերի ԷԹՍ-ների ստուգումների արդյունքները ստորագրելու համար.

զ) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից տրված՝ ինտեգրացված համակարգի՝ անդամ պետության վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու հավաստագիր, որի համապատասխան ԷԹՍ-ի բանալու վրա հիմնված է մտից էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքով անդորրագրի ԷԹՍ-ն.

է) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հավաստագիր, որի համապատասխան բանալու վրա հիմնված է այն անդորրագրերի համար նախատեսված ժամանակի դրոշմի ԷԹՍ-ն, որոնք օգտագործվում են Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի փոխգործակցության ժամանակ:

6. Այն ուղարկողի լիազորությունների ստուգման բաղադրիչը, որը ձևավորել և ստորագրել է էլեկտրոնային փաստաթուղթը, պետք է իրականացնի էլեկտրոնային փաստաթուղթն ուղարկողի՝ ԷԹՍ-ի ստուգման բանալու հավաստագրի տիրապետող հանդիսացող և Միության իրավունքի պահանջներին համապատասխան Հանձնաժողովի կոլեգիայի անդամի անունից հանդես եկող՝ Հանձնաժողովի պաշտոնատար անձի կամ աշխատակցի լիազորությունների ստուգում:

7. ԷԹՍ-ի ստուգման արդյունքներով անդորրագրերի ձևավորման և Հանձնաժողովի վստահված երրորդ կողմի համապատասխան ԷԹՍ-ներով դրանց ստորագրման բաղադրիչը պետք է իրականացնի՝

ա) վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից Հանձնաժողովի վստահված երրորդ կողմին տրված՝ ԷԹՍ-ի ստուգման բանալու հավաստագրին համապատասխանող ԷԹՍ-ի բանալու վրա հիմնված ԷԹՍ-ի, ինչպես նաև ելից էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքով անդորրագրի ձևավորում և ստորագրում.

բ) Հանձնաժողովի հավաստագրման կենտրոնի կողմից Հանձնաժողովի վստահված երրորդ կողմին տրված՝ ԷԹՍ-ի ստուգման բանալու հավաստագրին համապատասխանող ԷԹՍ-ի բանալու վրա հիմնված ԷԹՍ-ի, ինչպես նաև մտից էլեկտրոնային փաստաթղթի ստուգման արդյունքով անդամ պետության վստահված երրորդ կողմի անդորրագրի ԷԹՍ-ի ստուգման արդյունքով անդորրագրի ձևավորում և ստորագրում:

8. Հանձնաժողովի ինտեգրացիոն հատվածի մեջ մտնող էլեկտրոնային փաստաթղթերի համար ժամանակի գրանցման բաղադրիչը պետք է Հանձնաժողովի հավաստագրման կենտրոն ուղարկի հարցում՝ մտից էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքով անդամ պետության վստահված երրորդ կողմի անդորրագրի ԷԹՍ-ի ստուգման արդյունքով ձևավորված և ստորագրված անդորրագրի համար ժամանակի դրոշմ դնելու մասին՝ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթի 28-րդ կետին համապատասխան: Ընդ որում, ժամանակի դրոշմերի նշումը ելից էլեկտրոնային փաստաթղթի ԷԹՍ-ի ստուգման արդյունքով անդորրագրի վրա իրականացվում է վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի կողմից:

9. Հանձնաժողովի վստահված երրորդ կողմի միջոցներով կատարվող գործառնությունների փաստաթղթավորման բաղադրիչը պետք է նախատեսի տվյալ վստահված երրորդ կողմի կողմից կատարված գործառնություններին համապատասխանող էլեկտրոնային փաստաթղթերի պահպանում՝ սահմանված ժամանակի ընթացքում: Նշված էլեկտրոնային փաստաթղթերը պետք է ստորագրված լինեն Հանձնաժողովի հավաստագրման կենտրոնի կողմից Հանձնաժողովի վստահված երրորդ կողմին տրված՝ այդ նպատակի համար հատուկ նախատեսված ԷԹՍ-ի ստուգման բանալու հավաստագրին համապատասխանող ԷԹՍ-ի բանալու վրա հիմնված ԷԹՍ-ով: Նշված ԷԹՍ-ի ստուգման բանալիների գործողության ժամկետը լրանալուց հետո պետք է նախատեսվեն ԷԹՍ-ի նոր բանալիների օգտագործմամբ այդ էլեկտրոնային փաստաթղթերի ստորագրման ընթացակարգ, ինչպես նաև այդ էլեկտրոնային փաստաթղթերի ստորագրումն իրականացնելու լիազորություն ունեցող անձանց լիազորությունների հաջորդականություն:

10. Միության իրավունքով նախատեսված հարցումներով Հանձնաժողովի վստահված երրորդ կողմի գործառնությունների մասին տեղեկատվության տրամադրման բաղադրիչը պետք է իրականացնի տեղեկատվության տրամադրում՝ Միության իրավունքով սահմանված պահանջներին համապատասխան:

2. Վստահված երրորդ կողմի միջոցների ծրագրային ապահովմանը   
ներկայացվող պահանջները

11. Վստահված երրորդ կողմի միջոցների ծրագրային ապահովումը չպետք է պարունակի այնպիսի միջոցներ, որոնք թույլ են տալիս ձևափոխել կամ խեղաթյուրել ծրագրային ապահովման աշխատանքի ալգորիթմները։

12. Ծրագրային ապահովումը պետք է օգտագործի օպերացիոն համակարգի միայն փաստաթղթավորված գործառույթները։

13. Վստահված երրորդ կողմի միջոցների կողմից օգտագործվող համակարգային ծրագրային ապահովումը չպետք է ունենա հայտնի խոցելի տեղեր։

14. Ծրագրային ապահովումը պետք է ապահովի համակարգային ադմինիստրատորի, օպերատորի և օգտագործողների՝ վստահված երրորդ կողմի միջոցներով մշակվող տեղեկատվությանը հասանելիության սահմանազատումը՝ համակարգային ադմինիստրատորի կողմից տրված՝ հասանելիության սահմանազատման կանոնների հիման վրա։

15. Հանձնաժողովի վստահված երրորդ կողմի ԷԹՍ-ի բանալիների ստեղծման, պահպանման, կիրառման և ոչնչացման համար օգտագործվող և BIOS ծրագրային ծածկագրի վերլուծության հետ համատեղ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2016 թվականի հունիսի 2-ի թիվ 49 որոշմանը (ԾՕՀ) համապատասխան ստեղծվող կրիպտոգրաֆիկ մոդուլի (վստահված հաշվիչ սարքի) համակարգային և կիրառական ծրագրային ապահովման ելակետային տեքստերը պետք է անցնեն ֆորմալ վերիֆիկացում՝ դրանցում չհայտարարագրված հնարավորությունների բացակայության մասով, ինչպես նաև դրանցում՝ Հանձնաժողովի գտնվելու պետությունում սահմանված կարգով տեղեկատվության պաշտպանության մեթոդների և եղանակների իրագործման ֆորմալ վերիֆիկացում:

16. Ծրագրային ապահովումը պետք է իր կազմում պարունակի մեխանիզմ, որն ապահովում է պաշտպանվող տեղեկատվության պահպանման համար օգտագործվող՝ օպերատիվ և արտաքին հիշողության մաքրումը, որի ցանկը սահմանվում է վստահված երրորդ կողմի միջոցների ստեղծման (արդիականացման) տեխնիկական առաջադրանքով, հիշողությունում քողարկող տեղեկատվության (պայմանանշանների պատահական կամ կեղծ-պատահական հաջորդականության) գրանցման միջոցով հիշողության ազատման (վերաբաշխման) ժամանակ։

17. Ծրագրային ապահովումը պետք է իր կազմում պարունակի բաղադրիչներ, որոնք ապահովում են սահմանափակ հասանելիության տեղեկատվության շտապ ջնջում՝ սահմանափակ հասանելիության տեղեկատվության ցանկին և վստահված երրորդ կողմի միջոցների ստեղծման (արդիականացման) տեխնիկական առաջադրանքով սահմանվող՝ իրագործման ու ջնջման հուսալիության պահանջներին համապատասխան։

18. Ծրագրային ապահովումը պետք է իր կազմում պարունակի մեխանիզմ, որն ապահովում է արտաքին ցանցերից համակարգչային հարձակումների նկատմամբ կայունություն:

19. Համակարգային և կիրառական ծրագրային ապահովման ելակետային տեքստերը պետք է ենթարկվեն ստուգման դրանցում տեղեկատվության պաշտպանության այն մեթոդների և եղանակների իրագործման մասով, որոնք դիմակայում են այն հարձակումներին, որոնք իրականացվում են ընդհանուր օգտագործման ցանցերից խախտողի կողմից, որը որակավորված խմբային խախտող է, որն օգտագործում է խոցելի տեղերի որոնման նպատակով համակարգային ծրագրային ապահովումը վերլուծող գիտական կենտրոնների հնարավորությունները։

20. Վստահված երրորդ կողմի միջոցների ինժեներական-կրիպտոգրաֆիկ պաշտպանությունը պետք է բացառի այնպիսի իրադարձություններ, որոնք հանգեցնում են վստահված երրորդ կողմի ապարատային միջոցների կամ հաշվողական տեխնիկայի այն միջոցի ապարատային բաղադրիչի հնարավոր անսարքությունների կամ խափանումների պայմաններում հաջող հարձակումների անցկացման հնարավորությանը, որի վրա իրագործված են վստահված երրորդ կողմի միջոցները:

3. Վստահված երրորդ կողմի միջոցների ապարատային միջոցներին   
ներկայացվող պահանջները

21. Վստահված երրորդ կողմի միջոցների նպատակային գործառույթների իրագործումը, ներառյալ՝ BIOS ելակետային ծածկագիրը պետք է հաստատվեն Հանձնաժողովի կողմից հաստատվող՝ ապարատային միջոցների համար փորձարկումների համակարգի հիման վրա ստուգմամբ։

22. Պետք է անցկացվի վստահված երրորդ կողմի միջոցների ապարատային միջոցների գործունեության հուսալիության պարամետրերի գնահատում։

23. Վստահված երրորդ կողմի միջոցների ապարատային միջոցների կազմում տեղեկատվությունը գաղտնի կերպով ստանալու համար նախատեսված սարքերի բացակայությունը, ինչպես նաև կողմնակի էլեկտրամագնիսական ճառագայթումների և մակածումների ուղիներով տեղեկատվության արտահոսքից պաշտպանության մակարդակը պետք է հաստատված լինեն Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխանության ստուգմամբ։

4. Վստահված երրորդ կողմի միջոցների ամբողջականության ապահովմանը ներկայացվող պահանջները

24. Վստահված երրորդ կողմի միջոցներում պետք է իրագործվի տեղեկատվության, ծրագրային միջոցների և ապարատային միջոցների՝ մինչև օպերացիոն համակարգի ներբեռնումը պատահական կամ կանխամտածված խեղաթյուրման հսկողության մեխանիզմ։

5. Հասանելիության կառավարմանը ներկայացվող պահանջները

25. Վստահված երրորդ կողմի միջոցներում պետք է իրագործվեն հասանելիության սահմանազատման մեխանիզմներ, որոնք ապահովում են հետևյալ պարտադիր դերերը՝

ա) համակարգային ադմինիստրատոր, որի լիազորությունները ներառում են վստահված երրորդ կողմի միջոցների տեղադրումը, փոխդասավորության և աշխատանքի ապահովումը, վստահված երրորդ կողմի միջոցների ադմինիստրատորների խմբի անդամների պրոֆիլների ստեղծումը և պահպանումը, աուդիտի մատյանի պրոֆիլի և պարամետրերի փոխդասավորության ապահովումը (բացառությամբ աուդիտի մատյանում փոփոխություններ կատարելու հնարավորության).

բ) ադմինիստրատոր, որի լիազորությունները ներառում են էլեկտրոնային փաստաթղթերի ԷԹՍ-ի ստուգման արդյունքներով անդորրագրերի ստորագրման համար օգտագործվող՝ ԷԹՍ-ի ստեղծման և ստուգման կառավարումը.

գ) տեղեկատվական անվտանգության ադմինիստրատոր, որի լիազորությունները ներառում են տեղեկատվության պաշտպանության միջոցների հսկողություն և դրանց գործունեության ապահովում, վստահված երրորդ կողմի միջոցների պաշտպանվածության վիճակի վերլուծություն և մոնիթորինգ, պաշտպանության կազմակերպչական միջոցառումների իրականացում և դրանց իրականացման նկատմամբ հսկողություն.

դ) աուդիտի ադմինիստրատոր, որի լիազորությունները ներառում են աուդիտի մատյանի ստուգում և վարում.

ե) օպերատոր, որի լիազորությունները ներառում են վստահված երրորդ կողմի միջոցներում պահվող տեղեկատվության պահուստային պատճենում և վերականգնում:

26. Վստահված երրորդ կողմի միջոցները պետք է ապահովեն հասանելիության կառավարման կամավոր և պարտադիր սկզբունքների իրագործումը, ինչպես նաև փակ աշխատանքային միջավայրի ստեղծումը (ծրագրային միջավայր, որը թույլ է տալիս դրանում ունենալ ծրագրերի և գործընթացների միայն ֆիքսված լրակազմ)։

27. Վստահված երրորդ կողմի միջոցներում պետք է իրագործվի մեխանիզմ, որը բացառում է տարբեր դերերի լիազորությունների օգտագործման նպատակով հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբից 1 անդամի ավտորիզացման հնարավորությունը:

6. Նույնականացմանը և իսկորոշմանը ներկայացվող պահանջները

28. Վստահված երրորդ կողմի միջոցները պետք է ճանաչեն օգտագործողին, այդպիսի միջոցների կամ գործընթացի ադմինիստրատորների խմբի անդամին (այսուհետ՝ հասանելիության սուբյեկտներ), ինչպես նաև կատարեն դրանց իսկության ստուգումը։

29. Իսկորոշման մեխանիզմը պետք է իսկորոշման բացասական արդյունքի դեպքում արգելափակի հասանելիության սուբյեկտների համար վստահված երրորդ կողմի միջոցների գործառույթների հասանելիությունը։

30. Իսկորոշման ցանկացած իրականացված ընթացակարգի համար պետք է կիրառվի հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի քանակի սահմանափակման մեխանիզմ, որոնց թիվը չպետք է գերազանցի 3-ը։

31. Հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի թիվը նախատեսված սահմանային արժեքի նկատմամբ գերազանցելու դեպքում հասանելիության այդ սուբյեկտի համար վստահված երրորդ կողմի միջոցների հասանելիությունը պետք է արգելափակվի՝ վստահված երրորդ կողմի միջոցների ստեղծման (արդիականացման) տեխնիկական առաջադրանքով սահմանված ժամանակահատվածով։

32. Վստահված երրորդ կողմի միջոցներին հասանելիություն ունեցող բոլոր անձանց համար պետք է անցկացվի երկգործոն իսկորոշում։

33. Վստահված երրորդ կողմի միջոցների բոլոր օգտագործողների համար թույլատրվում է կիրառել հեռավար իսկորոշման մեխանիզմներ՝ իսկորոշման բանալիների ստուգման հավաստագրերի օգտագործմամբ՝ վստահված երրորդ կողմի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ միջոցներին ներկայացվող՝ Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխան մշակված կրիպտոգրաֆիկ միջոցների հիման վրա։

34. Վստահված երրորդ կողմի միջոցների լոկալ հասանելիություն ստանալիս վստահված երրորդ կողմի միջոցների ադմինիստրատորների խմբի անդամների իսկորոշումը պետք է կատարվի նախքան այդ միջոցների՝ աշխատանքային վիճակի անցնելը (օրինակ՝ մինչև օպերացիոն համակարգի ներբեռնումը)։

35. Լոկալ իսկորոշման համար պայմանանշանային, պարբերաբար փոփոխվող գաղտնաբառ օգտագործելու դեպքում այն պետք է կազմված լինի առնվազն 8 պայմանանշանից (այն դեպքում, երբ այբուբենի պայմանանշանների ընդհանուր թիվը կազմում է առնվազն 36): Գաղտնաբառի փոփոխման ժամանակահատվածը չպետք է գերազանցի 3 ամիսը։

7. Վստահված երրորդ կողմի միջոցներ մուտքագրվող և դրանցից դուրս բերվող տվյալների պաշտպանությանը ներկայացվող պահանջները

36. Վստահված երրորդ կողմի միջոցները պետք է ապահովեն պաշտպանվող այն տեղեկատվությունը պարունակող տվյալների փոխանցումը, որի ցանկը սահմանվում է վստահված երրորդ կողմի միջոցների ստեղծման (արդիականացման) տեխնիկական առաջադրանքով՝ չարտոնված հասանելիությունից պաշտպանված եղանակով։

37. Վստահված երրորդ կողմի միջոցները պետք է պարունակեն ֆիզիկապես առանձնացված բաղադրիչների միջև տվյալների փոխանցման դեպքում դրանց պաշտպանության մեխանիզմներ, որոնք օգտագործում են կրիպտոգրաֆիկ այնպիսի միջոցներ, որոնք համապատասխանում են Հանձնաժողովի կողմից հաստատվող՝ վստահված երրորդ կողմի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ միջոցներին ներկայացվող պահանջներին։

38. Վստահված երրորդ կողմի միջոցները պետք է ընդունեն բոլոր մուտքային հաղորդագրություններն այն պայմանով, որ դրանք ստորագրված են ԷԹՍ-ով, և ԷԹՍ-ի ստուգման արդյունքը դրական է։

8. Իրադարձությունների գրանցմանը ներկայացվող պահանջները

39. Վստահված երրորդ կողմի միջոցների օպերացիոն համակարգը պետք է ապահովի համակարգային իրադարձությունների և վստահված երրորդ կողմի միջոցների կողմից իրենց գործառույթների կատարման հետ կապված իրադարձությունների աուդիտի պաշտպանված մատյանի վարումը։

40. Վստահված երրորդ կողմի միջոցների օպերացիոն համակարգը պետք է գրանցի իրադարձությունները գրանցման ենթակա իրադարձությունների ցանկին և օպերացիոն համակարգին ներկայացվող այն պահանջներին համապատասխան, որոնք սահմանվում ու հիմնավորվում են վստահված երրորդ կողմի միջոցների ստեղծման (արդիականացման) տեխնիկական առաջադրանքում։

41. Աուդիտի մատյանը պետք է հասանելի լինի միայն աուդիտի ադմինիստրատորին, որը կարող է կատարել միայն դրա դիտում, պատճենում և ամբողջական մաքրում։

42. Աուդիտի մատյանի ամբողջական մաքրումը պետք է կատարվի միայն մաքրման ենթակա ամբողջ տեղեկատվությունը պատճենելուց հետո։ Աուդիտի մատյանի մաքրումից հետո աուդիտի այդ մատյանում առաջին գրառմամբ պետք է ավտոմատ գրանցվի մաքրման փաստը՝ այդ մաքրման ամսաթվի, ժամի և այն կատարած անձի մասին տեղեկատվության նշմամբ։

9. Վստահված երրորդ կողմի միջոցի հուսալիությանը և դրա գործունեության կայունությանը ներկայացվող պահանջները

43. Ապարատային միջոցների այնպիսի խափանումների և անսարքությունների առաջացման հավանականությունը, որոնք հանգեցնում են վստահված երրորդ կողմի միջոցների կողմից իրենց գործառույթները չկատարելուն, մեկ օրվա ընթացքում չպետք է գերազանցի նույնանման հավանականությունը՝ վստահված երրորդ կողմի միջոցների կազմում օգտագործվող կրիպտոգրաֆիկ միջոցների համար։

44. Վստահված երրորդ կողմի միջոցների (համալիր) հրաժարման միջին աշխատատևությունը կազմում է առնվազն 20 000 ժամ։

45. Պետք է իրականացվի վստահված երրորդ կողմի միջոցների գործունեության կայունության փորձարկում։

46. Խափանումներից և վթարներից հետո վստահված երրորդ կողմի միջոցների վերականգնման ժամանակը չպետք է գերազանցի 4 ժամը։

47. Վստահված երրորդ կողմի միջոցների հուսալիության և դրանց գործունեության կայունության բարձրացման միջոցառումներն ու միջոցները պետք է պարունակեն վստահված երրորդ կողմի միջոցների ռեսուրսների քվոտավորման մեխանիզմներ։

10. Առանցքային տեղեկատվության ստեղծմանը, օգտագործմանը,   
պահպանմանը և ոչնչացմանը ներկայացվող պահանջները

48. Առանցքային տեղեկատվության ստեղծման, օգտագործման, պահպանման և ոչնչացման կարգը, այդ թվում՝ դրա գործողության ժամկետները պետք է համապատասխանեն ԷԹՍ-ի միջոցների և վստահված երրորդ կողմի միջոցների կողմից օգտագործվող այլ կրիպտոգրաֆիկ միջոցների շահագործման փաստաթղթերի պահանջներին, ինչպես նաև Հանձնաժողովի կողմից հաստատվող՝ վստահված երրորդ կողմի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ միջոցներին ներկայացվող պահանջներին։

49. Առանցքային փաստաթղթերի պատճենումը պետք է իրականացվի միայն վստահված երրորդ կողմի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ միջոցների շահագործման փաստաթղթերին համապատասխան։

50. Առանցքային փաստաթղթերի տեղեկատվության պատճենումը մասնագիտացված առանցքային կրիչներ չհանդիսացող կրիչների վրա պետք է իրականացվի միայն դրա նախնական ծածկագրման ընթացակարգն անցկացնելուց հետո, որն իրականացվում է օգտագործվող կրիպտոգրաֆիկ միջոցի ներկառուցված գործառույթի միջոցով։

51. Հանձնաժողովի վստահված երրորդ կողմի կազմած անդորրագրերը ԷԹՍ-ով ստորագրելու համար օգտագործվող ԷԹՍ-ի բանալին պետք է գեներացվի, պահպանվի, օգտագործվի և ոչնչացվի կրիպտոգրաֆիկ մոդուլում (վստահված հաշվիչ սարքում), որը ստեղծվում է Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2016 թվականի հունիսի 2-ի թիվ 49 (ԾՕՀ) որոշմանը համապատասխան։

11. Տեղեկատվության պահուստային պատճենմանը   
ներկայացվող պահանջները

52. Վստահված երրորդ կողմի միջոցները պետք է իրականացնեն տվյալների պահուստային պատճենման և վերականգնման գործառույթներ։

53. Վստահված երրորդ կողմի միջոցների շահագործման կարգով պետք է նախատեսված լինեն պահպանված տվյալների չարտոնված փոփոխությունների հայտնաբերման միջոցառումներ։

12. ԷԹՍ-ի ստուգման բանալու հավաստագրի վերլուծությանը (ուսումնասիրությանը) ներկայացվող պահանջները

54. Վստահված երրորդ կողմի միջոցները պետք է աշխատեն միայն ԷԹՍ-ի ստուգման բանալու այն հավաստագրերի հետ միասին, որոնք համապատասխանում են Հանձնաժողովի կողմից հաստատվող պահանջներին։

55. Վստահված երրորդ կողմի միջոցներում պետք է իրագործվի Հանձնաժողովի կողմից սահմանված պահանջներին ԷԹՍ-ի ստուգման բանալիների հավաստագրերի համապատասխանության հսկողության մեխանիզմ։

56. Հանձնաժողովի կողմից հաստատվող պահանջներին վստահված երրորդ կողմի միջոցների համապատասխանությունը որոշելու նպատակով դրանք պետք է ունենան մեխանիզմներ, որոնք փոխգործակցում են անդամ պետությունների և Հանձնաժողովի տեղեկատվական ռեսուրսների հետ և իրականացնում են ԷԹՍ-ի ստուգման բանալու հավաստագրի այն ընդլայնումների վերլուծություն, որոնք պարունակում են՝

ա) տեղեկություններ հավաստագրման կենտրոնի այն միջոցների կրիպտոգրաֆիկ պաշտպանվածության մակարդակի (դասի) մասին, որոնց օգտագործմամբ այն ստեղծվել է.

բ) տեղեկություններ՝ ԷԹՍ-ի ստուգման բանալու հավաստագիրը տիրապետողի ԷԹՍ-ի միջոցի կրիպտոգրաֆիկ պաշտպանվածության մակարդակի (դասի) մասին.

գ) տեղեկություններ՝ վստահության անդրսահմանային տարածքում սահմանված անվտանգության քաղաքականությանը ԷԹՍ-ի ստուգման բանալու հավաստագրի համապատասխանության մասին.

դ) ԷԹՍ-ի այն միջոցների և հավաստագրման կենտրոնի այն միջոցների անվանումները, որոնք օգտագործվել են ԷԹՍ-ի բանալու, ԷԹՍ-ի ստուգման բանալու և ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծման համար.

ե) հավաստագիրը տիրապետողի կողմից օգտագործվող ԷԹՍ-ի միջոցի անվանումը։

57. Վստահված երրորդ կողմի միջոցները պետք է իրականացնեն ԷԹՍ-ի ստուգման բանալու հավաստագրի բոլոր այն ընդլայնումների և ԷԹՍ-ի ստուգման բանալիների հավաստագրերի եզակի համարների այն ցանկերի վերլուծություն (ուսումնասիրություն), որոնց գործողությունը հավաստագրման կենտրոնի կողմից որոշակի պահի դրությամբ դադարեցվել է նախքան դրանց գործողության ժամկետը լրանալը (հետ կանչված հավաստագրերի ցուցակ)՝ առաջին անգամ ստուգման ենթարկվող՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից յուրաքանչյուր հավաստագրի համար, ինչպես նաև ԷԹՍ-ի ստուգման բանալիների հավաստագրերի նախկինում ստուգված շղթայից հավաստագրերի կրկնակի վերլուծություն (ուսումնասիրություն)՝ ԷԹՍ-ի ստուգման բանալիների կրկին թողարկված հավաստագրերի համար։

13. Կրիպտոգրաֆիկ ստանդարտներին ներկայացվող պահանջները

58. Վստահված երրորդ կողմի միջոցները պետք է օգտագործեն ԷԹՍ-ի միայն այն միջոցները և կրիպտոգրաֆիկ այլ միջոցներ, որոնք իրագործում են կրիպտոգրաֆիկ այն ալգորիթմները, որոնց նույնականացուցիչները նշված են Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթի թիվ 8 հավելվածում։

14. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգմանը ներկայացվող պահանջները

59. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականությունը ստուգելիս վստահված երրորդ կողմի միջոցները պետք է ստուգեն ԷԹՍ-ի ստուգման բանալու յուրաքանչյուր հավաստագրի վավերականությունը, ինչպես նաև յուրաքանչյուր այն ԷԹՍ-ի վավերականությունը, որով ստորագրված են այդ հավաստագրերը՝ ԷԹՍ-ի ստուգման բանալիների հավաստագրերի հետևյալ 4 շղթաներից՝

ա) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի 1-ին շղթան սկսվում է Հանձնաժողովի հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագրով և ավարտվում է ուղարկողի ԷԹՍ-ի ստուգման բանալու ստուգվող հավաստագրով.

բ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի 2-րդ շղթան սկսվում է վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագրով և ավարտվում է անդամ պետության վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու ստուգվող հավաստագրով.

գ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի 3-րդ շղթան սկսվում է վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագրով և ավարտվում է Հանձնաժողովի վստահված երրորդ կողմի ԷԹՍ-ի ստուգման բանալու ստուգվող հավաստագրով.

դ) ԷԹՍ-ի ստուգման բանալիների հավաստագրերի 4-րդ շղթան սկսվում է վստահված երրորդ կողմի ծառայության հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական հավաստագրով և ավարտվում է ԷԹՍ-ի ստուգման բանալու ստուգվող այն հավաստագրով, որի ԷԹՍ-ի համապատասխան բանալու վրա հիմնված է ժամանակի դրոշմի ԷԹՍ-ը՝ Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի փոխգործակցության ժամանակ օգտագործվող անդորրագրերի համար։

60. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից յուրաքանչյուր հավաստագիր ենթակա է վերլուծության (ուսումնասիրության)՝ սույն բաժնի 12-րդ ենթաբաժնին համապատասխան։

61. ԷԹՍ-ի ստուգման բանալու հավաստագրում ԷԹՍ-ի ստուգումը պետք է իրականացվի «Տեղեկատվական տեխնոլոգիաներ։ Բաց համակարգերի փոխկապակցվածություն։ Տեղեկատու. բաց բանալիների հավաստագրերի և ատրիբուտների կառուցվածքներ» ITU-T Х.509 միջազգային առաջարկություններին (3-րդ տարբերակ) համապատասխան և ներառի բոլոր կրիտիկական ընդլայնումների պարտադիր ստուգում՝ վստահության անդրսահմանային տարածքում սահմանված անվտանգության քաղաքականությանը համապատասխան։

15. Լրացուցիչ պահանջներ

62. Վստահված կողմի միջոցների նկատմամբ կապուղիների օգտագործմամբ հարձակումներ կազմակերպելու հնարավորությունների սահմանափակման համար պետք է կիրառվեն միջցանցային էկրանացման միջոցներ, որոնք ապահովում են հսկողությունն ու ֆիլտրումն ըստ տեղեկատվական այն հոսքերի հիպերտեքստի փոխանցման արձանագրության, որոնք անցնում են դեպի վեբ-սպասարկիչ և վեբ-սպասարկչից։

63. Պետք է կիրառվեն համակարգչային վիրուսներից պաշտպանության միջոցներ, որոնք ապահովում են պաշտպանվող տեղեկատվության չարտոնված ոչնչացման, արգելափակման, ձևափոխման, պատճենման կամ տեղեկատվության պաշտպանության միջոցների չեզոքացման համար նախատեսված համակարգչային ծրագրերի կամ այլ համակարգչային տեղեկատվության հայտնաբերումը, ինչպես նաև պետք է ապահովվի այդպիսի ծրագրերի և տեղեկատվության հայտնաբերման առնչությամբ արձագանքումը։

64. Պետք է կիրառվեն համակարգչային հարձակումներից պաշտպանության միջոցներ, որոնք ապահովում են այնպիսի գործողությունների հայտնաբերումը, որոնք ուղղված են տեղեկատվության չարտոնված հասանելիությանը, վստահված երրորդ կողմի միջոցների վրա հատուկ ներգործություններին՝ պաշտպանվող տեղեկատվության ստացման, ոչնչացման, խեղաթյուրման և (կամ) դրա հասանելիության արգելափակման նպատակով, ինչպես նաև պետք է ապահովվի այդպիսի գործողությունների առնչությամբ արձագանքումը (այդպիսի գործողությունների կանխումը)։

65. Միջցանցային էկրանացման, համակարգչային վիրուսներից պաշտպանության և համակարգչային հարձակումներից պաշտպանության կիրառվող միջոցները պետք է համապատասխանեն Հանձնաժողովի կողմից հաստատվող պահանջներին։

66. Վստահված երրորդ կողմի միջոցների՝ սույն պահանջներին համապատասխանության հաստատման նպատակով դրանց ուսումնասիրությունները պետք է անցկացվեն վստահված երրորդ կողմի միջոցներում իրագործվող պաշտպանության մեխանիզմների պարամետրերի և բնութագրերի թվային արժեքների օգտագործմամբ, որոնք սահմանվում են Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից։

III. Վստահված երրորդ կողմի միջոցների կազմում ԷԹՍ-ի միջոցին   
ներկայացվող պահանջները

1. Ընդհանուր պահանջներ

67. Վստահված երրորդ կողմի միջոցների կազմում ԷԹՍ-ի միջոցը (այսուհետ՝ ԷԹՍ-ի միջոց) պետք է օգտագործվի Հանձնաժողովի վստահված երրորդ կողմի և անդամ պետությունների վստահված երրորդ կողմերի փոխգործակցության ժամանակ։

68. ԷԹՍ-ի միջոցը պետք է ապահովի դրա գործունեության հնարավորությունը 2 ռեժիմով՝ ԷԹՍ-ի ավտոմատ ստուգման և ստեղծման ռեժիմով և ադմինիստրատորի ղեկավարությամբ ԷԹՍ-ի ստուգման և ստեղծման ռեժիմով։

69. Ադմինիստրատորի ղեկավարությամբ ԷԹՍ-ի ստուգման և ստեղծման ռեժիմով ԷԹՍ-ի միջոցը պետք է կատարի հետևյալ գործողությունները՝

ա) ԷԹՍ-ն ստեղծելիս՝

էլեկտրոնային փաստաթուղթը ստորագրող անձին ցույց տալ այն տեղեկատվության բովանդակությունը, որն այդ անձը ստորագրում է.

ստեղծել ԷԹՍ միայն էլեկտրոնային փաստաթուղթը ստորագրող անձի կողմից ԷԹՍ-ի ստեղծման գործողությունը հաստատվելուց հետո.

միանշանակ ցույց տալ, որ ԷԹՍ-ն ստեղծվել է.

բ) ԷԹՍ-ն ստուգելիս՝

ցույց տալ ԷԹՍ-ով ստորագրված էլեկտրոնային փաստաթղթի բովանդակությունը.

ցույց տալ ԷԹՍ-ով ստորագրված էլեկտրոնային փաստաթղթում փոփոխություններ կատարելու վերաբերյալ տեղեկատվությունը.

նշել այն անձին, որի ԷԹՍ-ի բանալու օգտագործմամբ ստորագրվել են էլեկտրոնային փաստաթղթերը։

2. ԷԹՍ-ի միջոցի ծրագրային ապահովմանը   
ներկայացվող պահանջները

70. ԷԹՍ-ի միջոցի ծրագրային ապահովումը չպետք է պարունակի այնպիսի միջոցներ, որոնք թույլ են տալիս ձևափոխել կամ խեղաթյուրել ծրագրային ապահովման աշխատանքի ալգորիթմները։

71. ԷԹՍ-ի միջոցի ծրագրային ապահովումը պետք է օգտագործի օպերացիոն համակարգի միայն փաստաթղթավորված գործառույթները։

72. ԷԹՍ-ի միջոցի կողմից օգտագործվող համակարգային ծրագրային ապահովումը չպետք է հայտնի խոցելի տեղեր ունենա։

73. ԷԹՍ-ի միջոցի ծրագրային ապահովման ելակետային տեքստերը պետք է համապատասխանեն չհայտարարագրված հնարավորությունների բացակայության հսկողության՝ Հանձնաժողովի կողմից սահմանվող մակարդակին։

74. ԷԹՍ-ի միջոցի ծրագրային ապահովման կազմի մեջ պետք է մտնի պաշտպանվող տեղեկատվության պահպանման համար օգտագործվող օպերատիվ և արտաքին հիշողության մաքրումն ապահովող մեխանիզմ՝ հիշողության մեջ քողարկող տեղեկատվություն (պայմանանշանների պատահական կամ պսևդո-պատահական հաջորդականություն) գրանցելու միջոցով հիշողության ազատման (վերաբաշխման) դեպքում։

75. ԷԹՍ-ի միջոցի ծրագրային ապահովման կազմի մեջ պետք է մտնեն պաշտպանվող այն տեղեկատվության շտապ ջնջումն ապահովող բաղադրիչներ, որի ցանկը և ջնջման իրականացմանը և հուսալիությանը ներկայացվող պահանջները սահմանվում են ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքով։

76. ԷԹՍ-ի միջոցի ծրագրային ապահովման ելակետային տեքստերը պետք է ստուգվեն դրանցում տեղեկատվության պաշտպանության այնպիսի մեթոդների ու եղանակների իրագործման մասով, որոնք դիմակայում են հարձակումներին, որոնք իրականացվում են ընդհանուր օգտագործման ցանցերից խախտողի կողմից, որը որակավորված խմբային խախտող է, որն օգտագործում է խոցելի տեղերի որոնման նպատակով համակարգային ծրագրային ապահովումը վերլուծող գիտական կենտրոնների հնարավորությունները։

77. ԷԹՍ-ի միջոցի ինժեներական-կրիպտոգրաֆիկ պաշտպանությունը պետք է բացառի այնպիսի իրադարձություններ, որոնք հանգեցնում են հաջող հարձակումների անցկացման հնարավորությանը՝ ԷԹՍ-ի միջոցի ապարատային միջոցների կամ հաշվիչ տեխնիկայի միջոցի ապարատային այն բաղադրիչի հնարավոր անսարքությունների կամ խափանումների պայմաններում, որի վրա իրագործվել է ԷԹՍ-ի միջոցը։

3. ԷԹՍ-ի միջոցի ապարատային միջոցներին ներկայացվող պահանջները

78. ԷԹՍ-ի միջոցի նպատակային գործառույթների իրագործումը, ներառյալ BIOS ելակետային ծածկագիրը պետք է հաստատվեն Հանձնաժողովի կողմից հաստատվող՝ ապարատային միջոցների համար փորձարկումների համակարգի հիման վրա ստուգմամբ։

79. Պետք է անցկացվի ԷԹՍ-ի միջոցի ապարատային միջոցների գործունեության հուսալիության պարամետրերի գնահատում։

80. Ապարատային միջոցների կազմում տեղեկատվությունը գաղտնի կերպով ստանալու համար նախատեսված սարքերի բացակայությունը, ինչպես նաև կողմնակի էլեկտրամագնիսական ճառագայթումների և մակածումների ուղիներով տեղեկատվության արտահոսքից պաշտպանության մակարդակը պետք է հաստատված լինեն Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանված պահանջներին համապատասխանության ստուգմամբ։

81. ԷԹՍ-ի ստեղծման և ստուգման համար ԷԹՍ-ի միջոցը պետք է օգտագործի ԷԹՍ-ի ստեղծման և ստուգման արդյունքներն արտացոլելու միջոցներ ունեցող կրիպտոգրաֆիկ մոդուլ։

4. ԷԹՍ-ի միջոցի ամբողջականության ապահովմանը ներկայացվող պահանջները

82. ԷԹՍ-ի միջոցը պետք է պարունակի տեղեկատվության, ԷԹՍ-ի միջոցի չարտոնված պատահական և (կամ) կանխամտածված խեղաթյուրման (փոփոխման, ձևափոխման) և (կամ) ոչնչացման հսկողության մեխանիզմ։

83. Ամբողջականության հսկողությունը պետք է կատարվի՝

ա) օպերացիոն համակարգի յուրաքանչյուր վերաբեռնման ժամանակ՝ նախքան դրա ներբեռնումը.

բ) ԷԹՍ-ի միջոցի գործունեության ընթացքում (ամբողջականության դինամիկ հսկողություն).

գ) շահագործման վայրերում ԷԹՍ-ի միջոցի կանոնակարգային ստուգումների ընթացքում (կանոնակարգային հսկողություն)՝ ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքով սահմանված ժամանակահատվածին համապատասխան։

84. Ամբողջականության դինամիկ հսկողությունը պետք է իրականացվի առնվազն օրը 1 անգամ:

85. Ամբողջականության կանոնակարգային հսկողության մեխանիզմը պետք է ԷԹՍ-ի միջոցի կազմի մեջ մտնի։

86. Վստահված երրորդ կողմի ծրագրային և (կամ) ապարատային միջոցների կազմում պետք է առկա լինեն ԷԹՍ-ի միջոցի ամբողջականության վերականգնման միջոցներ:

5. Հասանելիության կառավարմանը ներկայացվող պահանջները

87. Սուբյեկտների համար ԷԹՍ-ի միջոցի տարբեր բաղադրիչների և (կամ) նպատակային գործառույթների հասանելիության կառավարումը պետք է իրականացվի վստահված երրորդ կողմի այն միջոցներով, որոնց կազմում գործում է ԷԹՍ-ի տվյալ միջոցը՝ վստահված երրորդ կողմի միջոցներին ներկայացվող պահանջներին համապատասխան։

6. Նույնականացմանը և իսկորոշմանը ներկայացվող պահանջները

88. ԷԹՍ-ի միջոցը պետք է ճանաչի ԷԹՍ-ի միջոցը կամ գործընթացն օգտագործողին, ինչպես նաև կատարի դրանց իսկության ստուգում։

89. Իսկորոշման մեխանիզմը պետք է արգելափակի սուբյեկտների համար ԷԹՍ-ի միջոցի գործառույթների հասանելիությունը՝ իսկորոշման բացասական արդյունքի դեպքում։

90. ԷԹՍ-ի միջոցում իսկորոշման ցանկացած իրականացված ընթացակարգի համար պետք է կիրառվի հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի քանակի սահմանափակման մեխանիզմ, որոնց թիվը չպետք է գերազանցի 3-ը։

91. Հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի թիվը նախատեսված սահմանային արժեքի նկատմամբ գերազանցելու դեպքում հասանելիության այդ սուբյեկտի համար ԷԹՍ-ի միջոցների հասանելիությունը պետք է արգելափակվի՝ ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքով սահմանված ժամանակահատվածով։

92. ԷԹՍ-ի միջոցի հասանելիության դեպքում պետք է անցկացվի երկգործոն իսկորոշում։

93. Թույլատրվում է կիրառել հեռավար իսկորոշման մեխանիզմ՝ իսկորոշման բանալիների ստուգման հավաստագրերի օգտագործմամբ՝ վստահված երրորդ կողմի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ միջոցներին ներկայացվող՝ Հանձնաժողովի կողմից հաստատվող պահանջներին համապատասխան մշակված կրիպտոգրաֆիկ միջոցների հիման վրա։

94. ԷԹՍ-ի միջոցի լոկալ հասանելիությունն ապահովելիս ԷԹՍ-ի միջոցն օգտագործողի իսկորոշումը պետք է կատարվի նախքան ԷԹՍ-ի այդ միջոցի՝ աշխատանքային վիճակի անցնելը (օրինակ՝ նախքան այդ միջոցի կողմից օգտագործվող օպերացիոն համակարգի ներբեռնումը)։

95. Լոկալ իսկորոշման համար պայմանանշանային, պարբերաբար փոփոխվող գաղտնաբառ օգտագործելու դեպքում այն պետք է կազմված լինի առնվազն 8 պայմանանշանից (այն դեպքում, երբ այբուբենի պայմանանշանների ընդհանուր թիվը կազմում է առնվազն 36): Գաղտնաբառի փոփոխման ժամանակահատվածը չպետք է գերազանցի 3 ամիսը։

7. Իրադարձությունների գրանցմանը ներկայացվող պահանջները

96. ԷԹՍ-ի միջոցի կազմի մեջ պետք է մտնի այնպիսի միջոց, որն իրականացնում է պաշտպանված էլեկտրոնային մատյանում այն իրադարձությունների գրանցումը, որոնք կապված են ԷԹՍ-ի միջոցի կողմից իր նպատակային գործառույթների կատարման հետ։ Նշված միջոցին ներկայացվող պահանջները և գրանցվող իրադարձությունների ցանկը սահմանվում և հիմնավորվում են ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքում։

97. Իրադարձությունների գրանցման մատյանը պետք է հասանելի լինի միայն այն տեղեկատվական համակարգի օպերատորի կողմից սահմանված անձանց, որում օգտագործվում է ԷԹՍ-ի միջոցը։ Ընդ որում, իրադարձությունների գրանցման մատյանի հասանելիությունը պետք է ապահովվի միայն գրառումները դիտելու և իրադարձությունների գրանցման մատյանի պարունակությունը արխիվային կրիչների վրա տեղափոխելու համար։ ԷԹՍ-ի միջոցն օգտագործողին մատյանը պետք է հասանելի լինի միայն դիտելու համար։

8. ԷԹՍ-ի միջոցի հուսալիությանը և դրա գործունեության կայունությանը ներկայացվող պահանջները

98. Պետք է անցկացվի ԷԹՍ-ի միջոցի ապարատային միջոցների այն խափանումների և անսարքությունների հավանականության հաշվարկ, որոնք հանգեցնում են ԷԹՍ-ի միջոցի կողմից իր գործառույթները չկատարելուն։

99. ԷԹՍ-ի միջոցի ապարատային միջոցների հրաժարման միջին աշխատատևությունը կազմում է առնվազն 20 000 ժամ։

9. ԷԹՍ-ի միջոցի կազմում օգտագործվող պատահական թվերի տվիչին ներկայացվող պահանջները

100. ԷԹՍ-ի բանալիների մշակումը և ԷԹՍ-ի ստեղծումը պետք է իրականացվեն ԷԹՍ-ի միջոցի կողմից՝ պատահական թվերի ֆիզիկական տվիչի օգտագործմամբ (արտաքին պայմանների և սեփական պարամետրերի իրապես հնարավոր փոփոխությունների նկատմամբ կայուն՝ չդետերմինացվող ֆիզիկական համակարգի կողմից գեներացվող պատահական գործընթացի ազդանշանի կերպափոխման միջոցով թվերի պատահական հաջորդականություն մշակող սարք), որը ԷԹՍ-ի միջոցի բաղկացուցիչ մասն է։

101. ԷԹՍ-ի միջոցի կազմի մեջ մտնող պատահական թվերի ֆիզիկական տվիչի համար պետք է մշակվի այդ տվիչում օգտագործվող պատահական ֆիզիկական գործընթացի տեսական հավանականության մոդելը, ինչպես նաև պետք է անցկացվի պատահական թվերի ֆիզիկական տվիչի իրագործմանը նշված մոդելի համապատասխանության փորձնական ստուգում։

102. Ըստ տեսական հավանականության մոդելի պարամետրերի՝ պետք է տեսականորեն հիմնավորվի պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության որակի գնահատականը, ինչպես նաև պետք է անցկացվի ստացված գնահատականի վիճակագրական ստուգում՝ պատահական թվերի ֆիզիկական տվիչի իրագործման համար։

103. ԷԹՍ-ի միջոցի շահագործման դեպքում պետք է իրականացվի պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության վիճակագրական որակի ստուգում։ Տվյալ ստուգումը պետք է իրականացվի պատահական թվերի ֆիզիկական տվիչի կանոնակարգային ստուգումների ընթացքում (կանոնակարգային հսկողություն) և ԷԹՍ-ի միջոցի գործունեության ընթացքում ավտոմատ ռեժիմով (դինամիկ հսկողություն)։

104. Կանոնակարգային հսկողության ժամանակահատվածը, ինչպես նաև պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության վիճակագրական որակի ստուգման եղանակը կանոնակարգային և դինամիկ հսկողության ընթացքում սահմանվում և հիմնավորվում են ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքում։

10. Առանցքային տեղեկատվության ստեղծմանը, օգտագործմանը,   
պահպանմանը և ոչնչացմանը ներկայացվող պահանջները

105. Առանցքային տեղեկատվության ստեղծման, օգտագործման, պահպանման և ոչնչացման կարգը սահմանվում է ԷԹՍ-ի միջոցի շահագործման փաստաթղթերի պահանջներին համապատասխան։

106. Առանցքային փաստաթղթերի պատճենումը պետք է իրականացվի միայն ԷԹՍ-ի միջոցի շահագործման փաստաթղթերին համապատասխան։

107. Առանցքային փաստաթղթերի տեղեկատվության պատճենումը մասնագիտացված առանցքային կրիչներ չհանդիսացող կրիչների վրա պետք է իրականացվի միայն դրա նախնական ծածկագրման ընթացակարգն անցկացնելուց հետո, որն իրականացվում է օգտագործվող կրիպտոգրաֆիկ միջոցի ներկառուցված գործառույթի միջոցով։

108. ԷԹՍ-ի միջոցի առանցքային տեղեկատվության հետ գործողությունների իրականացումն ապահովող կրիպտոգրաֆիկ արձանագրությունները պետք է անմիջականորեն իրագործվեն ԷԹՍ-ի միջոցում։

109. ԷԹՍ-ի միջոցի կողմից օգտագործվող՝ ԷԹՍ-ի բանալիների ու ԷԹՍ-ի ստուգման բանալիների գործողության ժամկետները սահմանվում են ԷԹՍ-ի միջոցի շահագործման փաստաթղթերին համապատասխան, սակայն չպետք է լինեն համապատասխանաբար 3 և 7 տարուց ավելի։

110. ԷԹՍ-ի միջոցում պետք է իրագործվի ԷԹՍ-ի բանալիների գործողության ժամկետի հսկողության մեխանիզմ։

111. ԷԹՍ-ի բանալիների գործողության ժամկետի հսկողության մեխանիզմը պետք է թույլ տա սահմանել ԷԹՍ-ի բանալու գործողության ժամկետը և նախազգուշացնել ԷԹՍ-ի բանալու գործողության ժամկետի ավարտի մասին՝ ԷԹՍ-ի միջոցի ստեղծման (արդիականացման) տեխնիկական առաջադրանքով սահմանված ժամանակահատվածում՝ մինչև ԷԹՍ-ի բանալու գործողության ժամկետի ավարտը, ինչպես նաև արգելափակել ԷԹՍ-ի այն միջոցի աշխատանքը, որի ԷԹՍ-ի բանալու գործողության ժամկետն ավարտվել է։

11. Կրիպտոգրաֆիկ ստանդարտներին ներկայացվող պահանջները

112. ԷԹՍ-ի միջոցը պետք է իրագործի միայն կրիպտոգրաֆիկ այն ալգորիթմները, որոնց նույնականացուցիչները նշված են Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի սեպտեմբերի 28-ի թիվ 125 որոշմամբ հաստատված՝ «Եվրասիական տնտեսական միության անդամ պետությունների պետական իշխանության մարմինների՝ միմյանց միջև և Եվրասիական տնտեսական հանձնաժողովի հետ անդրսահմանային փոխգործակցության ժամանակ էլեկտրոնային փաստաթղթերի փոխանակման մասին» հիմնադրույթի թիվ 8 հավելվածում։

12. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգմանը ներկայացվող պահանջները

113. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգումը պետք է իրականացվի վստահված երրորդ կողմի այն միջոցներով, որոնց կազմում գործում է ԷԹՍ-ի տվյալ միջոցը՝ վստահված երրորդ կողմի միջոցներին ներկայացվող պահանջներին համապատասխան։

13. Լրացուցիչ պահանջներ

114. Սույն պահանջներին ԷԹՍ-ի միջոցի համապատասխանության հաստատման նպատակով դրա ուսումնասիրությունները պետք է անցկացվեն Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանվող՝ ԷԹՍ-ի միջոցում իրագործվող պաշտպանության մեխանիզմների պարամետրերի և բնութագրերի թվային արժեքների օգտագործմամբ։

ՀԱՎԵԼՎԱԾ ԹԻՎ 4

Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների

**ՊԱՀԱՆՋՆԵՐ**

էլեկտրոնային թվային ստորագրության միջոցներին և   
Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնի միջոցներին ներկայացվող

I. Ընդհանուր դրույթներ

1. Սույն պահանջներով սահմանվում են Եվրասիական տնտեսական միության (այսուհետ՝ Միություն) ինտեգրացված տեղեկատվական համակարգի՝ Եվրասիական տնտեսական հանձնաժողովի (այսուհետ՝ Հանձնաժողով) ինտեգրացիոն հատվածում և Հանձնաժողովի տեղեկատվական համակարգերում օգտագործվող էլեկտրոնային թվային ստորագրության (էլեկտրոնային ստորագրության) (այսուհետ՝ ԷԹՍ) միջոցներին, ինչպես նաև Հանձնաժողովի հավաստագրման կենտրոնի (այսուհետ՝ հավաստագրման կենտրոն) այն միջոցներին ներկայացվող պահանջները, որոնք նախատեսված են ԷԹՍ-ի միջոցներ օգտագործող՝ Միության ինտեգրացված տեղեկատվական համակարգի՝ Հանձնաժողովի ինտեգրացիոն հատվածի ենթահամակարգերի և Հանձնաժողովի տեղեկատվական համակարգերի գործունեությունն ապահովելու համար։

II. ԷԹՍ-ի միջոցներին ներկայացվող պահանջները

1. ԷԹՍ-ի միջոցների գործառույթներին ներկայացվող պահանջները

2. ԷԹՍ-ի ստեղծման ժամանակ ԷԹՍ-ի միջոցները պետք է կատարեն հետևյալ գործողությունները՝

ա) էլեկտրոնային փաստաթուղթը ստորագրող անձին ցույց տալ այն տեղեկատվության բովանդակությունը, որն այդ անձը ստորագրում է.

բ) ստեղծել ԷԹՍ՝ էլեկտրոնային փաստաթուղթը ստորագրող անձի կողմից ԷԹՍ-ի ստեղծման գործողությունը հաստատվելուց հետո.

գ) միանշանակ ցույց տալ, որ ԷԹՍ-ն ստեղծվել է:

3. ԷԹՍ-ի ստուգման ժամանակ ԷԹՍ-ի միջոցները պետք է կատարեն հետևյալ գործողությունները՝

ա) ցույց տալ ԷԹՍ-ով ստորագրված էլեկտրոնային փաստաթղթի բովանդակությունը.

բ) ցույց տալ ԷԹՍ-ով ստորագրված էլեկտրոնային փաստաթղթում փոփոխություններ կատարելու վերաբերյալ տեղեկատվությունը.

գ) ստուգել ԷԹՍ-ի ստուգման բանալու հավաստագիրը տիրապետողին այն ԷԹՍ պատկանելիությունը, որի օգտագործմամբ ստորագրվել է էլեկտրոնային փաստաթուղթը։

4. Սույն պահանջների 2-րդ ու 3-րդ կետերում նշված՝ ԷԹՍ-ի միջոցների գործառույթներին ներկայացվող պահանջներն իրագործվում են ապարատային և ծրագրային այն միջոցների օգտագործմամբ, որոնց հետ միասին նախատեսված ձևով գործում են ԷԹՍ-ի միջոցները, որոնք կարող են ազդել ԷԹՍ-ի միջոցներին ներկայացվող պահանջների կատարման վրա, և որոնց ամբողջությունը ԷԹՍ-ի միջոցների գործունեության միջավայրն է (այսուհետ՝ գործունեության միջավայր)։

2. ԷԹՍ-ի միջոցների ծրագրային ապահովմանը ներկայացվող պահանջները

5. ԷԹՍ-ի միջոցների ծրագրային ապահովումը չպետք է պարունակի այնպիսի միջոցներ, որոնք թույլ են տալիս ձևափոխել կամ խեղաթյուրել ԷԹՍ-ի միջոցի ծրագրային ապահովման աշխատանքի ալգորիթմները։

6. ԷԹՍ-ի միջոցների ծրագրային ապահովումը պետք է օգտագործի օպերացիոն համակարգի միայն փաստաթղթավորված գործառույթները։

7. ԷԹՍ-ի միջոցի կողմից օգտագործվող համակարգային ծրագրային ապահովումը չպետք է հայտնի խոցելի տեղեր ունենա։

8. ԷԹՍ-ի միջոցների ծրագրային ապահովման ելակետային տեքստերը պետք է ենթարկվեն ստուգման՝ չհայտարարագրված հնարավորությունների բացակայության մասով։ ԷԹՍ-ի միջոցների ծրագրային ապահովումը պետք է համապատասխանի չհայտարարագրված հնարավորությունների բացակայության հսկողության՝ Միության անդամ պետությունների (այսուհետ՝ անդամ պետություններ) լիազորված մարմինների կողմից սահմանվող մակարդակին։

9. ԷԹՍ-ի միջոցների ծրագրային ապահովման կազմի մեջ պետք է մտնի սահմանափակ հասանելիություն ունեցող տեղեկատվության պահպանման համար օգտագործվող օպերատիվ և արտաքին հիշողության մաքրումն ապահովող մեխանիզմ՝ հիշողության մեջ քողարկող տեղեկատվություն (պայմանանշանների պատահական կամ պսևդո-պատահական հաջորդականություն) գրանցելու միջոցով հիշողության ազատման (վերաբաշխման) դեպքում։

10. ԷԹՍ-ի միջոցների ծրագրային ապահովման ելակետային տեքստերը պետք է ենթարկվեն ստուգման՝ տեղեկատվության պաշտպանության և այն հարձակումներին դիմակայելու մեթոդների և եղանակների իրագործման մասով, որոնք իրականացվում են խախտողի կողմից՝ նախատեսված միջոցների օգտագործմամբ (ինչպես հսկվող գոտու սահմաններից դուրս, այնպես էլ դրա սահմաններում գտնվելու դեպքում)՝ նրա մոտ հաշվիչ տեխնիկայի այն միջոցների հասանելիության առկայության դեպքում, որոնցում իրագործվել են ԷԹՍ-ի միջոցները, ինչպես նաև ԷԹՍ-ի միջոցի և գործունեության միջավայրի ապարատային բաղադրիչներ ունենալու հնարավորության դեպքում այն ծավալով, որը կախված է չարտոնված այնպիսի գործողությունների կանխմանն ու կանխարգելմանն ուղղված միջոցառումներից, որոնք իրականացվել են տեղեկատվական այն համակարգում, որտեղ օգտագործվում է ԷԹՍ-ի միջոցը։

11. ԷԹՍ-ի միջոցների ինժեներական-կրիպտոգրաֆիկ պաշտպանությունը պետք է բացառի այնպիսի իրադարձությունների ի հայտ գալը, որոնք հանգեցնում են հաջող հարձակումների անցկացման հնարավորությանը՝ ԷԹՍ-ի միջոցի ապարատային միջոցների կամ հաշվիչ տեխնիկայի միջոցի ապարատային այն բաղադրիչի հնարավոր անսարքությունների կամ խափանումների պայմաններում, որի վրա իրագործվել է ԷԹՍ-ի ծրագրային միջոցը։

3. ԷԹՍ-ի միջոցների ապարատային միջոցներին   
ներկայացվող պահանջները

12. ԷԹՍ-ի միջոցների ապարատային միջոցներին ներկայացվում են հետևյալ պահանջները՝

ա) ԷԹՍ-ի միջոցների նպատակային գործառույթների իրականացման համապատասխանության ստուգման անցկացում՝ Հանձնաժողովի կողմից սահմանվող՝ ԷԹՍ-ի միջոցների ապարատային միջոցների փորձարկումների համակարգի օգտագործմամբ.

բ) ԷԹՍ-ի միջոցների ապարատային միջոցների գործունեության հուսալիության պարամետրերի գնահատման անցկացում.

գ) ԷԹՍ-ի միջոցների ապարատային միջոցների ուսումնասիրությունների անցկացում՝ Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանված՝ կողմնակի էլեկտրամագնիսական ճառագայթումների և մակածումների ուղիներով տեղեկատվության արտահոսքից պաշտպանությանը ներկայացվող պահանջներին համապատասխանության մասով։

4. ԷԹՍ-ի միջոցների ամբողջականությանը ներկայացվող պահանջները

13. ԷԹՍ-ի միջոցներում պետք է իրագործվի տեղեկատվության չարտոնված պատահական և (կամ) կանխամտածված խեղաթյուրման (փոփոխման, ձևափոխման) և (կամ) ոչնչացման, ինչպես նաև ԷԹՍ-ի միջոցի ձևափոխման հսկողության (այսուհետ՝ ամբողջականության հսկողություն) մեխանիզմ։

14. Ամբողջականության հսկողությունը պետք է իրականացվի օպերացիոն համակարգի յուրաքանչյուր վերաբեռնման ժամանակ՝ նախքան դրա ներբեռնումը, և ԷԹՍ-ի միջոցի գործունեության ընթացքում (ամբողջականության դինամիկ հսկողություն), ինչպես նաև շահագործման վայրերում ԷԹՍ-ի միջոցի կանոնակարգային ստուգումների ընթացքում (ամբողջականության կանոնակարգային հսկողություն)։

15. Ամբողջականության դինամիկ հսկողությունը պետք է իրականացվի առնվազն օրը 1 անգամ: Ամբողջականության կանոնակարգային հսկողության մեխանիզմը պետք է իրագործվի ԷԹՍ-ի միջոցի կազմում։ Ամբողջականության կանոնակարգային հսկողության իրականացման պարբերականությունը պետք է սահմանվի և հիմնավորվի ԷԹՍ-ի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքներում։

16. Հավաստագրման կենտրոնի ծրագրային և (կամ) ապարատային միջոցների կազմի մեջ պետք է մտնեն ԷԹՍ-ի միջոցի ամբողջականության վերականգնման միջոցներ:

5. Հասանելիության կառավարմանը ներկայացվող պահանջները

17. ԷԹՍ-ի միջոցների կամ գործունեության միջավայրի կազմի մեջ պետք է մտնեն այնպիսի բաղադրիչներ, որոնք ապահովում են հասանելիության սուբյեկտների համար ԷԹՍ-ի միջոցների տարբեր բաղադրիչների և (կամ) նպատակային գործառույթների հասանելիության կառավարումը տեղեկատվական այն համակարգերի ադմինիստրատորների կողմից սահմանված պարամետրերի հիման վրա, որոնցում օգտագործվում են ԷԹՍ-ի միջոցները, կամ ԷԹՍ-ի միջոցները մշակողների կողմից սահմանված պարամետրերի հիման վրա: Նշված բաղադրիչներին ներկայացվող պահանջները սահմանվում և հիմնավորվում են ԷԹՍ-ի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքներում:

6. Նույնականացմանը և իսկորոշմանը ներկայացվող պահանջները

18. Նույնականացումն ու իսկորոշումը ներառում են ԷԹՍ-ի միջոցները կամ գործընթացն օգտագործողի ճանաչումը, ինչպես նաև դրանց իսկության ստուգումը: Իսկորոշման բացասական արդյունքի դեպքում իսկորոշման մեխանիզմը պետք է արգելափակի հասանելիության այդ սուբյեկտների համար ԷԹՍ-ի միջոցների գործառույթների հասանելիությունը:

19. Իսկորոշման ցանկացած իրականացված ընթացակարգի համար ԷԹՍ-ի միջոցներում պետք է կիրառվի հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի քանակի սահմանափակման մեխանիզմ, որոնց թիվը չպետք է գերազանցի 3-ը:

Հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի թիվը գերազանցելու դեպքում հասանելիության այդ սուբյեկտի համար ԷԹՍ-ի միջոցների հասանելիությունը պետք է արգելափակվի ԷԹՍ-ի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքներով սահմանված ժամանակահատվածով:

20. ԷԹՍ-ի միջոցների հասանելիություն ունեցող անձանց համար պետք է անցկացվի երկգործոն իսկորոշում:

21. Թույլատրվում է կիրառել հեռավար իսկորոշման մեխանիզմներ՝ թույլատրված կրիպտոգրաֆիկ ալգորիթմների հիման վրա՝ իսկորոշման հավաստագրերի օգտագործմամբ։

22. ԷԹՍ-ի միջոցի լոկալ հասանելիությունն ապահովելիս ԷԹՍ-ի միջոցն օգտագործողի իսկորոշումը պետք է կատարվի նախքան այդ միջոցի՝ աշխատանքային վիճակի անցնելը (օրինակ՝ նախքան ԷԹՍ-ի միջոցի կողմից օգտագործվող օպերացիոն համակարգի ներբեռնումը)։

23. Լոկալ իսկորոշման համար պայմանանշանային, պարբերաբար փոփոխվող գաղտնաբառ օգտագործելու դեպքում այն պետք է կազմված լինի առնվազն 8 պայմանանշանից (այն դեպքում, երբ այբուբենի պայմանանշանների ընդհանուր թիվը կազմում է առնվազն 36): Գաղտնաբառի փոփոխման ժամանակահատվածը չպետք է գերազանցի 6 ամիսը։

7. Իրադարձությունների գրանցմանը ներկայացվող պահանջները

24. ԷԹՍ-ի միջոցների կազմի մեջ պետք է մտնի այնպիսի միջոց, որն իրականացնում է պաշտպանված էլեկտրոնային մատյանում այն իրադարձությունների գրանցումը, որոնք կապված են ԷԹՍ-ի միջոցների կողմից իրենց նպատակային գործառույթների կատարման հետ։ Նշված միջոցին ներկայացվող պահանջները և գրանցվող իրադարձությունների ցանկը սահմանվում են ԷԹՍ-ի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքներում։

25. Իրադարձությունների գրանցման էլեկտրոնային մատյանը պետք է հասանելի լինի միայն այն տեղեկատվական համակարգի օպերատորի կողմից սահմանված անձանց համար, որում օգտագործվում է ԷԹՍ-ի միջոցը։ Իրադարձությունների գրանցման էլեկտրոնային մատյանի հասանելիությունը պետք է տրամադրվի գրառումները դիտելու և դրա պարունակությունը արխիվային կրիչների վրա տեղափոխելու նպատակով։ ԷԹՍ-ի միջոցն օգտագործողի համար մատյանը պետք է հասանելի լինի միայն դիտելու համար։

8. ԷԹՍ-ի միջոցների հուսալիությանը և դրանց գործունեության կայունությանը ներկայացվող պահանջները

26. Կատարվում է ԷԹՍ-ի միջոցների ապարատային միջոցների այն խափանումների և անսարքությունների հավանականության հաշվարկ, որոնք հանգեցնում են ԷԹՍ-ի միջոցների կողմից իրենց գործառույթները չկատարելուն։

27. ԷԹՍ-ի միջոցների ապարատային միջոցների հրաժարման միջին աշխատատևությունը կազմում է առնվազն 10 000 ժամ։

9. Առանցքային տեղեկատվությանը ներկայացվող պահանջները

28. ԷԹՍ-ի բանալիների մշակումը պետք է կատարվի ԷԹՍ-ի միջոցի կողմից՝ պատահական թվերի ֆիզիկական տվիչի օգտագործմամբ (արտաքին պայմանների և սեփական պարամետրերի իրապես հնարավոր փոփոխությունների նկատմամբ կայուն՝ չդետերմինացվող ֆիզիկական համակարգի կողմից գեներացվող պատահական գործընթացի ազդանշանի կերպափոխման միջոցով թվերի պատահական հաջորդականություն մշակող սարք), որը ԷԹՍ-ի միջոցի կազմի մեջ է մտնում։

29. ԷԹՍ-ի միջոցի կազմի մեջ մտնող՝ պատահական թվերի ֆիզիկական տվիչի համար պետք է մշակվի այդ տվիչում օգտագործվող պատահական ֆիզիկական գործընթացի տեսական հավանականության մոդելը, և պետք է անցկացվի պատահական թվերի համապատասխան ֆիզիկական տվիչի իրագործմանը նշված մոդելի համապատասխանության փորձնական ստուգում։ Տեսական հավանականության մոդելի պարամետրերի հիման վրա պետք է տեսականորեն հիմնավորվի պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության որակի գնահատականը և անցկացվի այդ գնահատականի վիճակագրական ստուգում՝ պատահական թվերի ֆիզիկական տվիչի իրագործման նպատակով։

30. ԷԹՍ-ի միջոցի շահագործման դեպքում պետք է անցկացվի պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության որակի վիճակագրական ստուգում։ Տվյալ ստուգումը պետք է անցկացվի՝

ա) պատահական թվերի ֆիզիկական տվիչի կանոնակարգային ստուգումների անցկացման ընթացքում (կանոնակարգային հսկողություն).

բ) ԷԹՍ-ի միջոցի գործունեության ընթացքում՝ ավտոմատ ռեժիմով (դինամիկ հսկողություն)։

31. Կանոնակարգային հսկողության անցկացման պարբերականությունը և պատահական թվերի ֆիզիկական տվիչի ելքային հաջորդականության որակի վիճակագրական ստուգման եղանակը կանոնակարգային և դինամիկ հսկողություն իրականացնելու ընթացքում սահմանվում են ԷԹՍ-ի միջոցի մշակման (արդիականացման) տեխնիկական առաջադրանքում։

32. Առանցքային տեղեկատվության ստեղծման, օգտագործման, պահպանման և ոչնչացման կարգը սահմանվում է ԷԹՍ-ի միջոցի շահագործման փաստաթղթերով սահմանված պահանջներին համապատասխան, ինչպես նաև այն անդամ պետության օրենսդրությամբ, որի վստահված երրորդ կողմի միջոցների կազմի մեջ է մտնում ԷԹՍ-ի միջոցը։ Հանձնաժողովի վստահված երրորդ կողմի միջոցների առնչությամբ նշված կարգը կանոնակարգվում է Միության մարմինների ակտերով։

33. Առանցքային փաստաթղթերի պատճենումը պետք է իրականացվի ԷԹՍ-ի միջոցի շահագործման փաստաթղթերին համապատասխան։ Չի թույլատրվում ԷԹՍ-ի բանալիների պատճենումը մասնագիտացված առանցքային կրիչներ չհանդիսացող կրիչների (օրինակ՝ կոշտ սկավառակի) վրա՝ առանց դրանց նախնական ծածկագրման։

34. ԷԹՍ-ի միջոցի առանցքային տեղեկատվության հետ գործողությունների իրականացումն ապահովող կրիպտոգրաֆիկ արձանագրությունները պետք է իրագործվեն ԷԹՍ-ի միջոցում։

35. ԷԹՍ-ի միջոցի կողմից օգտագործվող՝ ԷԹՍ-ի բանալիների ու ԷԹՍ-ի ստուգման բանալիների գործողության ժամկետները սահմանվում են ԷԹՍ-ի միջոցի շահագործման փաստաթղթերին համապատասխան, սակայն չպետք է կազմեն համապատասխանաբար 1 տարի և 3 ամսից ու 7 տարուց ավելի։

36. ԷԹՍ-ի միջոցում պետք է իրագործվի ԷԹՍ-ի բանալու գործողության ժամկետի հսկողության մեխանիզմ։ ԷԹՍ-ի բանալու գործողության ժամկետի հսկողության մեխանիզմը պետք է թույլ տա սահմանել ԷԹՍ-ի բանալու գործողության ժամկետը և ազդանշանել դրա գործողության ժամկետի ավարտի մասին սահմանված ժամանակահատվածում՝ մինչև ԷԹՍ-ի բանալու գործողության ժամկետի ավարտը, ինչպես նաև արգելափակել ԷԹՍ-ի այն միջոցի աշխատանքը, որի ԷԹՍ-ի բանալու գործողության ժամկետն ավարտվել է։ ԷԹՍ-ի բանալու գործողության ժամկետի ավարտի մասին ազդանշանման ժամանակահատվածը սահմանվում է ԷԹՍ-ի միջոցի մշակման (արդիականացման) տեխնիկական առաջադրանքում։

10. Կրիպտոգրաֆիկ ստանդարտներին ներկայացվող պահանջները

37. ԷԹՍ-ի միջոցը պետք է իրագործի կրիպտոգրաֆիկ ալգորիթմները՝ Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի փետրվարի 3-ի թիվ 10 (ԾՕՀ) որոշմանը համապատասխան։

11. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգմանը ներկայացվող պահանջները

38. ԷԹՍ-ի միջոցն ստուգում է ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից յուրաքանչյուր հավաստագրի վավերականությունը, այդ թվում՝ այն ԷԹՍ-ների վավերականությունը, որոնցով ստորագրված են այդ հավաստագրերը: Տվյալ շղթան կազմված է հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական ինքնաստորագրված հավաստագրից և ԷԹՍ-ի ստուգման բանալու այն հավաստագրից, որը ԷԹՍ-ի միջոցի կողմից օգտագործվում է ԷԹՍ-ի ստուգման համար:

12. Լրացուցիչ պահանջներ

39. Սույն պահանջներին ԷԹՍ-ի միջոցների համապատասխանության հաստատման նպատակով դրանց ուսումնասիրությունները պետք է անցկացվեն ԷԹՍ-ի միջոցներում իրագործվող պաշտպանության մեխանիզմների պարամետրերի և բնութագրերի թվային արժեքների օգտագործմամբ, որոնք սահմանվում են Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից։

III. Հավաստագրման կենտրոնի միջոցներին ներկայացվող պահանջները

1. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովմանը ներկայացվող պահանջները

40. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովումը չպետք է պարունակի միջոցներ, որոնք թույլ են տալիս ձևափոխել կամ խեղաթյուրել հավաստագրման կենտրոնի ծրագրային և ապարատային միջոցների աշխատանքի ալգորիթմները:

41. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովումը չպետք է հայտնի խոցելի տեղեր ունենա։

42. Հավաստագրման կենտրոնի միջոցների կիրառական ծրագրային ապահովումը և հավաստագրման կենտրոնի կողմից օգտագործվող՝ տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների ծրագրային ապահովումը պետք է օգտագործեն համակարգային ծրագրային ապահովման միայն փաստաթղթավորված գործառույթներ:

43. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովումը պետք է ապահովի հավաստագրման կենտրոնի միջոցների համակարգային ադմինիստրատորի, հավաստագրման կենտրոնի միջոցների հավաստագրման ադմինիստրատորի, հավաստագրման կենտրոնի միջոցների օպերատորների և հավաստագրման կենտրոնի օգտագործողների՝ հավաստագրման կենտրոնի միջոցներով մշակվող տեղեկատվությանը հասանելիության սահմանափակումը՝ հավաստագրման կենտրոնի միջոցների համակարգային ադմինիստրատորի կողմից սահմանված՝ հասանելիության սահմանափակման կանոններին համապատասխան:

44. Հավաստագրման կենտրոնի միջոցների համակարգային և (կամ) կիրառական ծրագրային ապահովման կազմի մեջ պետք է մտնի մեխանիզմ, որն ապահովում է սահմանափակ հասանելիության տեղեկատվության պահպանման համար օգտագործվող՝ օպերատիվ և արտաքին հիշողության մաքրումը:

45. Հավաստագրման կենտրոնի միջոցների համակարգային և կիրառական ծրագրային ապահովման ելակետային տեքստերը պետք է անցնեն հարձակումներին դիմակայելու տեղեկատվության պաշտպանության մեթոդների և եղանակների իրագործման ստուգում, որոնց նախապատրաստման և անցկացման համար օգտագործվում են խախտողի հնարավորությունները, որոնք նշված են Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2017 թվականի մայիսի 30-ի թիվ 58 (ԾՕՀ) որոշմամբ հաստատված՝ Եվրասիական տնտեսական հանձնաժողովի հավաստագրման կենտրոնում տեղեկատվության անվտանգության սպառնալիքների և խախտում կատարողի գործողությունների մոդելներում:

46. Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովման կազմի մեջ պետք է ընդգրկվի մեխանիզմ, որն ապահովում է կայունությունն արտաքին ցանցերից համակարգչային հարձակումների նկատմամբ:

47. Հավաստագրման կենտրոնի միջոցների կիրառական ծրագրային ապահովումը պետք է չհայտարարագրված հնարավորությունների բացակայության ստուգում անցնի։ Հավաստագրման կենտրոնի միջոցների ծրագրային ապահովումը պետք է համապատասխանի չհայտարարագրված հնարավորությունների բացակայության հսկողության՝ Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանված մակարդակին։

2. Հավաստագրման կենտրոնի ապարատային միջոցներին ներկայացվող պահանջները

48. Հավաստագրման կենտրոնի ապարատային միջոցներին ներկայացվում են հետևյալ պահանջները՝

ա) հավաստագրման կենտրոնի նպատակային գործառույթների իրագործման՝ Հանձնաժողովի կողմից սահմանվող՝ հավաստագրման կենտրոնի ապարատային միջոցների փորձարկումների համակարգի օգտագործման հետ համապատասխանության ստուգման անցկացում.

բ) հավաստագրման կենտրոնի ապարատային միջոցների աշխատանքի հուսալիության պարամետրերի գնահատման անցկացում.

գ) Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանվող՝ կողմնակի էլեկտրամագնիսական ճառագայթումների և մակածումների ուղիներով տեղեկատվության արտահոսքից պաշտպանությանը ներկայացվող պահանջներին հավաստագրման կենտրոնի ապարատային միջոցների համապատասխանության ուսումնասիրությունների անցկացում։

3. Դերերի սահմանազատմանը ներկայացվող պահանջները

49. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվեն հետևյալ պարտադիր դերերը՝

ա) համակարգային ադմինիստրատոր, որի լիազորությունները ներառում են հավաստագրման կենտրոնի միջոցների տեղադրումը, փոխդասավորության և աշխատանքի ապահովումը, հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների պրոֆիլների ստեղծումը և պահպանումը, աուդիտի մատյանի պրոֆիլի և պարամետրերի փոխդասավորության ապահովումը.

բ) հավաստագրման ադմինիստրատոր, որի լիազորությունները ներառում են ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծումը և չեղարկումը.

գ) աուդիտի ադմինիստրատոր, որի լիազորությունները ներառում են աուդիտի մատյանի ստուգումը և վարումը.

դ) օպերատոր, որի լիազորությունները ներառում են հավաստագրման կենտրոնի միջոցներում պահվող տեղեկատվության պահուստային պատճենումը և վերականգնումը:

50. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվի մեխանիզմ, որը բացառում է տարբեր դերերի լիազորությունների օգտագործման նպատակով հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի մեկ անդամի ավտորիզացման հնարավորությունը:

51. Օպերատորը չպետք է աուդիտի մատյանում փոփոխություններ կատարելու հնարավորություն ունենա:

4. Հավաստագրման կենտրոնի միջոցների ամբողջականությանը   
ներկայացվող պահանջները

52. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվի ամբողջականության հսկողության մեխանիզմ, որին ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում։

53. Ամբողջականության հսկողությունը պետք է իրականացվի օպերացիոն համակարգի յուրաքանչյուր վերագործարկման ժամանակ՝ նախքան դրա վերաբեռնումը, և հավաստագրման կենտրոնի միջոցների աշխատանքի ընթացքում (ամբողջականության դինամիկ հսկողություն)։

54. Ամբողջականության դինամիկ հսկողությունը պետք է կատարվի օրն առնվազն 1 անգամ։

55. Հավաստագրման կենտրոնի ծրագրային և (կամ) ապարատային միջոցների կազմում պետք է ներառվեն հավաստագրման կենտրոնի ծրագրային միջոցների ամբողջականության վերականգնման միջոցները։

5. Հասանելիության կառավարմանը ներկայացվող պահանջները

56. Հավաստագրման կենտրոնի միջոցները պետք է ապահովեն հասանելիության կառավարման կամավոր և պարտադիր սկզբունքների իրագործումը, ինչպես նաև փակ աշխատանքային միջավայրի ստեղծումը (ծրագրային միջավայր, որը թույլ է տալիս դրանում ունենալ ծրագրերի և գործընթացների միայն ֆիքսված լրակազմ)։ Հասանելիության կառավարմանը ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

6. Նույնականացմանը և իսկորոշմանը ներկայացվող պահանջները

57. Նույնականացումն ու իսկորոշումը ներառում են հավաստագրման կենտրոնի միջոցներն օգտագործողի, հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամի կամ գործընթացի ճանաչումը, ինչպես նաև դրանց իսկության ստուգումը։ Իսկորոշման բացասական արդյունքի դեպքում իսկորոշման մեխանիզմը պետք է արգելափակի հասանելիության սուբյեկտների հասանելիությունը հավաստագրման կենտրոնի գործառույթներին:

58. Հավաստագրման կենտրոնի միջոցներում իսկորոշման ցանկացած իրագործված ընթացակարգի համար պետք է կիրառվի հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի քանակի սահմանափակման մեխանիզմը, որոնց թիվը չպետք է գերազանցի 3-ը։ Հասանելիության մեկ սուբյեկտի իսկորոշման անընդմեջ հաջորդող փորձերի թիվը գերազանցելու դեպքում հասանելիության այդ սուբյեկտի համար հավաստագրման կենտրոնի միջոցներին հասանելիությունը պետք է արգելափակվի որոշակի ժամանակահատվածով, որը սահմանվում է հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում։

59. Հավաստագրման կենտրոնի միջոցներն օգտագործողների գրանցման ընթացակարգի (հավաստագրման կենտրոնի միջոցներն օգտագործողների ռեեստրում տվյալների մուտքագրման) նկարագրությունը, այդ թվում՝ գրանցման ժամանակ հավաստագրման կենտրոնի միջոցներն օգտագործողի կողմից անձը հաստատող փաստաթղթեր ներկայացնելու անհրաժեշտության մասին պահանջը պետք է պարունակվեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում։

60. Հավաստագրման կենտրոնի միջոցներին հասանելիություն ձեռք բերող անձանց համար պետք է անցկացվի երկգործոն իսկորոշում։

61. Հավաստագրման կենտրոնի միջոցներն օգտագործողների և հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների մասով թույլատրվում է օգտագործել հեռավար իսկորոշման մեխանիզմներ՝ թույլատրված կրիպտոգրաֆիկ ալգորիթմների հիման վրա՝ իսկորոշման հավաստագրերի օգտագործմամբ:

62. Հավաստագրման կենտրոնի միջոցներին լոկալ հասանելիություն ձեռք բերելիս հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամների իսկորոշումը պետք է կատարվի նախքան այդ միջոցների՝ աշխատանքային վիճակի անցնելը (օրինակ՝ մինչև բազային օպերացիոն համակարգի ներբեռնումը)։

63. Լոկալ իսկորոշման համար պայմանանշանային, պարբերաբար փոփոխվող գաղտնաբառ օգտագործելու դեպքում այն պետք է կազմված լինի առնվազն 8 պայմանանշանից (այն դեպքում, երբ այբուբենի պայմանանշանների ընդհանուր թիվը կազմում է առնվազն 36): Գաղտնաբառի փոփոխման ժամանակահատվածը չպետք է գերազանցի 6 ամիսը։

7. Հավաստագրման կենտրոնի կողմից ստացվող կամ փոխանցվող տվյալների պաշտպանությանը ներկայացվող պահանջները

64. Հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու ինքնաստորագրված հավաստագիրը պետք է պահվի դրա ձևափոխումը կամ խեղաթյուրումը բացառող եղանակով:

65. Հավաստագրման կենտրոնի միջոցները պետք է ապահովեն սահմանափակ հասանելիության տեղեկատվություն պարունակող այն տվյալների փոխանցումը, որոնք ստացվել են հավաստագրման կենտրոնի կողմից կամ փոխանցվում են հավաստագրման կենտրոնից՝ տեղեկատվության չարտոնված հասանելիությունը բացառող եղանակով:

66. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն կեղծ հաղորդագրություններ պարտադրելուց պաշտպանությունը (գործողություն, որը էլեկտրոնային փոխգործակցության սուբյեկտների կամ հավաստագրման կենտրոնի միջոցների կողմից ընկալվում է որպես իրական հաղորդագրության փոխանցում՝ չարտոնված հասանելիությունից պաշտպանված եղանակով)՝ թույլատրված կրիպտոգրաֆիկ ալգորիթմների հիման վրա՝ ԷԹՍ-ի ստուգման բանալու հավաստագրերի օգտագործմամբ։ Կեղծ հաղորդագրություններ պարտադրելուց պաշտպանության ընթացակարգին ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

67. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն հավաստագրման կենտրոնի միջոցներն օգտագործողի կողմից իր համար ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծման սկզբնական հարցման պաշտպանված փոխանցման ընթացակարգ։

68. Հավաստագրման կենտրոնի միջոցները պետք է ընդունեն հավաստագրման կենտրոնի գործունեության համար կրիտիկական տեղեկատվությունն այն դեպքում, երբ այն ստորագրված է ԷԹՍ-ով:

69. Հավաստագրման կենտրոնի միջոցների բաղադրիչները պետք է տեղադրվեն մեկ հսկվող գոտում:

8. Իրադարձությունների գրանցմանը ներկայացվող պահանջները

70. Հավաստագրման կենտրոնի միջոցների օպերացիոն համակարգը պետք է ապահովի համակարգային իրադարձությունների մասին տեղեկատվություն պարունակող՝ աուդիտի մատյանի վարումը։ Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվի հավաստագրման կենտրոնի կողմից իր գործառույթները կատարելու հետ կապված իրադարձությունների՝ աուդիտի մատյանում ընտրանքային գրանցման մեխանիզմը։

71. Գրանցվող իրադարձությունների ցանկը պետք է պարունակվի հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

72. Պետք է միջոցներ ձեռնարկվեն հայտնաբերելու համար հավաստագրման կենտրոնի միջոցների ադմինիստրատորների խմբի անդամ չհանդիսացող՝ հավաստագրման կենտրոնի միջոցներն օգտագործողների կողմից աուդիտի մատյանում չարտոնված փոփոխություններ կատարելու դեպքերը։

9. Հավաստագրման կենտրոնի միջոցների հուսալիությանը և   
գործունեության կայունությանը ներկայացվող պահանջները

73. Հավաստագրման կենտրոնի միջոցների հուսալիությանը և գործունեության կայունությանը ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

74. Կատարվում է հավաստագրման կենտրոնի ապարատային միջոցների այնպիսի խափանումների և անսարքությունների առաջացման հավանականության հաշվարկ, որոնք հանգեցնում են հավաստագրման կենտրոնի կողմից իր գործառույթները չկատարելուն:

75. Հավաստագրման կենտրոնի ապարատային միջոցների այնպիսի խափանումների և անսարքությունների առաջացման հավանականությունն օրվա ընթացքում, որոնք հանգեցնում են հավաստագրման կենտրոնի կողմից իր գործառույթները չկատարելուն, չպետք է գերազանցի հավաստագրման կենտրոնի կազմում օգտագործվող կրիպտոգրաֆիկ միջոցների խափանումների և անսարքությունների առաջացման նույնանման հավանականությունը։

76. Հավաստագրման կենտրոնի միջոցների (համալիր) միջին աշխատատևությունը մինչև խափանումը կազմում է առնվազն 10 000 ժ։

77. Պետք է իրականացվի հավաստագրման կենտրոնի միջոցների գործունեության կայունության փորձարկում։

78. Խափանումից հետո հավաստագրման կենտրոնի միջոցների վերականգնման ժամանակին ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում:

79. Հավաստագրման կենտրոնի միջոցների հուսալիության և դրանց գործունեության կայունության բարձրացման միջոցներն ու եղանակները պետք է նախատեսեն հավաստագրման կենտրոնի միջոցների ռեսուրսների քվոտավորում։

10. Առանցքային տեղեկատվության ստեղծմանը, օգտագործմանը,   
պահպանմանը և ոչնչացմանը ներկայացվող պահանջները

80. Առանցքային տեղեկատվության ստեղծման, օգտագործման, պահպանման և ոչնչացման կարգը, ինչպես նաև դրա գործողության ժամկետները սահմանվում են ԷԹՍ-ի միջոցների և հավաստագրման կենտրոնի միջոցների կողմից օգտագործվող կրիպտոգրաֆիկ այլ միջոցների շահագործման փաստաթղթերում սահմանված պահանջներին և Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության պաշտպանության ծածկագրման (կրիպտոգրաֆիկ) միջոցների մշակման և արդիականացման սկզբունքներին համապատասխան:

81. Առանցքային տեղեկատվության պատճենումը պետք է իրականացվի օգտագործվող կրիպտոգրաֆիկ միջոցների շահագործման փաստաթղթերին համապատասխան։ Չի թույլատրվում առանցքային փաստաթղթերի (կրիպտոգրաֆիկ բանալիների, այդ թվում՝ ԷԹՍ-ի բանալիների) տեղեկատվությունը պատճենել կրիչների վրա (օրինակ՝ կոշտ սկավառակի), որոնք մասնագիտացված առանցքային կրիչներ չեն, առանց դրա նախնական ծածկագրման, որը պետք է իրականացվի տեղեկատվության կրիպտոգրաֆիկ պաշտպանության օգտագործվող միջոցի ներկառուցված գործառույթի կիրառմամբ։

82. ԷԹՍ-ի այն բանալին, որն օգտագործվում է ԷԹՍ-ի ստուգման բանալիների ստեղծվող հավաստագրերի և ԷԹՍ-ի ստուգման բանալիների հավաստագրերի եզակի համարների ցանկի ստորագրման համար, որոնց գործողությունը ժամանակի որոշակի պահին դադարեցվել է հավաստագրման կենտրոնի կողմից մինչև դրանց գործողության ժամկետը լրանալը (այսուհետ՝ հետ կանչված հավաստագրերի ցանկ), չպետք է օգտագործվի այլ նպատակներով:

11. Տեղեկատվության պահուստային պատճենմանը և   
հավաստագրման կենտրոնի միջոցների աշխատունակության վերականգնմանը ներկայացվող պահանջները

83. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն հավաստագրման կենտրոնի միջոցներով մշակվող տեղեկատվության պահուստային պատճենման և այդ տեղեկատվության ու այդ միջոցների վնասման դեպքում հավաստագրման կենտրոնի ապարատային միջոցների աշխատունակության վերականգնման գործառույթներ։ Պահուստային պատճենման ընթացքում պետք է բացառվի կրիպտոգրաֆիկ բանալիների պատճենման հնարավորությունը:

84. Պահուստային պատճենման ժամանակ պահպանված տվյալները պետք է բավարար լինեն հավաստագրման կենտրոնի միջոցների գործունեության՝ մինչև տվյալների պատճենման պահի դրությամբ գրանցված վիճակը վերականգնելու համար:

85. Պետք է ձեռնարկվեն պահպանված տվյալների չարտոնված փոփոխությունների հայտնաբերմանն ուղղված միջոցներ:

86. Հավաստագրման կենտրոնի միջոցների աշխատունակության վերականգնման ժամանակին ներկայացվող պահանջները սահմանվում են հավաստագրման կենտրոնի միջոցների մշակման (արդիականացման) տեխնիկական առաջադրանքում և հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

12. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծմանը և   
չեղարկմանը ներկայացվող պահանջները

87. ԷԹՍ-ի ստուգման բանալիների հավաստագրերի ստեղծման և չեղարկման արձանագրությունները պետք է նկարագրված լինեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

88. Հավաստագրման կենտրոնի կողմից ստեղծվող ԷԹՍ-ի ստուգման բանալիների հավաստագրերը և հետ կանչված հավաստագրերի ցանկերը պետք է համապատասխանեն Եվրասիական տնտեսական հանձնաժողովի խորհրդի 2017 թվականի թիվ որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների թիվ 5 հավելվածով սահմանված պահանջներին:

89. Հավաստագրման կենտրոնի միջոցները պետք է իրագործեն Եվրասիական տնտեսական հանձնաժողովի խորհրդի 2017 թվականի թիվ որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների թիվ 5 հավելվածով սահմանված պահանջներին ԷԹՍ-ի ստուգման բանալիների ստեղծվող հավաստագրերի համապատասխանության հսկողության մեխանիզմ:

90. Հավաստագրման կենտրոնի միջոցները հետ կանչված հավաստագրերի ցանկերի օգտագործմամբ պետք է իրագործեն ԷԹՍ-ի ստուգման բանալու հավաստագրի չեղարկում։

91. Հավաստագրման կենտրոնի միջոցները ԷԹՍ-ի ստուգման բանալու հավաստագրի տիրապետողի նկատմամբ պետք է իրագործեն ԷԹՍ-ի ստուգման բանալու եզակիության ստուգում և ԷԹՍ-ի համապատասխան բանալուն տիրապետելու ստուգում:

92. ԷԹՍ-ի ստուգման բանալիների հավաստագրերում և չեղարկված հավաստագրերի ցանկերում ժամանակի արժեքների սխալանքը չպետք է գերազանցի 10 րոպեն։

13. ԷԹՍ-ի ստուգման բանալիների տրված, գործողությունը դադարած և չեղարկված հավաստագրերի ռեեստրին և դրան հասանելիություն տրամադրելուն ներկայացվող պահանջները

93. Հավաստագրման կենտրոնի միջոցներում պետք է իրագործվեն ԷԹՍ-ի ստուգման բանալիների տրված, գործողությունը դադարած և չեղարկված հավաստագրերի ռեեստրում (այսուհետ՝ հավաստագրերի ռեեստր) ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրված, գործողությունը դադարած և չեղարկված հավաստագրերը պահպանելու և ատրիբուտներով փնտրելու մեխանիզմներ, ինչպես նաև հավաստագրերի ռեեստրին ցանցային հասանելիություն տրամադրելու մեխանիզմներ:

94. Հավաստագրերի ռեեստրում կատարվող բոլոր փոփոխությունները պետք է գրանցվեն աուդիտի մատյանում:

14. Կրիպտոգրաֆիկ միջոցներին ներկայացվող պահանջները

95. Հավաստագրման կենտրոնի միջոցները պետք է օգտագործեն ԷԹՍ-ի միջոցներ և կրիպտոգրաֆիկ այլ միջոցներ, որոնք ունեն Հանձնաժողովի գտնվելու պետության լիազորված մարմինների՝ Հանձնաժողովի գտնվելու պետության օրենսդրությամբ ԿՄ3 դասի կրիպտոգրաֆիկ միջոցներին ներկայացվող պահանջներին և Հանձնաժողովի կողմից հաստատվող՝ տեղեկատվության պաշտպանության ծածկագրման (կրիպտոգրաֆիկ) միջոցների մշակման և արդիականացման սկզբունքներին համապատասխանության մասին եզրակացություն:

15. Կրիպտոգրաֆիկ ստանդարտներին ներկայացվող պահանջները

96. Հավաստագրման կենտրոնի միջոցները պետք է օգտագործեն Եվրասիական տնտեսական հանձնաժողովի կոլեգիայի 2015 թվականի փետրվարի 3-ի թիվ 10 որոշմանը (ԾՕՀ) համապատասխան կրիպտոգրաֆիկ ալգորիթմներ իրականացնող կրիպտոգրաֆիկ միջոցներ։

16. ԷԹՍ-ի ստուգման բանալու հավաստագրի վավերականության ստուգմանը ներկայացվող պահանջները

97. ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրվող հավաստագրերում ԷԹՍ-ի ստուգման՝ հավաստագրման կենտրոնի միջոցներում իրագործված մեխանիզմը պետք է նշվի հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում: Այդ մեխանիզմը պետք է ապահովի ԷԹՍ-ի ստուգումը ԷԹՍ-ի ստուգման բանալիների՝ հավաստագրման կենտրոնի կողմից տրվող հավաստագրերում՝ ԷԹՍ-ի ստուգման բանալու հավաստագրի ստեղծումից հետո և մինչև դրա տրամադրումը:

98. Հավաստագրման կենտրոնի միջոցները ստուգում են ԷԹՍ-ի ստուգման բանալիների հավաստագրերի շղթայից յուրաքանչյուր հավաստագրի վավերականությունը, այդ թվում՝ այն ԷԹՍ-ի վավերականությունը, որով ստորագրված են այդ հավաստագրերը: Տվյալ շղթան կազմված է հավաստագրման կենտրոնի ԷԹՍ-ի ստուգման բանալու հիմնական ինքնաստորագրված հավաստագրից և ԷԹՍ-ի ստուգման բանալու ստուգվող հավաստագրից:

17. Լրացուցիչ պահանջներ

99. Հավաստագրման կենտրոնի միջոցների միացում այն տեղեկատվական-հեռահաղորդակցական ցանցին, որին հասանելիությունը սահմանափակված չէ անձանց որոշակի շրջանակի կողմից, չի թույլատրվում։

100. Կապի ուղիների օգտագործմամբ հավաստագրման կենտրոնի միջոցների վրա հարձակումների կազմակերպման հնարավորությունների սահմանափակման նպատակով պետք է կիրառվեն միջցանցային էկրանավորման միջոցներ, որոնք կիրառում են հավաստագրման կենտրոնի սպասարկիչները, որոնք փոխգործակցում են հավաստագրման կենտրոնի միջոցներն օգտագործողների հետ։

101. Պետք է կիրառվեն համակարգչային վիրուսներից պաշտպանության միջոցներ, որոնք ապահովում են պաշտպանվող տեղեկատվության չարտոնված ոչնչացման, արգելափակման, ձևափոխման, պատճենման կամ տեղեկատվության պաշտպանության միջոցների չեզոքացման համար նախատեսված համակարգչային ծրագրերի կամ այլ համակարգչային տեղեկատվության հայտնաբերումը, ինչպես նաև պետք է ապահովվի այդպիսի ծրագրերի և տեղեկատվության հայտնաբերման առնչությամբ արձագանքումը։

102. Միջցանցային էկրանավորման միջոցները և համակարգչային վիրուսներից պաշտպանության միջոցները պետք է համապատասխանեն Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանվող պահանջներին։

103. Հավաստագրման կենտրոնի միջոցների ուսումնասիրությունները սույն պահանջներին դրանց համապատասխանությունը հաստատելու նպատակով պետք է իրականացվեն Հանձնաժողովի գտնվելու պետության լիազորված մարմնի կողմից սահմանվող՝ հավաստագրման կենտրոնի միջոցներում իրագործվող՝ տեղեկատվության պաշտպանության մեխանիզմների պարամետրերի և բնութագրերի թվային արժեքների օգտագործմամբ:

104. Հավաստագրման կենտրոնի միջոցները պետք է շահագործվեն դրանց շահագործման փաստաթղթերին համապատասխան: Հավաստագրման կենտրոնի միջոցների անվտանգ գործունեությունն ապահովելու համար անհրաժեշտ կազմակերպատեխնիկական միջոցառումները պետք է նշվեն հավաստագրման կենտրոնի միջոցների շահագործման փաստաթղթերում:

ՀԱՎԵԼՎԱԾ ԹԻՎ 5

Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջների

**ՊԱՀԱՆՋՆԵՐ**

**տեղեկատվության պաշտպանության ապահովման միջոցներին և   
եղանակներին ներկայացվող**

I. Ընդհանուր դրույթներ

1. Սույն պահանջները պարունակում են տեղեկատվության պաշտպանության ապահովման այն միջոցների և եղանակների նկարագրությունը, որոնք պետք է իրագործվեն էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների կողմից վստահության անդրսահմանային տարածքի տարրերի և նրանց կողմից տրամադրվող ծառայությունների նկատմամբ, որոնց շահագործումն ապահովում է էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորը (այսուհետ՝ պաշտպանության օբյեկտ)։

2. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչի տարրերի և ծառայությունների պաշտպանությունն իրականացվում է սույն պահանջներին համապատասխան։

3. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների տարրերի և ծառայությունների պաշտպանությունն իրականացվում է Եվրասիական տնտեսական միության անդամ պետությունների օրենսդրությանը կամ միջազգային ստանդարտներին համապատասխան՝ հաշվի առնելով սույն պահանջները։

4. Սույն պահանջներով սահմանվում են պաշտպանության օբյեկտներում իրագործվող՝ տեղեկատվության պաշտպանության միջոցներին և եղանակներին ներկայացվող նվազագույն անհրաժեշտ պահանջները և ներառում են՝

ա) ֆիզիկական պաշտպանության ապահովմանը ներկայացվող պահանջները,

բ) վնասաբեր ծրագրային ապահովումից պաշտպանության ապահովմանը ներկայացվող պահանջները,

գ) պահուստային պատճենման ապահովմանը ներկայացվող պահանջները,

դ) տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի հաշվառմանը ներկայացվող պահանջները,

ե) պաշտպանության օբյեկտի տեխնիկական միջոցների, ծրագրային ապահովման և տեղեկատվական ակտիվների պաշտպանվածության հսկողությանը ներկայացվող պահանջները,

զ) կրիպտոգրաֆիկ պաշտպանության միջոցների հետ աշխատանքին ներկայացվող պահանջները,

է) հասանելիության կառավարմանը ներկայացվող պահանջները։

5. Սույն պահանջների իրագործման նպատակով վստահության անդրսահմանային տարածքի յուրաքանչյուր տարրի համար էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների կողմից պետք է մշակվեն համապատասխան փաստաթղթեր, որոնք պետք է կանոնավոր վերանայման և արդիականացման ենթարկվեն։

6. Վստահության անդրսահմանային տարածքի տարրերի շահագործման և ուղեկցման նկատմամբ հասանելիություն ունեցող անձանց իրենց իրավասության շրջանակներում պետք է ծանոթացնել սույն պահանջների 5-րդ կետում նշված փաստաթղթերին։

II. Ֆիզիկական պաշտպանության ապահովմանը   
ներկայացվող պահանջները

7. Պաշտպանության օբյեկտի համար պետք է սահմանված լինեն հսկվող գոտիներ, որտեղ ֆիզիկապես մուտք գործելը պետք է սահմանափակված լինի, այդ թվում՝ հասանելիության հսկման համակարգի միջոցներով։

8. Պետք է սահմանված լինի այն անձանց ցանկը, որոնց թույլատրվում է մուտք գործել պաշտպանության օբյեկտ՝ նշելով նրանց դերերը (հասանելիության մակարդակը)։

9. Պետք է բացառված լինի տեղեկատվության արտապատկերման միջոցներով կողմնակի անձանց համար տեղեկատվության նկատմամբ հասանելիություն ստանալու հնարավորությունը։

10. Հսկվող գոտու տարածքով կողմնակի անձանց տեղաշարժը պետք է արգելված լինի։

11. Այն հաշվողական տեխնիկայի միջոցների տեղակայումը, որի միջոցով իրականացվում է հսկող գոտուց դուրս պաշտպանության օբյեկտի տվյալների մշակումը, պետք է արգելված լինի։

12. Հաշվողական տեխնիկայի միջոցների և տեղեկատվության պահպանման միջոցների ներսբերումը (դուրսբերումը) հսկվող գոտի (հսկվող գոտուց) պետք է գրանցվի հատուկ մատյաններում։

13. Պաշտպանության օբյեկտի ֆիզիկական պաշտպանության և հասանելիության հսկման վերաբերյալ փաստաթղթերը պետք է պարունակեն՝

ա) սահմանափակ հասանելիությամբ հսկվող գոտիների սարքավորվածության կարգը,

բ) այն անձանց ցանկը վարելու կարգը, որոնց թույլատրվում է մուտք գործել պաշտպանության օբյեկտ՝ նշելով նրանց դերերը (հասանելիության մակարդակը),

գ) հսկվող գոտուն հասանելիություն ստանալու և դրանով կողմնակի անձանց տեղաշարժի հսկման կարգը,

դ) հսկվող գոտի (հսկվող գոտուց) հաշվողական տեխնիկայի միջոցների և տեղեկատվության պահպանման միջոցների ներսբերման (դուրսբերման) կարգը,

ե) հսկվող գոտում գտնվող՝ պաշտպանության օբյեկտի տարրերի նկատմամբ հասանելիություն ունեցող օգտագործողների դերերի նկարագրությունը,

զ) հասանելիության կառավարման այն քաղաքականության նկարագրությունը, որով սահմանվում է տարբեր դերեր ունեցող օգտագործողների՝ ծառայությունների հետ և օգտագործողների անունից հանդես եկող ծառայությունների՝ պաշտպանության օբյեկտի տարրերի և ծառայությունների հետ թույլատրելի գործողությունների ամբողջությունը։

III. Վնասաբեր ծրագրային ապահովումից պաշտպանության   
ապահովմանը ներկայացվող պահանջները

14. Պաշտպանության օբյեկտի բոլոր սպասարկիչների վրա և աշխատանքային կայաններում պետք է նախատեսված լինեն և պետք է իրականացվեն վնասաբեր ծրագրային ապահովումից պաշտպանության միջոցներ։

15. Պետք է կանոնավոր կերպով կատարվի պաշտպանության օբյեկտի սպասարկիչների և աշխատանքային կայանների ստուգում վնասաբեր ծրագրային ապահովման առկայության առնչությամբ։

16. Պաշտպանության միջոցների անջատումը վնասաբեր ծրագրային ապահովումից պետք է արգելված լինի։

17. Պետք է կատարվի վնասաբեր ծրագրային ապահովումից պաշտպանության միջոցների կանոնավոր թարմացում։

18. Վնասաբեր ծրագրային ապահովման հայտնաբերման բոլոր դեպքերը պետք է արձանագրվեն։

19. Վնասաբեր ծրագրային ապահովումից պաշտպանության օբյեկտի պաշտպանության մասին փաստաթղթերը պետք է պարունակեն՝

ա) վնասաբեր ծրագրային ապահովումից պաշտպանության օբյեկտի պաշտպանության միջոցների կազմին ներկայացվող պահանջները,

բ) վնասաբեր ծրագրային ապահովումից պաշտպանության օբյեկտի պաշտպանության աշխատանքների կատարման կանոնակարգը,

գ) վնասաբեր ծրագրային ապահովում հայտնաբերելիս անձնակազմի գործողությունների կարգը,

դ) վնասաբեր ծրագրային ապահովման հայտնաբերման և վերացման իրադարձությունների գրանցման կարգը,

ե) վնասաբեր ծրագրային ապահովումից օբյեկտի պաշտպանության միջոցների աշխատունակության փորձարկման կարգը։

IV. Պահուստային պատճենման ապահովմանը   
ներկայացվող պահանջները

20. Պաշտպանության օբյեկտի հաշվողական տեխնիկայի միջոցների կազմում պետք է նախատեսված լինեն տվյալների պատճենման և վերականգնման միջոցներ, պահուստային պատճենների կառավարման և հաշվառման միջոցներ, տվյալների պահպանման միջոցներ, պահուստային պատճենների պահպանման համար օգտագործվող տեղեկատվության կրիչներ։

21. Պահուստային պատճենման բոլոր իրադարձությունները պետք է գրանցվեն հատուկ մատյաններում։

22. Պետք է կատարվի պահուստային պատճենման միջոցների աշխատունակության կանոնավոր փորձարկում։

23. Տվյալների պահուստային պատճենում կատարելու մասին փաստաթղթերը պետք է պարունակեն՝

ա) տվյալների պատճենման և վերականգնման միջոցների կազմին ներկայացվող պահանջները,

բ) տեղեկատվության պահուստային պատճենման աշխատանքների կատարման կանոնակարգը,

գ) պահուստային պատճեններից տվյալների վերականգնման անհրաժեշտություն առաջանալու դեպքում անձնակազմի գործողությունների կարգը,

դ) տվյալների պահուստային պատճենման և վերականգնման իրադարձությունների գրանցման կարգը,

ե) պահուստային պատճենման միջոցների աշխատունակության փորձարկման կարգը։

V. Տեղեկատվական անվտանգության իրադարձությունների ու   
միջադեպերի հաշվառմանը ներկայացվող պահանջները

24. Պետք է վարել տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի հաշվառում։

25. Պետք է մշակել տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի մշակման կարգ։

26. Պետք է սահմանված լինեն տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի մշակման համար պատասխանատու անձինք։

27. Տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի գրանցման ու հաշվառման մասին փաստաթղթերը պետք է պարունակեն՝

ա) տեղեկատվական անվտանգության իրադարձությունների ու միջադեպերի հաշվառման կարգը,

բ) իրադարձությունների ու միջադեպերի մշակման քաղաքականությունը,

գ) իրադարձությունների ու միջադեպերի մշակման համար պատասխանատու անձանց նշանակման կարգն ու գործողությունների նկարագրությունը։

VI. Պաշտպանության օբյեկտի տեխնիկական միջոցների,   
ծրագրային ապահովման և տեղեկատվական ակտիվների պաշտպանվածության հսկողությանը ներկայացվող պահանջները

28. Պետք է կատարվի պաշտպանության օբյեկտի տարրերի կանոնավոր գույքագրում՝ պաշտպանության օբյեկտում բացված տեխնիկական միջոցների, ծրագրային ապահովման և տեղեկատվական ակտիվների, ինչպես նաև պետք է արձանագրվեն պաշտպանության օբյեկտի հետ տեղի ունեցող բոլոր փոփոխությունները։

29. Պետք է կատարել խոցելի տեղերի հսկում, որը ներառում է խոցելի տեղերի հայտնաբերումը (խոցելի տեղերին մշտապես հետևելը), հայտնաբերված խոցելի տեղերի հետ կապված՝ անվտանգության սպառնալիքների գնահատումը, խոցելի տեղերի վերացմանը (մեկուսացմանը) ուղղված պաշտպանության միջոցների ձեռնարկումը։

30. Պաշտպանության օբյեկտում բացված տեխնիկական միջոցների, ծրագրային ապահովման և տեղեկատվական ակտիվների պաշտպանվածության հսկման մասին փաստաթղթերը պետք է պարունակեն՝

ա) պաշտպանության օբյեկտի տարրերի կանոնավոր գույքագրում կատարելու կարգը. պաշտպանության օբյեկտում բացված տեխնիկական միջոցներ, ծրագրային ապահովման և տեղեկատվական ակտիվներ,

բ) խոցելի տեղերի հսկում կատարելու կարգը, որը ներառում է խոցելի տեղերին հետևելը, հայտնաբերված խոցելի տեղերի հետ կապված՝ անվտանգության սպառնալիքների գնահատումը, խոցելի տեղերի վերացմանն (մեկուսացմանն) ուղղված պաշտպանության միջոցների ձեռնարկումը,

գ) պաշտպանական միջոցների նկարագրությունը։

VII. Տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների հետ աշխատանքին ներկայացվող պահանջները

31. Պետք է իրականացվի տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների բաղադրիչների ամբողջականության հսկողություն։

32. Պետք է սահմանված և ճշգրիտ իրագործված լինեն տեղեկատվության պաշտպանության միջոցների բաղադրիչների ամբողջականության հսկողության ապահովման կրիպտոգրաֆիկ մեթոդները։

33. Պետք է սահմանված և ճշգրիտ իրագործված լինեն տեղեկատվության պաշտպանության ապարատային մեթոդները։

34. Պետք է սահմանված և ճշգրիտ իրագործված լինեն գաղտնիքի բաժանման մեթոդները։

35. Տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցներից տվյալներն արտահանելիս պետք է սահմանվի այդ տվյալների պաշտպանությունը և պետք է կատարվի ամբողջականության հսկում։

36. Բոլոր սեանսային կրիտիկական օբյեկտները պետք է մաքրվեն նախքան սեանսներն ավարտվելը։

37. Պետք է օգտագործվեն տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միայն հավաստագրված միջոցներ։

38. Տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցները պահելու վայրերը պետք է սարքավորված լինեն պաշտպանության հատուկ միջոցներով, որոնք բացառում են կողմնակի անձանց՝ այդ վայրեր մուտք գործելու ցանկացած եղանակի հնարավորությունը, ներառյալ՝ ֆիզիկական ներթափանցումից պաշտպանությունը, տեղեկատվության վիզուալիզացման միջոցների պաշտպանությունը, պաշտպանությունը ցանցային հասանելիության մակարդակում և պաշտպանության այլ միջոցներ։

39. Պետք է կատարվի տեղեկատվության կրիպտոգրաֆիկ պաշտպանության պահպանվող միջոցների նմուշ առ նմուշ հաշվառում։

40. Հատուկ մատյաններում պետք է կատարվի սպասարկող անձնակազմի բոլոր աշխատանքների գրանցում տեղեկատվության պաշտպանության կրիպտոգրաֆիկ միջոցներով։

41. ԷԹՍ-ի բանալիները պահող հանովի կրիչների համար պետք է սարքավորվեն հատուկ պահոցներ (սեյֆեր)։

42. Տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների շահագործումը պետք է կատարվի այն անձանց կողմից, որոնք պատրաստություն են անցել և ուսումնասիրել տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների շահագործման փաստաթղթերը։

43. Տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների հետ աշխատանքի մասին փաստաթղթերը պետք է պարունակեն՝

ա) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների բաղադրիչների ամբողջականության հսկողության իրականացման կանոնակարգը.

բ) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների բաղադրիչների ամբողջականության, պաշտպանության ապարատային մեթոդների հսկողության ապահովման կրիպտոգրաֆիկ մեթոդների իրագործմանը ներկայացվող պահանջները.

գ) ամբողջականության պաշտպանությանն ու հսկողությանը ներկայացվող պահանջները տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցներից տվյալներ արտահանելիս.

դ) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության հավաստագրված միջոցների ցանկը.

ե) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցները պահելու վայրերի՝ պաշտպանության այնպիսի հատուկ միջոցներով սարքավորմանը ներկայացվող պահանջները, որոնք բացառում են կողմնակի անձանց՝ այդ վայրեր մուտք գործելու ցանկացած եղանակի հնարավորությունը, ներառյալ՝ ֆիզիկական ներթափանցումից պաշտպանությունը, տեղեկատվության վիզուալիզացման միջոցների պաշտպանությունը, պաշտպանությունը ցանցային հասանելիության մակարդակում և պաշտպանության այլ միջոցներ.

զ) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության պահպանվող միջոցների հաշվառման կարգը.

է) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների հետ բոլոր աշխատանքների գրանցման կարգը.

ը) տեղեկատվության կրիպտոգրաֆիկ պաշտպանության միջոցների շահագործում իրականացնող անձանց պատրաստվածությանը ներկայացվող պահանջները։

VIII. Հասանելիության կառավարմանը ներկայացվող պահանջները

44. Հասանելիության կառավարումն ապահովելու համար պետք է սահմանված լինեն օգտագործողների դերերը։

45. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի օպերատորների կողմից պետք է հստակեցվի հասանելիության կառավարման կարգը, որով սահմանվում է տարբեր դերեր ունեցող օգտագործողների՝ ծառայությունների և օգտագործողների անունից հանդես եկող ծառայությունների՝ օբյեկտների և այլ ծառայությունների հետ թույլատրելի գործառնությունների ամբողջությունը։

ՀԱՍՏԱՏՎԱԾ Է

Եվրասիական տնտեսական հանձնաժողովի խորհրդի  
20 թվականի ի  
թիվ որոշմամբ

**ՀԻՄՆԱԴՐՈՒՅԹ**

էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների՝ վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջներին համապատասխանության ստուգման հարցերով հանձնաժողովի մասին

1. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի բաղադրիչների՝ վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջներին համապատասխանության ստուգման հարցերով հանձնաժողովը (այսուհետ՝ միջպետական հանձնաժողով) ստեղծվում է «Եվրասիական տնտեսական միության շրջանակներում տեղեկատվական հաղորդակցական տեխնոլոգիաների և տեղեկատվական փոխգործակցության մասին» արձանագրության («Եվրասիական տնտեսական միության մասին» 2014 թվականի մայիսի 29-ի պայմանագրի թիվ 3 հավելված) 18-րդ կետին համապատասխան։

2. Սույն հիմնադրույթում կիրառվող հասկացությունները օգտագործվում են Եվրասիական տնտեսական հանձնաժողովի խորհրդի 20 թվականի թիվ որոշմամբ հաստատված՝ Վստահության անդրսահմանային տարածքի ստեղծմանը, զարգացմանը և գործունեությանը ներկայացվող պահանջներով (այսուհետ՝ Պահանջներ) սահմանված իմաստներով։

3. Միջպետական հանձնաժողովի կազմում ընդգրկվում են Եվրասիական տնտեսական հանձնաժողովի (այսուհետ՝ Հանձնաժողով) պաշտոնատար անձինք և Եվրասիական տնտեսական միության անդամ պետությունների (այսուհետ՝ անդամ պետություններ) լիազորված մարմինների ներկայացուցիչներ, որոնց իրավասությանն են վերապահված Եվրասիական տնտեսական միության ինտեգրացված տեղեկատվական համակարգի՝ անդամ պետությունների ազգային հատվածների ստեղծման, անդրսահմանային էլեկտրոնային փաստաթղթաշրջանառության շրջանակներում օգտագործվող էլեկտրոնային փաստաթղթերի տեղեկատվական անվտանգության և իրավաբանական նշանակության ապահովման հարցերը։

4. Միջպետական հանձնաժողովի կազմը հաստատվում է Հանձնաժողովի խորհրդի կարգադրությամբ։

5. Միջպետական հանձնաժողովի նախագահը Հանձնաժողովի կոլեգիայի այն անդամն է, որի իրավասությանն են վերապահված տեղեկատվայնացման և տեղեկատվական-հաղորդակցական տեխնոլոգիաների հարցերը։

6. Միջպետական հանձնաժողովի նախագահն իրականացնում է միջպետական հանձնաժողովի աշխատանքի ընդհանուր ղեկավարումը։

7. Միջպետական հանձնաժողովի որոշմամբ դրա կազմում կարող են ձևավորվել ենթահանձնաժողովներ, ինչպես նաև աշխատանքային և փորձագիտական խմբեր։

8. Միջպետական հանձնաժողովի նիստերի անցկացման, ենթահանձնաժողովների, աշխատանքային և փորձագիտական խմբերի ձևավորման, փորձագետների ներգրավման, միջպետական հանձնաժողովի կողմից որոշումների ընդունման և դրանց ձևակերպման, ինչպես նաև միջպետական հանձնաժողովի կողմից ընդունվող փաստաթղթերի ձևերը սահմանվում են Հանձնաժողովի կողմից սահմանվող՝ միջպետական հանձնաժողովի աշխատանքի կանոնակարգով։

9. Միջպետական հանձնաժողովը կատարում է հետևյալ հիմնական գործառույթները՝

ա) լիազորված մարմինների և Հանձնաժողովի առաջարկությունների հիման վրա յուրաքանչյուր տարի ձևավորում և հաստատում է էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական և ինտեգրացիոն բաղադրիչների՝ Պահանջներին համապատասխանության ստուգումների (այսուհետ՝ ստուգումներ) անցկացման պլան-ժամանակացույցը.

բ) մշակում և Հանձնաժողովի կոլեգիայի քննարկմանն է ներկայացնում անդամ պետություններում և Հանձնաժողովում ստուգումներ անցկացնելու վերաբերյալ մեթոդական փաստաթղթեր.

գ) ստուգումների արդյունքների հիման վրա ընդունում է որոշումներ՝ վստահության անդրսահմանային տարածքի՝ էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն կամ պետական բաղադրիչների մեջ մտնող տարրերի օպերատորների (այսուհետ՝ օպերատորներ) հավատարմագրման, ինչպես նաև համապատասխան վկայականների (վկայագրերի) տրամադրման մասին.

դ) վստահության անդրսահմանային տարածքի շրջանակներում իրականացնում է այլ գործառույթներ։

10. Ստուգումներն անցկացվում են հավատարմագրում ունեցող օպերատորների կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրերի մասով։

11. Օպերատորի հավատարմագրումը կատարվում է 2 հաջորդական փուլերով՝

ա) օպերատորի կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի նախնական գնահատում,

բ) օպերատորի հավատարմագրման և այդ օպերատորի հավատարմագրման մասին որոշման ընդունման վերաբերյալ լիազորված մարմնի կամ Հանձնաժողովի կողմից ուղարկված հարցման վերլուծություն։

12. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչի մեջ մտնող՝ վստահության անդրսահմանային տարածքի տարրի նախնական գնահատումն իրականացվում է լիազորված մարմնի կողմից՝ սահմանված կարգով լիազորված մարմին ներկայացվող՝ օպերատորի դիմումի հիման վրա։

Այդ նախնական գնահատման ընթացքում սահմանվում է օպերատորի կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի համապատասխանությունը Պահանջներին և անդամ պետության օրենսդրությանը։

13. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն բաղադրիչի մեջ մտնող՝ վստահության անդրսահմանային տարածքի տարրի նախնական գնահատումն իրականացվում է Հանձնաժողովի կողմից՝ միջպետական հանձնաժողովի կողմից սահմանվող կարգով։

Այդ նախնական գնահատման ընթացքում սահմանվում է օպերատորի (Հանձնաժողովի) կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի համապատասխանությունը Պահանջներին։

14. Էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի պետական բաղադրիչների մեջ մտնող՝ վստահության անդրսահմանային տարածքի տարրերի նախնական գնահատումն իրականացվում է լիազորված մարմինների կողմից՝ նրանց կողմից սահմանվող փաստաթղթերի օգտագործմամբ։

15. Օպերատորի (այսուհետ՝ դիմումատու) կողմից դիմումն ուղարկելու օրվանից 2 ամիսը չգերազանցող ժամկետում լիազորված մարմինը որոշում է ընդունում դիմումատուի կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի՝ Պահանջներին և անդամ պետության օրենսդրությանը համապատասխանելու կամ չհամապատասխանելու մասին։

Դիմումատուի կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի՝ Պահանջներին և անդամ պետության օրենսդրությանը համապատասխանելու մասին որոշում ընդունելու դեպքում լիազորված մարմինը դիմումատուին ծանուցում է այդ որոշման մասին և միջպետական հանձնաժողով հարցում է ուղարկում վերջինիս հավատարմագրում անցկացնելու մասին։

Դիմումատուի կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրի՝ Պահանջներին և անդամ պետության օրենսդրությանը չհամապատասխանելու մասին որոշում ընդունելու դեպքում լիազորված մարմինն այդ դիմումատուին ծանուցում է հայտնաբերված անհամապատասխանության մասին։

16. Միջպետական հանձնաժողովի կողմից սահմանվող կարգով Հանձնաժողովը միջպետական հանձնաժողով է ուղարկում Հանձնաժողովի՝ որպես օպերատորի հավատարմագրում անցկացնելու մասին հարցում։

17. Միջպետական հանձնաժողովը միջպետական հանձնաժողովի աշխատանքի կանոնակարգով սահմանվող կարգով և ժամկետներում անցկացնում է օպերատորի հավատարմագրում։

18. Օպերատորի հավատարմագրման արդյունքների մասին միջպետական հանձնաժողովի աշխատանքի կանոնակարգով սահմանվող կարգով և ժամկետներում միջպետական հանձնաժողովը ծանուցում է այդ օպերատորին և հավատարմագրում անցկացնելու մասին հարցում ուղարկած լիազորված մարմնին։

19. Հավատարմագրված օպերատորների մասին տեղեկությունները ներառվում են օպերատորների միասնական ռեեստրում, որը վարում է Հանձնաժողովը։

20. Լիազորված մարմիններն ու Հանձնաժողովն ստուգումներ են անցկացնում տարին առնվազն 1 անգամ։ Այդ ստուգումների նպատակը հավատարմագրված օպերատորների կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրերի՝ Պահանջներին և (կամ) անդամ պետության օրենսդրությանը համապատասխանության հաստատումն է։ Լիազորված մարմիններն ու Հանձնաժողովը պարտավոր են միջպետական հանձնաժողով ուղարկել ստուգումներ անցկացնելու մասին հաշվետվություն ոչ ուշ, քան այդ ստուգումներն ավարտելու օրվանից հետո 20 աշխատանքային օրվա ընթացքում։

21. Միջպետական հանձնաժողովն ու լիազորված մարմինն իրավունք ունեն հավատարմագրված օպերատորների կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրերի՝ Պահանջներին և անդամ պետության օրենսդրությանը համապատասխանության լրացուցիչ ստուգումներ անցկացնելու։

22. Օպերատորների կողմից շահագործվող՝ վստահության անդրսահմանային տարածքի տարրերի ստուգումների և նախնական գնահատումների անցկացման նպատակով անդամ պետությունների լիազորված մարմինները և Հանձնաժողովն իրավունք ունեն ներգրավել կողմնակի կազմակերպությունների։

23. Միջպետական հանձնաժողովն իրավունք ունի հետ կանչելու օպերատորի հավատարմագիրը, եթե հայտնաբերվել են Պահանջների և (կամ) անդամ պետության օրենսդրության խախտումներ։ Ընդ որում, օպերատորը սահմանված ժամկետում անհրաժեշտ գործողություններ չի ձեռնարկում միջպետական հանձնաժողովի կողմից ուղարկված ծանուցման մեջ նշված խախտումները վերացնելու ուղղությամբ։

Միջպետական հանձնաժողովն օպերատիվ կերպով լիազորված մարմնին և օպերատորին տեղեկացնում է օպերատորի հավատարմագրումը հետ կանչելու մասին։

24. Լիազորված մարմինն իրավունք ունի միջպետական հանձնաժողովին միջնորդել օպերատորի հավատարմագրումը հետ կանչելու մասին, եթե հայտնաբերվել են Պահանջների և (կամ) անդամ պետության օրենսդրության խախտումներ։ Ընդ որում, օպերատորը սահմանված ժամկետում անհրաժեշտ գործողություններ չի ձեռնարկում միջպետական հանձնաժողովի կողմից ուղարկված ծանուցման մեջ նշված խախտումները վերացնելու ուղղությամբ։

Լիազորված մարմինն օպերատորին տեղեկացնում է այդ օպերատորի հավատարմագրումը հետ կանչելու մասին միջնորդությունը միջպետական հանձնաժողով ուղարկելու վերաբերյալ՝ այդ միջնորդությունն ուղարկելու օրվանից 3 աշխատանքային օրվա ընթացքում։

25. Անդամ պետությունները կարող են լիազորել իրենց լիազորված մարմիններին անցկացնել էլեկտրոնային եղանակով տեղեկատվության փաստաթղթավորման ընդհանուր ենթակառուցվածքի ինտեգրացիոն և պետական բաղադրիչների մեջ մտնող՝ վստահության անդրսահմանային տարածքի տարրերի՝ Պահանջներին և (կամ) անդամ պետության օրենսդրությանը համապատասխանության համատեղ ստուգումներ, ինչպես նաև համատեղ քննություն՝ կոնֆլիկտային իրավիճակներ առաջանալու դեպքում։

\_\_\_\_\_\_\_\_\_\_\_\_\_