

# Հայաստանի Հանրապետության կենտրոնական բանկի խորհրդի 2013 թվականի հուլիսի 9-ի թիվ 173-Ն որոշման մեջ փոփոխություններ և լրացումներ կատարելու մասին

2017-03-17

Հայաստանի Հանրապետության  
կենտրոնական բանկի խորհուրդ

Որոշում թիվ 66-Ն

17.03.2017

Հայաստանի Հանրապետության կենտրոնական բանկի խորհրդի 2013 թվականի  
հուլիսի 9-ի թիվ 173-Ն որոշման մեջ փոփոխություններ և լրացումներ կատարելու  
մասին

Հրապարակման ամսաթիվ՝ 18.04.2017

Նպատակ ունենալով կատարելագործել Հայաստանի Հանրապետության տարածքում  
գործող բանկերի տեղեկատվական անվտանգության կառավարման  
համակարգը, *հիմք ընդունելով* «Հայաստանի Հանրապետության կենտրոնական  
բանկի մասին» Հայաստանի Հանրապետության օրենքի 20-րդ հոդվածի «ե», «իբ» և  
«իդ» կետերը, «Արժեթղթերի շուկայի մասին» Հայաստանի Հանրապետության օրենքի  
111-րդ հոդվածի 2-րդ մասը, 181-րդ հոդվածի 1-ին մասը, «Վարկային  
տեղեկատվության շրջանառության և վարկային բյուրոների գործունեության մասին»  
Հայաստանի Հանրապետության օրենքի 5-րդ հոդվածի 2-րդ մասի 4-րդ կետը,  
«Ապահովագրության և ապահովագրական գործունեության մասին» Հայաստանի  
Հանրապետության օրենքի 37-րդ հոդվածի 10-րդ մասի 4-րդ կետը, *դեկլարվելով*  
«Իրավական ակտերի մասին» Հայաստանի Հանրապետության օրենքի 16-րդ  
հոդվածով և 70-րդ հոդվածի 1-ին մասով՝ Հայաստանի Հանրապետության  
կենտրոնական բանկի խորհուրդը

Ո Ր Ո Շ Ո Ւ Մ Է.

1. Հայաստանի Հանրապետության կենտրոնական բանկի խորհրդի 2013 թվականի հուլիսի 9-ի ««Տեղեկատվական անվտանգության ապահովման նվազագույն պահանջների սահմանման վերաբերյալ կարգը» հաստատելու մասին» թիվ 173-Ն որոշմամբ հաստատված «Տեղեկատվական անվտանգության ապահովման նվազագույն պահանջների սահմանման վերաբերյալ կարգում» (այսուհետ՝ Կարգ) կատարել հետևյալ փոփոխությունները և լրացումները.

1) Կարգի 4-րդ կետի 4-րդ ենթակետում «ՀՀ տարածքում գործող բանկերը» բառերից հետո լրացնել «(այսուհետ՝ նաև բանկ)» բառերը,

2) Կարգի 4-րդ կետը 27-րդ ենթակետից հետո լրացնել հետևյալ բովանդակությամբ 28-37-րդ ենթակետերով.

«28) Ներքին ռիսկ՝ ներքին տեղեկատվական ցանցի օգտագործողի կողմից ոչ միտումնավոր (սխալմամբ, պատահական, չմտածված, ոչ չարամիտ, ոչ շահադիտական նպատակներով, օրինակ՝ անփութության կամ անտեղյակ լինելու պատճառով, հետաքրքրությունից ելնելով կամ այլ կերպ կատարված) և միտումնավոր (շահադիտական նպատակներով, երրորդ անձանց դրդմամբ, չարամտորեն կամ այլ կերպ կատարված) գործողությունների հետևանքով առաջացող հնարավոր ռիսկերը Կազմակերպության տեղեկատվական անվտանգության համար:

29) Արտաքին ռիսկ՝ Կազմակերպության աշխատակից չհամարվող անձանց միտումնավոր և ոչ միտումնավոր գործողությունների հետևանքով առաջացող հնարավոր ռիսկերը Կազմակերպության տեղեկատվական անվտանգության համար, ինչպես նաև այն ռիսկերը, որոնք չեն կարող կառավարվել Կազմակերպության կարգավորող փաստաթղթերով:

30) Ներքին ներթափանցման թեստ (Internal network penetration testing)՝ միջոցառումների ամբողջություն, որն ուղղված է ստուգելու Կազմակերպության ներքին տեղեկատվական ցանցի պաշտպանվածությունը ներքին ռիսկերից:

31) Արտաքին ներթափանցման թեստ (External network penetration testing)՝ միջոցառումների ամբողջություն, որն ուղղված է ստուգելու Կազմակերպության ներքին տեղեկատվական ցանցի պաշտպանվածությունը արտաքին ռիսկերից:

32) Սոցիալական ինժինիրինգ (Social engineering)՝ ներքին տեղեկատվական ցանցի լիազորված օգտագործողին մոլորեցնելու ճանապարհով գաղտնի տեղեկատվության ձեռքբերում:

33) Բարձր վտանգ պարունակող կայուն սպառնալիք (Advanced persistent threat - APT)՝ ցանցային գրոհ, որի ժամանակ չլիազորված անձը ձեռք է բերում հասանելիություն Կազմակերպության ներքին տեղեկատվական ցանցին և որոշակի ժամանակ մնում է չհայտնաբերված:

34) Բարձր վտանգ պարունակող կայուն սպառնալիքի թեստ (Advanced persistent threat test - APT, Red-teaming)՝ առկա բոլոր պաշտպանական միջոցների (այդ թվում՝ կազմակերպչական) արդյունավետությունը ստուգելու նպատակով իրականացվող արտոնված գրոհ:

35) Բարձր վտանգ պարունակող կայուն սպառնալիքի առկայության թեստ (APT hunting exercise)՝ մինչև մեկ շաբաթ տևողությամբ առավել կրիտիկական սերվերների և աշխատակայանների ուղղությամբ ցանցային հոսքի վերլուծության միջոցով Կազմակերպության ենթակառուցվածքում արդեն իսկ հաջողված բարձր վտանգ պարունակող կայուն սպառնալիքի գրոհի դրսևորման բացահայտում:

36) Ներքին տեղեկատվական ցանցի խոցելիության սքանավորում (զննում)՝ խոցելիության զննիչների կիրառմամբ կատարվող սերվերների, աշխատակայանների, ցանցային սարքավորումների, ինչպես նաև ներքին տեղեկատվական ցանցի այլ ակտիվների ծրագրային և (կամ) տեխնիկական ապահովման մեջ չարտոնված մուտքի պոտենցիալ հնարավորությունն ընձեռող անվտանգության բացերի հայտնաբերում:

37) Խոցելիության զննիչ՝ ծրագրային և (կամ) տեխնիկական ապահովման խոցելիությունների հայտնաբերման հատուկ համակարգ:»,

3) Կարգի 16-րդ կետը շարադրել հետևյալ խմբագրությամբ.

«16. Տեղեկատվական անվտանգության ապահովման համար մշակվող կանոնակարգերով, կարգերով և (կամ) կանոններով պետք է սահմանվեն այն խնդիրները, գործընթացները և միջոցառումները, որոնք ուղղված են Կազմակերպության կողմից տեղեկատվական ռեսուրսների պաշտպանության ապահովման նպատակների իրականացմանը: Նշված կանոնակարգող փաստաթղթերը մշակելիս, Կազմակերպությունը պետք է հաշվի առնի, որ տեղեկատվության անվտանգության ապահովման համար սահմանվող բոլոր միջոցների, միջոցառումների և պահանջների վերջնական նպատակն է տեղեկատվական հարաբերությունների սուբյեկտների պաշտպանության ապահովումը հնարավոր նյութական և ոչ նյութական վնասներից, որոնք կարող են առաջանալ Կազմակերպության տեխնիկա-ծրագրային համակարգերում շրջանառվող տեղեկատվության գործունեության ընթացքի մեջ ոչ միտումնավոր կամ միտումնավոր ներխուժման, ինչպես նաև՝ Կազմակերպության սեփական աշխատակիցներին (ինչպես նաև Կազմակերպությանը ծառայություններ մատուցող այլ ընկերությունների աշխատակիցներին) հայտնի դարձած դասակարգված տեղեկատվության ոչ միտումնավոր կամ միտումնավոր բացահայտման արդյունքում:»,

4) Կարգի 17-րդ կետը շարադրել հետևյալ խմբագրությամբ.

«17. Մարդկային գործոնը մեծ դեր է խաղում Կազմակերպության տեղեկատվական անվտանգության ապահովման գործընթացում, և առաջին հերթին պետք է կանոնակարգվեն տեղեկատվության հասանելիության հետ կապված խնդիրները: Կանոնակարգերով, կարգերով և (կամ) կանոններով պետք է սահմանվեն տեղեկատվական ռեսուրսների դասակարգման (գաղտնիության մակարդակները, գաղտնի համարվող տեղեկատվության բնութագրիչները) և դրանց նկատմամբ հասանելիության իրավասությունների տրամադրման սկզբունքները: Տեղեկատվության հասանելիության սկզբունքները պետք է կառուցվեն՝ հաշվի առնելով օգտագործողների բնութագրիչները, տեղեկատվական ռեսուրսի

բնութագրիչները, ինչպես նաև այլ բնութագրիչներ, ինչպիսիք են՝ ամիս-ամսաթիվ, աշխատանքային ժամեր, հասանելիության միջոցներ և այլն:»,

5) Կարգի 18-րդ կետում՝

ա.«17-րդ կետի 6-րդ ենթակետում» բառերը փոխարինել «17-րդ կետում» բառերով,  
բ. 2-րդ ենթակետում «Օբյեկտների բնութագրիչներ» բառերից հետո լրացնել «(տեղեկատվական ռեսուրսների բնութագրիչներ)» բառերը,

6) Կարգի 19-րդ կետում՝

ա. 46-րդ ենթակետն ուժը կորցրած ճանաչել,

բ. 47-րդ ենթակետը շարադրել հետևյալ խմբագրությամբ.

«Կազմակերպության կողմից կիրառվող թղթային գրանցամատյանների վարման ընթացակարգեր:»,

7) Կարգի 19-րդ կետից հետո լրացնել հետևյալ բովանդակությամբ 19.1-րդ և 19.2-րդ կետերը.

«19.1. Սույն կարգով սահմանված նվազագույն պայմաններից բխող բոլոր միջոցառումների իրականացման արդյունքներով պետք է կազմվեն արձանագրություններ, որոնցում պետք է նշվեն՝

1) միջոցառման տեսակը,

2) միջոցառման մասնակիցների տվյալները,

3) միջոցառման անցկացման վայրը,

4) միջոցառման անցկացման ամիս-ամսաթիվն ու ժամը,

5) պատասխանատու աշխատակիցների տվյալները,

6) միջոցառման ղեկավարի տվյալները,

7) եզրակացությունը (կարծիքը), բոլոր մասնակիցների ստորագրությունները:

19.2. Կազմակերպությունում վարվող թղթային գրանցամատյանները պետք է առնվազն.

1) լինեն էջանշված,

2) տողերը լինեն համարակալված,

3) գրանցամատյանի վարման սկզբի ամսաթիվը լինի նշված,

4) նշված լինի առարկան՝ ինչի համար վարվում է գրանցամատյանը,

5) առկա լինեն ընդունողի և հանձնողի ստորագրությունները,

6) առկա լինեն ընդունման և հանձնման ամսաթվերը,

7) պարունակի մատյանը վարողի տվյալները և գտնվելու վայրը:»,

8) Կարգի Գլուխ 8-ի վերնագիրը շարադրել հետևյալ խմբագրությամբ.

«Գլուխ 8. Գործարար գործընթացների անընդհատության ապահովում և թեստավորման կազմակերպում»,

9) Կարգի Գլուխ 8-ը 20-րդ կետից հետո լրացնել հետևյալ բովանդակությամբ 20.1-20.7-րդ կետերով.

«20.1. Բանկերի ներքին տեղեկատվական ցանցի թեստավորումն առնվազն պետք է ներառի.

1) ներքին ներթափանցման թեստ,

2) արտաքին ներթափանցման թեստ,

3) սոցիալական ինժինիրինգի ռիսկի գնահատում,

4) բարձր վտանգ պարունակող կայուն սպառնալիքի առկայության թեստ:

20.2. Կարգի 20.1-րդ կետով նախատեսված թեստավորումը պետք է իրականացվի սույն Կարգի 20.3-րդ կետի պահանջներին բավարարող անկախ թեստավորում իրականացնող ընկերության կողմից: Ընդ որում՝ բանկերը պետք է Կենտրոնական բանկ ներկայացնեն 20.3-րդ կետով սահմանված պահանջներին բավարարելու փաստը հավաստող համապատասխան փաստաթղթեր, ինչպես նաև՝ թեստավորման արդյունքները և (կամ) թեստավորում իրականացրած ընկերության եզրակացությունը:

20.3. Թեստավորում իրականացնող ընկերությունը պետք է.

1) լինի ԶՐԵՍԹ Ինթերնեյշնլ (CREST International) կազմակերպության անդամ,

2) ունենա այդ ոլորտում առնվազն 3 տարվա փորձ,

3) 20.1-րդ կետով սահմանված թեստերը իրականացրած լինի ՀՀ տարածքից դուրս իր չափերով պատվիրող բանկին համադրելի առնվազն 5 ֆինանսական կազմակերպություններում:

20.4. Կարգի 20.1-րդ կետի 1-3-րդ ենթակետերով սահմանված միջոցառումները պետք է իրականացվեն առնվազն տարին մեկ անգամ:

20.5. Կարգի 20.1-րդ կետի 4-րդ ենթակետով նախատեսված միջոցառումը պետք է իրականացվի առնվազն տարին երկու անգամ:

20.6. Բանկերը պետք է իրականացնեն ներքին տեղեկատվական ցանցի խոցելիության սքանավորում առնվազն եռամսյակը մեկ անգամ:

20.7. Ներքին տեղեկատվական ցանցի թեստավորումը սույն կարգի պահանջներին համապատասխան չիրականացնելու դեպքում, Կենտրոնական բանկը իրավասու է ընտրել թեստավորում իրականացնող ընկերություն, որը կիրականացնի բանկի ներքին տեղեկատվական ցանցի թեստավորումը, որի դիմաց ամբողջական վճարումը պետք է իրականացնի բանկը:»,

10) Կարգի 39-րդ կետի 1-ին և 2-րդ ենթակետերը ուժը կորցրած ճանաչել,

11) Կարգի 62-րդ կետը շարադրել հետևյալ խմբագրությամբ.

«62. Կազմակերպության կողմից առնվազն գաղտնի և հույժ գաղտնի (կրիտիկական) դասակարգված էլեկտրոնային տեղեկատվությունը պետք է պահպանվի առնվազն գաղտնագրված եղանակով:»,

12) Կարգի 80-րդ կետի 9-րդ ենթակետում «գրքեր» բառը փոխարինել «ձեռնարկներ» բառով,

13) Կարգի 87-րդ կետի 8-րդ ենթակետը շարադրել հետևյալ խմբագրությամբ.

«8) ունենա սերվերային սենյակի մուտքի/ելքի գրանցման համակարգ (առնվազն պետք է գրանցվի մուտք/ելք գործողի անուն-ազգանունը, մուտքի/ելքի ժամը և ամսաթիվը),»:

2. Սույն որոշումն ուժի մեջ է մտնում պաշտոնական հրապարակման օրվան հաջորդող

տասներորդ օրը:

Հայաստանի Հանրապետության  
կենտրոնական բանկի նախագահի տեղակալ

Ներսես Երիցյան

2017 թ. մարտի 23  
Երևան