

Հայաստանի Հանրապետության
Կենտրոնական բանկի խորհուրդ

Որոշում թիվ --Ն

--/-- 2007

**«SS ՌԻՍԿԻ ԿԱՌԱՎԱՐՄԱՆ ԵՎ ՆԵՐՔԻՆ ՀՄԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ
ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋՆԵՐ»-Ը ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ**

Հիմք ընդունելով «Հայաստանի Հանրապետության կենտրոնական բանկի մասին» Հայաստանի Հանրապետության օրենքի 20-րդ հոդվածի «իբ» կետի դրույթները՝ Հայաստանի Հանրապետության կենտրոնական բանկի խորհուրդը որոշում է.

1. Հաստատել «SS Ռիսկի կառավարման և ներքին հսկողության իրականացման նվազագույն պահանջները» կարգը՝ համաձայն հավելված 1-ի (կցվում է):
2. Սույն որոշումը ուժի մեջ է մտնում պաշտոնական հրապարակման օրվանից վեց ամիս հետո:
3. Սույն որոշումն ուժի մեջ մտնելու պահից ուժը կորցրած ճանաչել Հայաստանի Հանրապետության կենտրոնական բանկի խորհրդի 1999 թվականի մարտի 16-ի ««Հայաստանի Հանրապետության բանկային համակարգում գործառնական ռիսկերի կառավարումը» նվազագույն պարտադիր պահանջները կից ժամանակացույցով հաստատելու մասին» թիվ 40 որոշումը:

Հայաստանի Հանրապետության
Կենտրոնական բանկի նախագահ
Տ.Սարգսյան

SS Ռ-իսկի կառավարման և ներքին հսկողության իրականացման նվազագույն պահանջներ

ԳԼՈՒԽ 1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. Սույն որոշմամբ սահմանվում են Հայաստանի Հանրապետությունում գործող բոլոր ֆինանսական կազմակերպությունների Տեղեկատվական Տեխնոլոգիաների ռիսկի կառավարման և ներքին հսկողության նվազագույն պահանջները:

2. Բանկերի համար նվազագույն հսկողության իրականացման նվազագույն պահանջներ հաղիսանում են.

- 1) տեղեկատվության անվտանգության քաղաքականություն,
- 2) «Աուքսորսինգ» պայմանագրեր,
- 3) ֆիզիկական և միջավայրի անվտանգություն,
- 4) կոմունիկացիայի և գործունեության կառավարում,
- 5) մուտքի հսկում,
- 6) համակարգի մշակման և սպասարկման գործընթացների անվտանգություն,
- 7) բիզնեսի շարունակելիության կառավարում:

3. Ֆինանսական կազմակերպությունների (բացառությամբ բանկերի) նկատմամբ սույն որոշմամբ հաստատված նվազագույն հսկողության իրականացման պահանջներից յուրաքանչյուրը կիրառվում է այն պահից, երբ ֆինանսական կազմակերպությունն իր նախաձեռնությամբ օգտագործում է սույն որոշմամբ հաստատված նվազագույն հսկողության իրականացման պահանջներում ներառված գործիքները և/կամ ֆինանսական կազմակերպության գործունեության իրականացման կապակցությամբ կիրառվող պարագաները:

4. Սույն կարգում օգտագործվող հիմնական հասկացություններն են.

1) Ֆինանսական կազմակերպություն - բանկեր, ապահովագրական ընկերություններ, վարկային կազմակերպություններ, վճարային գործիքների և վճարահաշվարկային փաստաթղթերի պրոցեսինգ և քլիրինգ իրականացնող կազմակերպություններ, դրամական (փողային) փոխանցումներ իրականացնող կազմակերպություններ և նշված կազմակերպությունների բոլոր մասնաճյուղերն ու ներկայացուցչությունները:

2) Բանկային ծրագրային ապահովում – ֆինանսական միջոցների փոխանցման, կառավարման և/կամ այլ գործողություններ կատարող ծրագրային ապահովում, որոնք կիրառվում են ֆինանսական կազմակերպության կողմից, օրինակ՝ «Գործառնական Օր», և այլ համարժեք ծրագրային ապահովման միջոցներ:

3) Ցանցի տեր – ֆինանսական կազմակերպության ղեկավարության կողմից նշանակված աշխատակից, որը պատասխանատվություն է կրում ցանցի, նրա ֆիզիկական ու տեսական անվտանգության և ամբողջականության համար:

4) Աշխատանքային արխիվ - համակարգում շրջաբերվող տեղեկատվության ընթացիկ կարգավիճակն արտահայտող տեղեկությունների շտեմարան, որը պարունակում է անհրաժեշտ տեղեկություններ՝ համակարգի ընթացիկ աշխատանքին հետևելու և համակարգի ընթացիկ աշխատանքը կազմակերպելու համար:

5) Պարբերական արխիվ - համակարգի աշխատանքն արձանագրող մատյանի և համակարգում մշակվող տեղեկությունների կրկնօրինակում, որը կոչված է գրանցված տեղեկատվությունը կարճ ժամանակահատվածում հասանելի դարձնելու համապատասխան իրավասություններ ունեցող

օգտագործողներին, անհրաժեշտության դեպքում՝ նաև հնարավորություն ընձեռելու վերականգնել աշխատանքային արխիվը (վերջինիս խափանման, կորստի կամ այլ նման դեպքերում):

6) Երկարատև պահպանման արխիվ - աշխատանքային կամ պարբերական արխիվների, համակարգի աշխատանքն արձանագրող մատյանի և համակարգում մշակվող ու որոշակի ժամանակահատվածին վերաբերվող բոլոր տեղեկությունները պարունակող տեղեկատվական բազա:

7) «տաք» ռեգերվ - պահուստ, որի վերականգնումը կատարվում է ռեալ ժամանակում:

8) «սառը» ռեգերվ – պահուստ, որի վերականգնումը կատարվում է որոշակի ժամանակահատվածում:

9) «Աութոփսինգ» - կազմակերպության ներքին աշխատանքների (օրինակ՝ ծրագրային ապահովման մշակման, ցանցի և/կամ սերվերների սպասարկման և այլն) կատարման համար մեկ այլ կազմակերպության ռեսուրսների օգտագործում:

ԳԼՈՒԽ 2. ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՍԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

5. Ֆինանսական կազմակերպության կողմից տեղեկատվության անվտանգության քաղաքականության պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից տեղեկատվության անվտանգության փաստաթղթի, ինչպես նաև դիտարկման և գնահատման պահանջներին ներկայացվող պայմանների կատարմամբ: Ֆինանսական կազմակերպության կողմից տեղեկատվության անվտանգության քաղաքականության պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

6. Տեղեկատվության անվտանգության փաստաթղթին ներկայացվող պայմաններն են.

1) ֆինանսական կազմակերպությունում տեղեկատվության անվտանգության փաստաթղթավորված քաղաքականության և տեղեկատվական համակարգերում առկա ռիսկերի կարգավորման կարգի առկայությունը,

2) կազմակերպության կողմից մշակված և ընդունված արտակարգ իրավիճակներում գործողությունների ծրագրի առկայությունը, որում պետք է՝

ա. արտակարգ իրավիճակները դասակարգված լինեն ըստ իրենց հավանական վնասի չափի, ներդրված համակարգերը դասակարգված լինեն ըստ կարևորության: Ֆինանսական կազմակերպությունը պարբերաբար իրականացնում է նկարագրված արտակարգ իրավիճակների հետևանքների կանխարգելմանը և վերացմանն ուղղված գործողությունների իրականացման փորձնական ծրագրեր և միջոցառումներ առնվազն երեք տարին մեկ կամ նոր գործողության ծրագրի մշակման դեպքում՝ հաշվարկելու արտակարգ իրավիճակի ի հայտ գալու դեպքում դրա հետևանքների կանխարգելման ու վերացման համար անհրաժեշտ ժամանակը և ռեսուրսները, իսկ դրանց արդյունքները փաստաթղթավորվում են,

բ. նշվեն բոլոր պատասխանատուները:

7. Ցանցերի վերաբերյալ փաստաթղթերը ներառում են՝

1) ցանցի կառուցվածքը, ներառյալ՝ բոլոր հանգույցներն ու կապերը,

2) ցանցի ճարտարապետությունը, գծապատկերները,

3) կապի սարքավորումները, ծրագրային փաթեթները, նպատակն ու մատուցվող ծառայությունները,

4) ներքին լարանցումները:

8. Սույն կարգի 6-րդ և 7-րդ կետերում նշված փաստաթղթերը պետք է հասանելի լինեն միայն արտոնագրված օգտագործողներին: Սույն կետում նշված փաստաթղթերը հաստատվում, քարմացվում և վերահսկվում են ցանցի տիրոջ կողմից:

9. Դիտարկման և գնահատմանը ներկայացվող պայմաններն են.

1) ֆինանսական կազմակերպության ներքին աուդիտի կազմում տեղեկատվական տեխնոլոգիաների աուդիտով զբաղվող աշխատակցի առկայությունը կամ ֆինանսական կազմակերպության տեղեկատվական տեխնոլոգիաների աուդիտի իրականացումն այլ կազմակերպության կողմից՝ «աութօրսինգ» պայմանագրային հիմունքներով,

2) ֆինանսական կազմակերպությունում առանձին անվտանգության պատասխանատուի հաստիքի առկայությունը և համալրվածությունը:

ԳԼՈՒԽ 3. «ԱՌԻԹՍՈՐՄԻՆԳ» ՊԱՅՄԱՆԱԳՐԵՐԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՄԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

10. «Աութօրսինգ» պայմանագրերի պահանջին ներկայացվում են հետևյալ պայմանները.

1) ծրագրային ապահովումը մշակող և /կամ/ սպասարկող կազմակերպության հետ կնքվող պայմանագրում այնպիսի դրույթի առկայությունը, որը սահմանում է համակարգի սպասարկման պարտավորություններից հրաժարվելու դեպքում ֆինանսական կազմակերպությանը տեղեկացնելու նվազագույն ժամանակահատվածը, բայց ոչ պակաս, քան 3 ամիս:

2) պայմանագրում այնպիսի դրույթի առկայությունը, որը թույլ կտա ապահովել ֆինանսական կազմակերպությանը ծրագրային տեքստերի հասանելիությունը որոշակի դեպքերում, օրինակ՝ պայմանագրի լուծում մշակող և /կամ/ սպասարկող կազմակերպության հետ կամ սպասարկող կազմակերպության լուծարում,

3) մշակող կազմակերպության կողմից ցանկացած անձնական օգտագործման “բեքդոր”-ի, այսինքն՝ համակարգ մուտք գործելու հեռահար աշխատակայանից կամայական նպատակով մուտքի հնարավորություն ծրագրային համակարգ, արգելումը,

4) ծրագրային ապահովման միջոցով մեկ աշխատակցի կողմից կամայական ֆինանսական գործողության սկզբից մինչև վերջ կատարման անթույլատրելիությունը,

5) համակարգը մշակող կազմակերպության ստեղծած գլխավոր ադմինիստրատորի գաղտնաբառի փոփոխումը և փակ ծրարի միջոցով ֆինանսական կազմակերպության գլխավոր տնօրենին փոփոխված գաղտնաբառի հանձնումը վերջնական գործարկումից և ծրագրի ընդունման-հանձնման ակտը ստորագրելուց անմիջապես հետո:

11. Ֆինանսական կազմակերպության կողմից «Աութօրսինգ» պայմանագրերի պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

ԳԼՈՒԽ 4. ՖԻԶԻԿԱԿԱՆ ԵՎ ՍԻԶԱՎԱՅՐԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՄԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

12. Ֆինանսական կազմակերպության կողմից ֆիզիկական և միջավայրի անվտանգության պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից անվտանգության գոտիների և

սարքավորումների անվտանգության պահանջներին ներկայացվող պայմանների կատարմամբ: Ֆինանսական կազմակերպության կողմից ֆիզիկական և միջավայրի անվտանգության պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

13. Ֆինանսական կազմակերպության կողմից անվտանգության գոտիների պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից ֆիզիկական անվտանգության սահմանների, ֆիզիկական մուտքի կարգավորման, սենյակների և սարքավորումների անվտանգության ապահովման պահանջներին ներկայացվող պայմանների կատարմամբ:

14. Անվտանգության գոտիների ֆիզիկական անվտանգության սահմանների պահանջին ներկայացվում են հետևյալ պայմանները.

1) անվտանգության գոտիների ֆիզիկական պաշտպանության իրականացումը ինչպես ֆիզիկական, այնպես էլ էլեկտրոնային (ծրագրային միջոցներով) սահմանափակման և /կամ/ դրանց համադրությունների միջոցով: Դրանք են.

ա. առանձնացված սենյակները՝ չարտոնված անձանց մուտքի արգելմամբ,

բ. համակարգիչների մուտքը սահմանափակող սարքերը,

գ. համակարգ մուտքը սահմանափակող գաղտնագրերը,

դ. էլեկտրոնային թվային ստորագրությունը,

ե. անհաջող փորձերի գրանցամատյանները (log ֆայլը), որոնք գրանցվում և ստուգվում են:

զ. գաղտնի տեղեկատվության ծածկագրման տեխնիկան,

է. գաղտնի տեղեկատվության տարածումը կանխելու նպատակով ազատ մուտքի համար սահմանափակ սենյակներ և տեղեկատվական համակարգ մուտք գործելու կապակցությամբ ֆինանսական կազմակերպության աշխատողներին վերապահված իրավասությունները պարբերաբար դիտարկվում են և անհրաժեշտության դեպքում՝ փոփոխվում:

15. Անվտանգության գոտիների ֆիզիկական մուտքի կարգավորման պահանջին ներկայացվում են հետևյալ պայմանները.

1) բոլոր արտաքին մուտքերի պաշտպանվածությունն անօրինական մուտքերից, օրինակ՝ կիրառելով մուտքի կառավարման մեխանիզմներ, երկաթյա ճաղեր, ձայնաազդանշանային համակարգեր և այլն, բոլոր արտաքին դռների անվտանգության ձայնային համակարգի առկայությունը, իսկ գաղտնի սենյակների դռների համար՝ նաև ավտոմատ փակման հնարավորության առկայություն: Մուտքի և շարժման տվիչները պարբերաբար՝ առնվազն տարին մեկ կամ նոր տվիչների տեղադրման դեպքում, ստուգվում են, տեղադրվում այնպես, որ ընդգրկեն բոլոր պատուհաններ և դռները,

2) սահմանված լիազորություններ չունեցող անձանց մուտքի սահմանափակումը դեպի համակարգիչներ և կապի միջոցներ:

16. Անվտանգության գոտիների սենյակների և սարքավորումների անվտանգության ապահովման պահանջին ներկայացվում են հետևյալ պայմանները.

1) ֆինանսական կազմակերպությունում սերվերների և ցանցային սարքավորումների տեղադրման առանձնացված տարածքների առկայությունը: Տարածքները պետք է պաշտպանված լինեն տարբեր տեսակի աղետներից, օրինակ՝ հրդեհ, ջրամատակարարման համակարգի վթար և այլն,

2) սերվերային սենյակներում՝ նաև ջերմության կարգավորիչ որևէ համակարգի առկայությունը, որը սենյակի ջերմաստիճանը կպահի՝ համաձայն տվյալ համակարգչի սարքինության ապահովման համար

իրավական ակտերով, տեխնիկական անձնագրերով կամ այլ փաստաթղթերով նախատեսված նորմերի,

3) առնվազն տարին մեկ անգամ տեխնիկական սարքավորումների աշխատունակության ստուգումը, ամբողջ գործընթացի փաստաթղթավորումը, ընթացակարգի մշակումը, որտեղ մանրամասն նկարագրվում են ներդրված յուրաքանչյուր ծրագրի վերաբերյալ տեստավորման ժամկետները, պարբերականությունը, պատասխանատուները, տեստավորման արդյունքների արձանագրումը,

4) բոլոր սարքավորումների հողանցումը,

5) ցանցային սարքավորումների ֆիզիկական անվտանգությունն ապահովելու նպատակով դրանց ոչ տեսանելի տեղայնացման կատարումը, կապուղու ֆիզիկապես պաշտպանումը, միացման կետերի կողպումը, երկրորդային երթուղիչի (routing) կազմակերպումը, մարդաշատ վայրերում չտեղայնացումը:

17. Որպես սարքավորումների անվտանգության պահանջին ներկայացվող պայման՝ ֆինանսական կազմակերպությունում ապահովվում է սերվերների և ցանցային սարքավորումների անխափան էլեկտրասնուցումը: Անխափան սնուցման աղբյուրներ պետք է ունենան առնվազն այն համակարգիչները, որոնք ապահովում են ֆինանսական կազմակերպության աշխատանքի անընդհատությունը: Ֆինանսական կազմակերպությունում ապահովվում է անխափան սնուցման սարքերի կիրառումն այնպես, որ այն հնարավորություն ընձեռի էլեկտրասնուցման անջատման դեպքում շարունակել աշխատանքը 10-20 րոպեի ընթացքում և սահմանված ձևով անջատել համակարգիչները: Այն դեպքում, երբ ֆինանսական կազմակերպության ավտոմատացված համակարգի աշխատանքը պահանջվում է էլեկտրասնուցման երկարատև անջատման ժամանակ (30 րոպեից ավելի), ֆինանսական կազմակերպությունն ապահովվում է էլեկտրասնուցում գեներատոր-շարժիչի, արևային մարտկոցի կամ այլ տեխնիկական միջոցի օգնությամբ, որը կգործարկվի 10-15 րոպեի ընթացքում:

ԳԼՈՒԽ 5. ԿՈՄՈՒՆԻԿԱՑԻԱՅԻ ԵՎ ԳՈՐԾՈՒՆԵՈՒԹՅԱՆ ԿԱՌԱՎԱՐՈՒՄԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՍԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

18. Ֆինանսական կազմակերպության կողմից կոմունիկացիայի և գործունեության կառավարման պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից գործառնական գործընթացների և պատասխանատվության, արխիվացման, ցանցի կառավարման, կրիչների հետ աշխատանքի ու անվտանգության, տեղեկատվության և ծրագրային ապահովման փոխանակման պահանջներին ներկայացվող պայմանների կատարմամբ: Ֆինանսական կազմակերպության կողմից կոմունիկացիայի և գործունեության կառավարման պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

19. Որպես գործառնական գործընթացների և պատասխանատվության պահանջին ներկայացվող պայման՝ ֆինանսական կազմակերպությունում ստեղծվում են օգտագործվող հիմնական սերվերների կրկնօրինակներ՝ ռեզերվային սերվերներ («տաք»/«սառը» ռեզերվներ), որոնք յուրաքանչյուր պահի կարող են փոխարինել հիմնականին և ապահովել սարքավորումների ֆիզիկական խափանման հետևանքով ֆինանսական կազմակերպության աշխատանքի անընդհատությունը: Այս պահանջն ապահովելու համար կազմակերպությունում ապահովվում է՝

1) նույնպիսի կոնֆիգուրացիայով համակարգչի առկայությունը, ինչպիսին է հիմնական սերվերը, որպեսզի այն ի վիճակի լինի արտակարգ իրավիճակներում կատարել հիմնական սերվերի աշխատանքը,

2) ֆինանսական կազմակերպության կողմից սերվերների վերականգնման մեթոդների՝ «տաք» կամ «սառը», հարցի ինքնուրույն լուծումը՝ ելնելով սերվերների վերականգնման ժամանակային պահանջներից,

3) հիմնական սերվերների օգտագործման, տեստավորման և վերականգնման ընթացակարգերի առկայությունը, որտեղ հստակ նշվում են պատասխանատուները, տեստավորման պարբերականությունը, սերվերի ռեգերվի տեսակը («տաք» կամ «սառը»), տեստավորված վերականգնման ժամանակը:

20. Արխիվացման (HOUSEKEEPING) պահանջին ներկայացվում են հետևյալ պայմանները.

1) ֆինանսական կազմակերպության կողմից գործող բոլոր ծրագրային համակարգերում արխիվների վարման հնարավորության ապահովվումը արխիվացման երեք եղանակներով՝ աշխատանքային, պարբերական, երկարատև պահպանման,

2) արխիվների պաշտպանվածության համապատասխան մակարդակի ապահովվումը՝ կախված նրանցում պահպանվող տեղեկատվության գաղտնիության աստիճանից,

3) արխիվների վարումն առանձին կրիչների կամ, հնարավորության դեպքում, համակարգչի վրա (ոչ այն համակարգչի, որի վրա տեղադրված է և աշխատում է տվյալ ծրագիրը)՝ ելնելով անվտանգության պահանջներից: Այս գործողություններն իրականացնելու նպատակով յուրաքանչյուր ֆինանսական կազմակերպությունում ապահովվում է արխիվների հետ կապված գործողությունները կանոնակարգող փաստաթղթերի առկայությունը, որոնց մեջ նկարագրվում են՝

ա. արխիվներում ընդգրկված տվյալների պահպանման ժամկետները,

բ. արխիվներում ընդգրկված տվյալների պաշտպանության միջոցները (հսկիչ գումար, էլեկտրոնային ստորագրություն, ծածկագրում),

գ. աշխատանքային արխիվի արխիվացման (back up) պարբերականությունը, արխիվացման կարգը,

դ. կրիչների ցանկը, որի վրա կազմակերպվում է պահպանությունը (մագնիսական սկավառակներ, ստրիմերներ, կոշտ սկավառակներ), պահպանման տեղը, ձևը, դրանց վերաբերյալ արարողակարգերը,

ե. արխիվների նկատմամբ համապատասխան աշխատակիցների իրավասությունների ցանկը,

զ. իրավասու օգտագործողների ցանկը՝ հաստատված գլխավոր տնօրենի կողմից,

է. պարբերական արխիվներից տեղեկատվության վերականգնման կարգը: Կարգում հստակ նկարագրվում են դեպքերը, որոնց ժամանակ կատարվում են տեղեկատվության վերականգնումը, վերականգնման եղանակները, օգտագործողները, որոնք ունեն համապատասխան իրավասություններ, ը. պահպանման արխիվների ստեղծման պարբերականությունը, նվազագույն ժամկետները, որոնց կտրվածքով աշխատանքային արխիվում պահվում է տեղեկատվությունը,

թ. արխիվային տվյալների երկարաժամկետ պահպանման կարգը, պահպանման եղանակը, միջոցները, պահպանման հետ կապված արարողակարգերի հստակ նկարագրությունը, արխիվներ մուտքի իրավունք ունեցող օգտագործողների ցանկը,

ժ. սույն կարգի 20-րդ կետի 1-3-րդ ենթակետերում նկարագրված բոլոր արարողակարգերը հստակ և մանրամասն նկարագրվում են համապատասխան փաստաթղթերում,

ժա. օգտագործված կոնֆիդենցիալ տվյալների (օրինակ՝ կողերի ցուցակների) կամ դրանց պատճենների օգտագործումից հետո ոչնչացումն ապահովելու համար համապատասխան ընթացակարգը:

21. Ցանցի կառավարման պահանջին ներկայացվում են հետևյալ պայմանները.

1) Ֆինանսական կազմակերպությունում ցանցային և համակարգերի ադմինիստրատորների բաժնի կամ խմբի (սովորաբար՝ բաղկացած 3-5 հոգուց) առկայությունը՝ ներքին և արտաքին ցանցերի, ինչպես նաև անհրաժեշտության դեպքում կիրառական համակարգերի շահագործման համար,

2) ադմինիստրատորի փոխարինողի ապահովվումը՝ ֆինանսական կազմակերպությունում գործող համակարգերի աշխատանքային անխափանությունը ապահովելու նպատակով հիմնական ադմինիստրատորի բացակայության դեպքում նրա ֆունկցիաները ստանձնելու համար: Համակարգի հիմնական ադմինիստրատորի բացակայության ժամանակ իրավասությունները տրամադրվում են այնպես, որ բացառվի այն ադմինիստրատորի իրավասությունների համատեղումը, որի վրա դրվել են հիմնական ադմինիստրատորի պարտականությունները,

3) ադմինիստրատորների հերթափոխային աշխատանքի ապահովվումը՝ ստանդարտ աշխատանքային օրվանից երկար աշխատող կիրառական ծրագրերի համար,

4) ցանցերը սպասարկող անձնակազմի կողմից համակարգի խափանման ռիսկը (անկախ նրանից, թե խափանումը եղել է կանխատեսված, թե պատահական) կանխելու կամ նվազեցնելու համար հետևյալ պայմանները.

ա. ցանցի ադմինիստրատորների և այն նախագծող անձանց պարտականությունների տարանջատումը,

բ. տեղեկատվության գաղտնիության ապահովման համաձայնագրի ստորագրումը ցանցում գրանցված, սպասարկող, նախագծող բոլոր անդամների հետ,

գ. մարդկային գործոնի նվազեցումը,

դ. աշխատանքների այնպիսի կազմակերպումը, որի դեպքում կնվազեցվի չարտոնված գործողությունների թիվը (օրինակ՝ իրավասությունների տարանջատում, գործողությունների գրանցում, վերահսկում և այլն),

ե. որպես ցանցային ադմինիստրատորներ՝ որակյալ և վստահելի մասնագետների, այսինքն՝ համապատասխան կրթությամբ, փորձով և գիտելիքներով, նշանակումը,

զ. ադմինիստրատորների կողմից ֆինանսական գործողությունների, գործարքներ կատարելու հնարավորությունների բացառումը,

5) Ցանցի այնպիսի կառուցվածքը, որը.

ա. կպարունակի առանձին ենթացանցեր կոնկրետ օգտագործողների կամ աշխատանքային խմբերի համար, պաշտպանված միջցանցային էկրաններով (firewall),

բ. չթույլատրի միջցանցային էկրանների (firewall) շրջանցումը,

գ. կարգավորի ցանց մուտք գործելու տեղերը,

դ. թույլատրի ամբողջությամբ ցանցի կառավարումը նախանշված վայրից,

ե. համապատասխանի նորմատիվ իրավական ակտերով և կազմակերպության ներքին իրավական ակտերով սահմանված կանոններին,

զ. չթույլատրի չարտոնագրված սարքերի միացումը (ցանցի ֆիզիկական մակարդակով),

է. ապահովի ցանցի կառավարման հաշվետվությունների և աուդիտորական դիտարկումների հնարավորությունների ակտիվացվածությունը:

22. Որպես կրիչների հետ աշխատանքի ու անվտանգության ապահովմանը համապատասխանության պայման ֆինանսական կազմակերպության կողմից մշակվում են արտաքին կրիչների օգտագործման հստակ կարգեր:

23. Տեղեկատվության և ծրագրային ապահովման փոխանակման պահանջին ներկայացվում են հետևյալ պայմանները.

- 1) ֆինանսական կազմակերպությունում էլեկտրոնային մամուլագրության առանձին սերվերի առկայությունը,
- 2) ֆինանսական կազմակերպությունում միջցանցային էկրանի (firewall) առկայությունը, որը կֆիլտրացնի և կհեռացնի բոլոր էլեկտրոնային մամուլները, որոնք ունեն անթույլատրելի և/կամ կասկածելի պարունակություն:

ԳԼՈՒԽ 6. ՄՈՒՏՔԻ ՀՍԿՈՒՄԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՍԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

24. Ֆինանսական կազմակերպության կողմից մուտքի հսկման պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից մուտքի հսկման գործառնական պահանջները, օգտագործողի մուտքի կառավարման, ցանցային մուտքի հսկման, օպերացիոն համակարգերի մուտքի հսկման, համակարգի մուտքի և օգտագործման մոնիտորինգի, շարժական և հեռահար աշխատանքների պահանջներին ներկայացվող պայմանների կատարմամբ: Ֆինանսական կազմակերպության կողմից մուտքի հսկման պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

25. Որպես մուտքի հսկման գործառնական պահանջներին ներկայացվող պայման՝ ֆինանսական կազմակերպությունում սահմանվում են հատուկ իրավունքներ ու իրավասություններ աշխատակիցների կողմից համակարգ մուտք գործելու համար՝ կախված յուրաքանչյուր աշխատակցի ֆունկցիոնալ պարտականություններից:

26. Ֆինանսական կազմակերպության կողմից մուտքի հսկման օգտագործողի մուտքի կառավարման պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից օգտագործողի գրանցման և օգտագործողի գաղտնաբառի կառավարման պահանջներին ներկայացվող պայմանների կատարմամբ:

27. Օգտագործողի մուտքի կառավարման օգտագործողի գրանցման պահանջին ներկայավում են հետևյալ պայմանները.

- 1) ֆինանսական կազմակերպությունում օգտագործողների գրանցման քաղաքականության առկայությունը՝ փաստաթղթավորված և հաստատված ղեկավարության կողմից: Օգտագործողների գրանցումն ու իրավասությունների տրամադրումն իրականացվում է՝ համաձայն իրենց աշխատատեղի նկարագրի, հնարավորության դեպքում՝ մեխանիկորեն,
- 2) օգտագործողի գրանցման ժամանակ տվյալների մուտքագրման երկակի վերահսկման մեխանիզմի (այսինքն՝ մուտքագրումը, ստուգումը և հաստատումը պետք է կատարվի առնվազն 2, հնարավորության դեպքում 3, աշխատակիցների կողմից) կիրառումը:

28. Որպես օգտագործողի գաղտնաբառի կառավարման պահանջ՝ ֆինանսական կազմակերպությունում ապահովվում է գաղտնաբառերի, գաղտնաբանալիների և էլեկտրոնային

նույնականացուցիչ ֆայլերի պահպանման և կառավարման քաղաքականության առկայությունը, որը պարունակում է՝

- 1) բարդ գաղտնաբառերի կիրառության պարտադիր պահանջ, այսինքն՝ գաղտնաբառը պետք է լինի առնվազն 4 նիշանոց, բաղկացած լինի տառերից, թվերից, չպարունակի անձնական տվյալներ,
- 2) գաղտնաբառերի պահպանման պահանջներ,
- 3) գաղտնաբառերի փոփոխության պահանջներ,
- 4) էլեկտրոնային նույնականացուցիչ ֆայլերի օգտագործման պահանջներ:

29. Ֆինանսական կազմակերպության կողմից ցանցային մուտքի հսկման պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից արտաքին միացումների դեպքում օգտագործողի նույնականացման, ցանցերում տարանջատման, ցանցի միացումների հսկման և ցանցի երթուղու հսկման պահանջներին ներկայացվող պայմանների կատարմամբ:

30. Օգտագործողի նույնականացումը արտաքին միացումների դեպքում ցանցային մուտքի հսկման պահանջին ներկայացվում են հետևյալ պայմանները.

1) արտաքին յուրաքանչյուր մուտքի թույլատրումն անձամբ ցանցային ադմինիստրատորի կողմից և դրա վերաբերյալ համապատասխան գրանցամատիանում գրանցումը նշելով՝

ա. արտոնագրված արտաքին օգտագործողի տվյալները (անուն, ազգանուն, նույնականացուցիչ ID),
բ. ցանցի թույլատրելի/հասանելի հատվածները,

գ. այդպիսի միացումների պատասխանատուների տվյալները,

2) Ցանցը պետք է կառուցված լինի այնպես, որ

ա. հարցումը անցկացնի միջցանցային էկրանի (firewall) միջով,

բ. թաքցնի ցանցային անուններն ու կառուցվածքը արտաքին օգտագործողներից,

գ. թույլատրի արտաքին միացումները ցանցի միայն կոնկրետ հատվածներին,

դ. թույլատրի մուտքերը միայն կանխանշված մուտքային կետերից,

ե. հաստատի արտաքին միացման իսկությունը,

3) անօրինական արտաքին միացումների կամ փորձերի գրանցումը և մանրամասն հետազոտումը պատասխանատուի կողմից՝ հետագայում կանխելու կամ այդ հասցեն բլոկավորելու նպատակով,

4) dial-up-ի օգտագործման դեպքերում միացումների պաշտպանումը՝ «հետգանգման» (dial-back) տեխնիկայի օգտագործմամբ և միացման խզումով ոչ թե միացող, այլ ընդունող համակարգչից,

5) արտաքին միացումների անմիջապես հեռացումը՝ իրենց պարագաներով, երբ նրանք այլևս անհրաժեշտ չեն:

31. Տարանջատումը ցանցերում ցանցային մուտքի հսկման պահանջին ներկայացվում են հետևյալ պայմանները.

1) ցանցային բոլոր սարքավորումների նույնականացուցիչների առկայությունը,

2) բոլոր այն ցանցերի պաշտպանվածությունը միջցանցային էկրանների միջոցով (firewall), որոնք հանդիսանում են մեկ այլ ցանցի ենթացանց, կամ կապված են մեկ այլ ցանցի հետ:

32. Ցանցի միացումների հսկման պահանջին ներկայացվում են հետևյալ պայմանները.

1) անօրինական մուտքի հայտնաբերման համակարգի հասանելիությունը միայն հավատարմագրված օգտագործողին,

2) ցանցին ցանկացած անլար (wireless) միացման հաստատումը ցանցի ադմինիստրատորի կողմից,

3) Անլար (wireless) բոլոր միացումների կարգավորվածությունը: Անլար (wireless) բոլոր միացումները պետք է պարունակեն.

ա. տեղադրման և միացման եղանակները,

բ. մուտքի սահմանափակման եղանակները,

գ. գաղտնագրության օգտագործումը,

դ. չհավաստագրված մուտքի կետերի հայտնաբերման ձևերը (օրինակ շենքի պատերի պարուրում անլար (wireless) ցանցի հայտնաբերման լարերով),

4) միացման կետերի տեղադրվածությունը շենքի դրսի պատերից և հնարավոր շեղման աղբյուրներից հեռու (օրինակ՝ միկրոալիքային վառարաններ),

5) ցանցի պաշտպանվածությունը միջցանցային էկրանների միջոցով (firewall),

6) անլար (wireless) միացումների համար կիրառվող հետևյալ սահմանափակումները՝

ա. Այ-փի (IP) հասցեի ֆիլտրացիա, որը թույլ կտա ցանցին միանալ միայն հավաստագրված համակարգիչներին,

բ. ՄԱԲ (MAC) հասցեների ֆիլտրացիա, որը թույլ կտա միանալ անլար (wireless) ներքուք ինտերֆեյս քարդսին (Network Interface Cards (NIC)) միայն հավաստագրված ՄԱԲ (MAC) հասցեներով,

7) համակարգիչների ներքուք ինտերֆեյս քարդսին (Network Interface Cards (NIC)) քարտերի ստուգումն այն նպատակով, որպեսզի դրանք ձևավորված լինեն այնպես որ,

ա. չհանդիսանան մուտքի կետեր,

բ. թույլատրեն միայն կլիենտ – կլիենտ միացումներ, եթե չկա հստակ գրավոր այլ միացման թույլատվություն,

8) գաղտնագրային ֆունկցիաների ակտիվացվածությունը, որոնք կապահովեն գոնե ցածրակարգ գաղտնագրություն և էլեմենտար պաշտպանության մակարդակ, իսկ առնվազն վեց ամիսը մեկ գաղտնագրման բանալիները փոփոխումը,

9) հույժ կարևոր միացման կետերի առավել պաշտպանվածության ապահովումը ՎՓՆ-երի (VPN) օգտագործման միջոցով:

33. Ցանցի երթուղու հսկման պահանջին ներկայացվում են հետևյալ պայմանները.

1) միջցանցային էկրանների (firewall) կառավարման կարգավորվածությունը և փաստաթղթավորվածությունը, իսկ միջցանցային էկրանի (firewall) միջոցով ներքոնշյալ պահանջների կատարումը.

ա. որոշակի տիպի ինֆորմացիոն հոսքի (traffic) ֆիլտրացում (օրինակ՝ ԱՅ-ՓԻ (IP) հասցեները, ԹԻ-ՄԻ-ՓԻ (TCP) պորտերը),

բ. որոշակի ինֆորմացիոն հոսքի (traffic) ձևերի կամ տեսակների արգելում,

գ. հարձակումներից պաշտպանություն,

դ. ցանցի մասին տվյալների գաղտնիության պահպանում,

2) Միջցանցային էկրանների (firewall) այնպիսի կառուցվածքի առկայությունը, որը կապահովվի.

ա. կապի միջոցները խիստ ստուգումը, որոնք շատ մատչելի են կեղծիքների համար (օրինակ՝ ԴՆՍ (DNS), ՖՏՊ (FTP), ՆՆԹՓ (NNTP), ՌԻՓ (RIP), ՍՄԹՓ (SMTP), Թելնեթ (Telnet), Յու-Յու-Մի-Փի (UUCP)),

բ. փաթեթների բլոկավորումը, որոնք օգտագործվում են ծառայության մերժման (denial of service) հարձակումների համար (օրինակ՝ Այ-Սի-Էմ-Փի էքո (ICMP Echo), Յու-Դի-Փի (UDP) և Թի-Սի-Փի էքո (TCP Echo), Չարջեն (Chargen) և Դիսքարդ (Discard)),

գ. ինֆորմացիոն հոսքի (traffic) մերժումն այնպիսի հասցեներից, որոնք ենթադրաբար կարող էին լինել ապօրինի ձեռք բերված (spoofed) (օրինակ՝ երբ հասցեն պատկանում է ցանցին, բայց ստեղծումը եղել է ցանցից դուրս),

3) միջցանցային էկրանների (firewall) ունակությունը բլոկավորելու կապի որոշակի հարցումները՝ հիմնվելով օրինակ՝

ա. հասցեի վրա (օրինակ՝ կոնկրետ IP հասցե)

բ. պորտի վրա (օրինակ՝ ՖԹՓ (FTP) 20 և 21 կամ Թելնեթ (Telnet) 23).

4) Ֆիլտրացման կատարումը ֆինանսական կազմակերպության կողմից ընդունված կանոնների հիման վրա, որոնք

ա. մշակվել և փորձարկվել են վստահելի անձանց կողմից,

բ. եղել են «ամենաքիչ հարցման» (least access) հիման վրա,

գ. փաստաթղթավորված և պարբերաբար վերանայված են,

4) մինչև նոր կամ փոփոխված կանոնների կիրառումը դրանց տեստավորվածության, փաստաթղթավորվածության և հաստատվածության իրականացումը համապատասխանաբար պատասխանատուների և տնօրենի կողմից, որի արդյունքները փաստաթղթավորվում են,

5) ցանցի մասին տեղեկատվության բացահայտման սահմանափակումը.

ա. ցանցային մակարդակում հասցեների ձևափոխմամբ (օրինակ՝ հասցեի փոխարինում մեկ ուրիշով ցանցից դուրս գալու դեպքում),

բ. ծրագրային մակարդակում փրոքսի սերվերների (proxy server) օգտագործմամբ (օրինակ՝ Էյչ-Թի-Թի-Փի (HTTP) հարցումները անցկացնել Էյչ-Թի-Թի-Փի (HTTP) փրոքսի սերվերի (proxy server) միջով):

34. Օպերացիոն համակարգերի մուտքի հսկման պահանջին ներկայացվում են հետևյալ պայմանները.

1) Ֆինանսական կազմակերպությունում հստակ քաղաքականության առկայությունը՝ համակարգ մուտք գործելու և աշխատանքներ կատարելու ժամանակների վերաբերյալ, որն առնվազն պարունակում է՝

ա. համակարգ մուտքի արգելման պահանջ աշխատանքային օրերից և/կամ ժամերից դուրս, հակառակ դեպքում՝ մուտքն իրականացվում է ղեկավարության գրավոր թույլտվությամբ, որտեղ նշվում են թույլատրվող անձի անուն, ազգանուն, թույլատրվող մուտքի օրը, ժամը, նպատակը, հասանելիության գոտիները և ենթադրվող տևողությունը,

բ. օգտագործողի ավտոմատ կերպով անջատում համակարգից պարապուրդի կանխորոշված ժամանակահատվածի դեպքում:

35. Ֆինանսական կազմակերպության կողմից համակարգի մուտքի և օգտագործման մոնիտորինգի պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից դեպքերի գրանցման, ինչպես նաև համակարգի օգտագործման մոնիտորինգի պահանջներին ներկայացվող պայմանների կատարմամբ:

36. Որպես դեպքերի գրանցման ապահովման պայման ֆինանսական կազմակերպությունում մոնիտորինգի արդյունքները պարբերաբար ներկայացվում են տնօրինության քննարկմանը (առնվազն եռամսյակը մեկ), իսկ արդյունքներն արձանագրվում են:

37. Համակարգի օգտագործման մոնիտորինգի պահանջին ներկայացվում են հետևյալ պայմանները.

1) ցանցի գործունեության դիտարկման մեջ ներառելը գործող ցանցային սարքավորումների շահագործումը նորմալ և զբաղված ժամանակահատվածներում, մասնավորապես.

ա. ցանցի ավտոմատ մոնիտորինգ իրականացնող ծրագրերի կիրառություն,

բ. պարբերաբար ցանցի լոգ ֆայլերի ուսումնասիրում,

գ. ցանցի խցանումների և գերծանրաբեռնվածության հետազոտում,

դ. ցանցի և ցանցային սարքավորումների խոցելիության ստուգում համապատասխան համակարգերի միջոցով (օրինակ Nessus), Փինգուայեր (Pingware) կամ ՍԱԹԱՆ (SATAN)),

ե. չհավատարմագրված անլար (wireless) ցանցերի փնտրում (հայտնաբերում),

2) անօրինական մուտքերի հայտնաբերման մեխանիզմները պետք է ուղղված լինեն՝

ա. հայտնաբերելու հայտնի հարձակման ձևերը,

բ. պարբերաբար թարմացնելու անօրինական մուտքի հայտնաբերման համակարգը, ավելացնելու նոր հարձակման ձևերի մասին տվյալներ,

գ. ցանկացած անհասկանալի և/կամ չարտոնված գործողություն գրանցելու համապատասխան գրանցամատյանում,

դ. պաշտպանելու անօրինական մուտքի հայտնաբերման համակարգը տարբեր տեսակի հարձակումներից:

38. Շարժական և հեռահար աշխատանքների պահանջին ներկայացվում են հետևյալ պայմանները.

1) հեռահար (remote) աշխատակայանի միջոցով աշխատելու համար ֆինանսական կազմակերպությունում ընթացակարգի առկայությունը, որում մանրամասն նկարագրվում են այն դեպքերը, երբ պետք է օգտվել աշխատակայանից, անվտանգության ապահովման միջոցները, այն անձանց ցանկի ներառումը, որոնց տրված են հիմնավորված իրավասություններ՝ օգտվելու աշխատակայանից: Անվտանգության ապահովման նկատառումներով աշխատակայանում գրանցվում է նաև անվտանգության պատասխանատու աշխատակից, որն աղմինիստրատորի հետ համատեղ տնօրինում է մուտքի գաղտնաբառը: Գրանցված անձանց ցանկը պետք է խիստ սահմանփակ լինի,

2) հեռահար աշխատանքները (օրինակ հեռահար տեստավորում) պետք է լինեն.

ա. կանխորոշված, պլանավորված և համաձայնեցված տնօրինության հետ,

բ. անհատական արտոնություններ տրամադրելով,

գ. սահմանափակ արտոնություններով՝ կախված կանխորոշված աշխատանքի տեսակից,

դ. գրանցվող հատուկ գրանցամատյանում,

3) հեռահար աշխատանքների ավարտից անմիջապես հետո.

ա. կատարվում են հեռահար աշխատանքների լոգ ֆայլերի դիտարկում,

բ. փաստաթղթավորվում են և կամայական անհամաձայնություն կանխորոշված միացման նպատակների հետ ենթարկվում են մանրամասն դիտարկման տնօրինության հետ:

ԳԼՈՒԽ 7. ՀԱՄԱԿԱՐԳԻ ՄՇԱԿՄԱՆ ԵՎ ՍՊԱՍԱՐԿՄԱՆ ԳՈՐԾԸՆԹԱՅՆԵՐԻ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՍԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՁ

39. Համակարգի մշակման և սպասարկման գործընթացների անվտանգության պահանջին ներկայացվում են հետևյալ պայմանները.

1) ֆինանսական կազմակերպությունում կիրառվող բանկային ծրագրային ապահովումների տեստավորման իրականացում նրանց վերջնական ներդրումից առաջ՝ բանկային ավտոմատացված համակարգերի աշխատանքի անխափանությունն ապահովելու նպատակով, ընդ որում, տեստավորման արդյունքները փաստաթղթավորվում են՝ հաստատվելով պատասխանատու անձանց ստորագրությամբ,

2) ֆինանսական կազմակերպությունում բանկային ծրագրային ապահովման ներդրումը (ինչպես նոր տարբերակը, այնպես էլ հերթական թարմացված տարբերակը) միայն այն դեպքում, երբ ա. այն անցել է տեստավորման բոլոր փուլերը և առկա են տեստավորման արդյունքների վերաբերյալ փաստաթղթեր՝ պատասխանատու անձանց ստորագրությամբ,

բ. ընդունվել է համակարգի պատվիրատուի (օգտագործողների) կողմից՝ պահպանելով ֆորմալ ընթացակարգ (ընդունման – հանձնման ակտ),

3) ծրագրային ապահովման նոր տարբերակի ներդրումից հետո հին տարբերակի առանձին պահպանումը՝ որպես ռեզերվային տարբերակ:

40. Ֆինանսական կազմակերպության կողմից համակարգի մշակման և սպասարկման գործընթացների անվտանգության պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

ԳԼՈՒԽ 8. ԲԻԶՆԵՍԻ ՇԱՐՈՒՆԱԿԵԼԻՈՒԹՅԱՆ ԿԱՌԱՎԱՐՈՒՄԸ՝ ՈՐՊԵՍ ՖԻՆԱՆՍԱԿԱՆ ԿԱԶՄԱԿԵՐՊՈՒԹՅԱՆ ՆԵՐՔԻՆ ՀՍԿՈՂՈՒԹՅԱՆ ԻՐԱԿԱՆԱՑՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋ

41. Ֆինանսական կազմակերպության կողմից բիզնեսի շարունակելիության կառավարման պահանջի կիրառումը որոշվում է ֆինանսական կազմակերպության կողմից Բիզնեսի շարունակելիության կառավարման գործընթացի, ինչպես նաև շարունակելիության պլանի մշակման և իրագործման պահանջներին ներկայացվող պայմանների կատարմամբ: Ֆինանսական կազմակերպության կողմից բիզնեսի շարունակելիության կառավարման պահանջը համարվում է չկատարված, եթե ֆինանսական կազմակերպությունը չի ապահովել սույն գլխում նշված պայմանների և /կամ/ դրանցից մեկի պատշաճ կատարումը:

42. Բիզնեսի շարունակելիության կառավարման գործընթացի պահանջին ներկայացվում են հետևյալ պայմանները.

1) ֆինանսական կազմակերպությունում արտակարգ իրավիճակներում գործողության հստակ կարգերի առկայություն՝ հաստատված ղեկավարության կողմից, փորձարկված և փաստաթղթավորված,

2) ցանցի խափանման դեպքում.

ա. դրա մասին տեղեկացվում են կանխորոշված անձինք, օրինակ ցանցի տերը,

բ. դրանք գրանցվում են հատուկ գրանցամատյանում ավտոմատ կամ ոչ ավտոմատ,

գ. դրանք դասակարգվում են ըստ տեսակի (օրինակ ֆիզիկական խափանում, հարձակում),

դ. դասակարգվում են ըստ հասցված վնասի,

ե. հայտնաբերվում են խափանման պատճառը,

զ. արգելվում են բոլոր տեսակի գործողությունները աշխատակիցների կողմից մինչև ցանցի ամբողջական վերականգնումը,

է. փաստաթղթավորվում են բոլոր վերականգնողական աշխատանքները,

ը. իրականացվում է վերլուծություն տեստավորման միջոցով, որն ուղղված է պարզելու, թե արդյոք ցանցի անվտանգությունը չի խաթարվել խափանման կամ վերականգնման արդյունքում:
Վերլուծությունների արդյունքները փաստաթղթավորվում են,

3) վերականգնումից անմիջապես հետո համապատասխան քայլերի ձեռնարկումը նույնատիպ խափանումներից խուսափելու համար:

43. Շարունակելիության պլանի մշակման և իրագործման պահանջին ներկայացվում են հետևյալ պայմանները.

1) ֆինանսական կազմակերպությունում միջոցառումների իրականացումը՝ ցանցի մեկ հատվածի խափանումից խուսափելու համար, որը ներառում է՝

ա. խափանման նշանի դեպքում ցանցի հոսքի ավտոմատ փոփոխում (re-routing),

բ. կրկնակի կամ այլընտրանքային միջցանցային էկրանների (firewall), կոմուտատորների (switch) և հոսանքի աղբյուրների տեղայնացում,

2) կարևոր ցանցային սարքավորումների և ծրագրային ապահովումների խափանման ռիսկի նվազեցման միջոցառումներ՝

ա. արտոնված, որակյալ սարքավորումներ/ծրագրային ապահովումների ձեռք բերում,

բ. պարբերական թարմացումներ կատարում,

գ. կարճ ժամանակահատվածում կարևոր սարքավորումների/ծրագրային ապահովումների փոխարինելիության ապահովումը,

դ. ցանցի նպատակին և կառուցվածքին հարմար պրոտոկոլների (protocol) օգտագործումը,

3) միջցանցային էկրանների (firewall) թերությունների հայտնաբերման և վերացման գործընթացների անցկացումը, որոնք ներառում են.

ա. միջցանցային էկրանների (firewall) պարբերական դիտարկումներ, տեստավորումներ համապատասխան ծրագրերի միջոցով, և/կամ բոլոր նախազգուշական ցուցումների դիտարկումների միջոցով (օր. ՍԵՌԹ (CERT) նախազգուշացումներ),

բ. սխալի կամ խափանման դեպքում կատարվելիք հստակ գործողություններ, որոնք փաստաթղթավորվում են: