ՀԱՎԵԼՎԱԾ
Հաստատված է
Հայաստանի Հանրապետության
կենտրոնական բանկի խորհրդի
2013 թվականի հուլիսի 9-ի թիվ 173-Ն որոշմամբ

ԿԱՐԳ
ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ՆՎԱԶԱԳՈՒՅՆ ՊԱՀԱՆՋՆԵՐԻ ՍԱՀՄԱՆՄԱՆ ՎԵՐԱԲԵՐՅԱԼ

Գլուխ 1. Ընդհանուր դրույթներ

1. Սույն կարգը սահմանում է Հայաստանի Հանրապետության կենտրոնական բանկի (այսուհետ՝ Կենտրոնական բանկ) կողմից լիցենզավորվող և/կամ գրանցվող կազմակերպություններում (այսուհետ՝ Կազմակերպություն(ներ))՝ Տեղեկատվական տեխնոլոգիաների ոլորտում առկա ռիսկերի կառավարմանը և նվազեցմանն ուղղված նվազագույն պահանջները: Այս պահանջները մշակվել են հիմք ընդունելով Ստանդարտացման միջազգային կազմակերպություն (ԻՍՕ/ISO)/Միջազգային էլեկտրատեխնիկական հանձնաժողովի (ԻԷԿ, IEC) կողմից մշակված՝ ԻՍՕ/ԻԷԿ 27001:2005 *«Տեղեկատվական տեխնոլոգիաներ. Անվտանգության ապահովման մեխանիզմներ. Տեղեկատվական Անվտանգության Կառավարման Համակարգեր. Պահանջներ» (ISO/IEC 27001:2005 Information technology - Security techniques – Information security* management systems - Requirements) ստանդարտը:
2. Սույն կարգը հիմք է հանդիսանում Կազմակերպություններում տեղեկատվական անվտանգության ապահովման ոլորտում կիրառվող միջազգային ստանդարտների ներդրման և համապատասխան հավաստագրման պահանջների սահմանման համար: Ընդ որում, նշված ստանդարտների պահանջներին համապատասխանության վկայագրում անցնելը՝ Կազմակերպությանը չի ազատում սույն կարգով սահմանված պահանջների կատարումից:
3. Սույն կարգում ներկայացված են Կազմակերպությունների տեղեկատվական անվտանգության ապահովման մոտեցումները, որոնք հանդիսանում են պաշտպանության նպատակների և խնդիրների համակարգված շարադրանք, այդ թվում՝ տեղեկատվական անվտանգության ընդունելի մակարդակի

ապահովման միջոցների, ընթացակարգերի և հիմնական սկզբունքների նկարագրություն, այսինքն՝ ներկայացվում են Կազմակերպության տեղեկատվական անվտանգության ապահովման հիմնական սկզբունքները:

Գլուխ 2. Հիմնական հասկացություններ

4. Սույն կարգի իմաստով՝
   1) **Տեղեկատվական անվտանգություն (ՏԱ)՝** Կազմակերպությանը պատկանող տեղեկատվությունը չթույլատրված մուտքից, օգտագործումից, հրապարակումից, խեղաթյուրումից, փոփոխումից կամ ոչնչացումից պահպանում/պաշտպանություն:
   2) **Տեղեկատվական անվտանգության ապահովման քաղաքականությունը (ՏԱ քաղաքականություն)** իրենից ներկայացնում է Կազմակերպության հստակ տեսլականը տեղեկատվական անվտանգության ապահովման ճանապարհների և մեթոդների վերաբերյալ, որով սահմանվում են ընդհանուր դրույթներ՝ Կազմակերպության տեղեկատվական ռեսուրսների և տեխնիկածրագրային համակարգերի կառավարման, տեղեկատվության մշակման, փոխանցման և տրամադրման վերաբերյալ:
   3) **Տեղեկատվություն՝** տեղեկատվություն, որը Կազմակերպության կողմից պահպանվում, մշակվում, փոխանցվում և/կամ ներկայացվում է ցանկացած միջոցով՝ էլեկտրոնային և թղթային կրիչներով, բանավոր (այդ թվում նաև հեռախոսային խոսակցություններ) և/կամ վիզուալ տեսքով տեղեկատվության ներկայացմամբ (օրինակ՝ համակարգչի էկրանին պատկերվող տեղեկատվություն, տելեկոնֆերանսներ և այլն):
   4) **Կազմակերպություն՝** սույն կարգի իմաստով Կազմակերպություններ են համարվում.
      ա. ՀՀ տարածքում գործող բանկերը (այսուհետ նաև բանկ),
      բ. Ապահովագրական ընկերությունները,
      գ. Վճարահաշվարկային կազմակերպությունները,
      դ. Կենտրոնական դեպոզիտարիան,
      ե. Կարգավորող շուկայի օպերատորը,
      զ. Վարկային բյուրոները,
      է) լեվերիջով գործարքների, այդ թվում՝ ֆորեքս գործարքների հետ կապված ներդրումային և ոչ հիմնական ծառայություններ մատուցող անձիք:
      (4-րդ կետը լրաց. 10.12.18թ. թիվ 214Ն)

   5) **«Գործառնական օր» Ծրագրային համակարգ՝** Կազմակերպության հիմնական գործունեության իրականցման համար կիրառվող ավտոմատացված համակարգ, որը նախատեսված է միասնական հաշվառման, հաշվապահական հաշվառման, որոշակի բնույթի

գործառնությունների իրականացման համար և/կամ, որը հնարավորություն է տալիս կատարել վճարումներ՝ նախապես վերահսկելով օգտագործողների իրավունքները, հաշիվների մնացորդները, մնացորդների սահմանաչափերը (լիմիտները):

6) **Ղեկավարության վերին օղակ՝** Կազմակերպության կառավարման բարձրագույն մարմին, գործադիր տնօրեն, խորհուրդ կամ այլ:
7) **Ղեկավար աշխատակազմ՝** Կազմակերպության դեպարտամենտի, վարչության և/կամ բաժնի պետեր:
8) **Ներքին տեղեկատվական ցանց՝** Կազմակերպության լարային և/կամ անլար, ներառյալ՝ նաև մասնաճյուղերի և ներկայացուցչությունների համակարգչային ֆիզիկական և/կամ անլար ցանցերը:
9) **Պահուստային կրկնօրինակ՝** համակարգի աշխատանքն արձանագրող մատյանի և համակարգում մշակվող տեղեկությունների կրկնօրինակում, որի նպատակն է համակարգի խափանման, տեղեկատվության կորստի կամ այլ նմանատիպ դեպքերում՝ գրանցված տեղեկատվությունը իրավասու օգտագործողներին որոշակի ժամանակահատվածում հասանելի դարձնելը:
10) **Արխիվ՝** տեղեկատվության պարբերական հավաքագրումը և Կազմակերպության տարածքում և/կամ տարածքից դուրս տեղեկատվական կրիչների կամ համակարգիչների և/կամ այլ տարբերակով երկարաժամկետ պահպանվող տեղեկատվություն:
11) **«տաք» ռեզերվ կամ «տաք» սերվեր՝** պահուստ կամ սերվեր, որը նախատեսված է հիմնական սերվերի խափանման դեպքում՝ անմիջապես անցում կատարելու համար պահուստային սերվերին:
12) **«սառը» ռեզերվ կամ «սառը» սերվեր՝** պահուստ կամ սերվեր, որի վերականգնումը կատարվում է որոշակի ժամանակահատվածում:
13) **Արտաքին մուտք՝** Կազմակերպության ներքին տեղեկատվական ցանցից դուրս գտնվող աշխատակայանից միացում Կազմակերպության ներքին տեղեկատվական ցանցին:
14) **Արտաքին օգտագործող՝** օգտագործող, որը միանում է Կազմակերպության ներքին տեղեկատվական ցանցին այդ ցանցից դուրս գտնվող աշխատակայանից (արտաքին մուտքից օգտվող աշխատակից կամ օգտագործող)
15) **Համակարգերի ադմինիստրատոր՝** աշխատակից, որը պատասխանատու է համակարգերի տեղադրման, կառավարման և սպասարկման, համակարգի թարմացման և համակարգի արխիվացման և վերականգնման համար:
16) **Ցանցային ադմինիստրատոր՝** աշխատակից, ով իրականացնում է ցանցային ենթակառուցվածքի բաղադրիչների (երթուղիչներ, ուղղորդիչներ, միջցանցային էկրաններ, ցանցի սեգմենտներ և այլն) կարգաբերումը/կառավարումը և սպասարկումը: Ցանցային ադմինիստրատորը պատասխանատու է նաև ցանցի պահուստավորման,

համապատասխան ծրագրային միջոցների և սարքավորման ձեռք բերման վերահսկման, ինչպես նաև տեղադրման արտոնագրման համար: Ցանցային ադմինիստրատորները պատասխանատու են նաև ինտերնետային կապ տրամադրող ընկերությունների կողմից տրամադրվող ծառայությունների մոնիտորինգի և արտաքին (թույլատրված, արտոնագրված) տեղեկատվական ռեսուրսների հասանելիության ապահովման համար:

17) **Երրորդ անձանց՝** Կազմակերպությանը ժամանակավոր և/կամ անժամկետ պայմանագրային հիմունքներով ծառայություններ մատուցող ընկերություն կամ անձ, որը որևէ կերպ առնչվում է, կարող է առնչվել կամ հասանելիության իրավասություններ ձեռք բերել Կազմակերպության կողմից որևէ սկզբունքով դասակարգված տեղեկատվության հետ:
18) **Դասակարգված տեղեկատվություն՝** Կազմակերպության կողմից որպես *կոնֆիդենցիալ, գաղտնի, հույժ գաղտնի կամ այլ կերպ դասակարգված տեղեկատվություն, որոնց թվի մեջ առնվազն պետք է մտնի* առևտրային, բանկային գաղտնիք կազմող տեղեկատվությունը, Կազմակերպության զարգացման ծրագրերը, հնարավոր կլանման թիրախները, որոշ հեռախոսային համարներ, անձնակազմի և հաճախորդների վերաբերյալ տեղեկատվությունը: Այսպիսի տեղեկատվության թվին են պատկանում նաև երրորդ կազմակերպությունների/ ընկերությունների վերաբերյալ տեղեկատվությունը, որոնք տրամադրվել են չբացահայտման պայմանով:
19) ***Բաց (հանրամատչելի) տեղեկատվություն՝*** *տեղեկատվությունը, որը* համապատասխան իրավասություններ ունեցող մարմնի կողմից հանրության համար հասանելի է բնութագրվել, որը ներկայացված է փաստաթղթային և/կամ տեղեկատվության զանգվածների տեսքով, անկախ տեղեկատվության պահպանման, ներկայացման և արտապատկերման եղանակից (օրինակ՝ տվյալ Կազմակերպության ինտերնետային էջի հանրամատչելի մասում ներկայացված տեղեկատվությունը, մամլում տպագրվող տվյալներ և այլն):
20) **Ծածկագրում՝** բաց տեղեկատվության ձևափոխումը որոշակի ծածկագրման ալգորիթմով:
21) **Տեղեկատվական հենքի ադմինիստրատոր՝** Կազմակերպության տվյալների հենքերի տեղեկատվության պահպանման, կառուցվածքի սահմանման և սպասարկման համար պատասխանատու աշխատակից: Տեղեկատվական հենքի ադմինիստրատորի պարտականությունների մեջ է մտնում տեղեկատվական հենքերի կառավարման համակարգերի տեղադրումն ու կարգաբերումը, ինչպես նաև տեղեկատվական հենքերում պահվող տեղեկատվության հասանելիության և ամբողջականության ապահովումը:
22) **Անվտանգության պատասխանատու՝** իրականացնում է Կազմակերպության տեղեկատվական անվտանգության քաղաքականության փոփոխությունների նախաձեռնումը, տեղեկատվական ենթակառուցվածքի բոլոր բաղադրիչների, ռեսուրսների և գործընթացների, Կազմակերպության անվտանգության

կանոնների համապատասխանության հսկումը, տեղեկատվական ռիսկերի կառավարումը, տեղեկատվական անվտանգության խախտման պատահարների վարումը և քննության իրականացնումը, տեղեկատվական ռեսուրսների հանդեպ հասանելիությունների կառավարման գործընթացում մասնակցությունը և վերահսկումը, ինչպես նաև օգտագործողների ուսուցումը և իրազեկության մակարդակի բարձրացումը:

23) **«Արգելված է ամեն ինչ, բացի…» սկզբունք՝** Իրավասությունների տրամադրման սկզբունք, որտեղ համապատասխան համակարգում բոլոր օգտագործողներին սկզբում արգելվում է իրականացնել ցանկացած գործողություն, այսինքն՝ փակվում են բոլոր իրավասությունները, այնուհետև բացվում են միայն տվյալ աշխատատեղով սահմանված աշխատանքային պարտականությունների իրականացման համար անհրաժեշտ և/կամ Կազմակերպության ղեկավարության վերին օղակի կողմից հաստատված իրավասությունները:

24) **Տեխնիկական առաջադրանք՝** Կազմակերպության ծրագրային համակարգի տեխնիկածրագրային պահանջները սահմանող փաստաթուղթ:

25) **Մշակող ընկերություն՝** Կազմակերպության «Գործառնական օր» ծրագրային համակարգը և/կամ այլ տիպի ծրագրային համակարգեր մշակող, Կազմակերպության ստորաբաժանումներից տարբերվող, ընկերություն:

26) **Գլխավոր օգտագործող/ադմինիստրատոր՝** Կազմակերպության ծրագրային ապահովման հիմնական ադմինիստրատոր, որն, ի սկզբանե, առկա է համակարգում կամ տվյալների հենքում և ստացել է համապատասխան իրավասություններ համակարգը մշակող որևէ ընկերության կամ Կազմակերպության կողմից՝ ծրագրային համակարգի նախնական, սկզբնական, հիմնական, բազային կարգաբերումների իրականացման համար (օրինակ՝ sysadmin, BANK, root, sa և այլն):

27) **Պատվիրակում (outsourcing)՝** Կազմակերպության ներքին գործարար գործառույթների որոշ մասի իրականացման հանձնումը, պայմանագրային հիմունքներով, երրորդ անձին/ ընկերությանը:

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 հնարավորություն ընձեռող անվտանգության բացերի հայտնաբերում:

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

(4-րդ կետը լրաց.17.03.17թ. թիվ 66 Ն)

Գլուխ 3. ՏԱ կազմակերպումը

5. Կազմակերպության տեղեկատվական անվտանգության համակարգի կառուցումը պետք է հիմնված լինի համալիր մոտեցման վրա: Այս մոտեցումը ուղղված է Կազմակերպության ներսում տեղեկատվության մշակման, հավաքագրման, պահպանման և տրամադրման համար անվտանգ միջավայրի ստեղծմանը՝ միավորելով սպառնալիքների դեմ ուղղված միջոցառումները:
6. Կազմակերպության տեղեկատվական անվտանգության ապահովման համակարգը պետք է կառուցված լինի հետևյալ սկզբունքների հիման վրա.
   1) *օրինականություն*. ՏԱ ապահովման միջոցները և միջոցառումները պետք է ընտրվեն գործող օրենսդրությանը համապատասխան,
   2) *համակարգային*. ՏԱ ապահովման համակարգի կառուցման համալիր մոտեցումը ենթադրում է տեղեկատվության անվտանգության ապահովման խնդիրների ընկալման և լուծման համար էական նշանակություն ունեցող բոլոր փոխկապակցված, փոխազդող և ժամանակի մեջ փոփոխվող տարրերի և պայմանների հաշվի առնում,
   3) *ամբողջականություն*. տեխնիկածրագրային համակարգերի պաշտպանության միջոցների և մեթոդների ամբողջական օգտագործումը ենթադրում է տարաբնույթ միջոցների համաձայնեցված կիրառություն պաշտպանության ամբողջական համակարգի կառուցման ժամանակ, որը կծածկի սպառնալիքների իրագործման առկա բոլոր ուղիները (ուղղությունները),
   4) *պաշտպանության անընդհատություն*. անընդհատ, նպատակաուղղված գործընթաց, որը ենթադրում է համապատասխան որոշումների կայացումը Կազմակերպության գործունեության ողջ ժամանակահատվածի ընթացքում,
   5) *արդիականություն և կատարելագործում*. կանխարգելիչ բնույթի միջոցառումների ներդրում և ՏԱ ապահովման միջոցառումների և միջոցների անընդհատ կատարելագործում,
   6) *արդյունավետություն*. ենթադրում է ՏԱ ապահովման նպատակով ծախսված գումարների, տեղեկատվական ռեսուրսների և հնարավոր վնասների չափի հարաբերակցության վերլուծություն,
   7) *անձնական պատասխանատվություն*. ենթադրում է տեղեկատվության և այն մշակող համակարգերի անվտանգությունը ապահովող բոլոր աշխատակիցների պատասխանատվության սահմանումը՝ նրանց իրավասությունների սահմաններում,

8) *իրավասությունների նվազեցման սկզբունք*. նշանակում է իրավասությունների տրամադրում միայն աշխատանքային անհրաժեշտությունից ելնելով,
9) *փոխհամագործակցություն*. Կազմակերպության ներսում աշխատանքային բարենպաստ և բարիդրացիական մթնոլորտի ձևավորում,
10) *ՏԱ ապահովման համակարգի ճկունություն*. ՏԱ ապահովման մակարդակի փոփոխության հնարավորություն,
11) *ՏԱ ապահովման համակարգերի կիրառման դյուրինություն*. ՏԱ ապահովման համակարգը պետք է լինի ինտուիտիվ հասկանալի,
12) *գիտականորեն հիմնավորված և տեխնիկապես իրագործելի*. տեղեկատվական տեխնոլոգիաները, տեխնիկածրագրային համակարգերը, տեղեկատվության պաշտպանության միջոցառումները և միջոցները պետք է իրագործված լինեն հաշվի առնելով գիտատեխնիկական առաջընթացները և ժամանակակից տեխնոլոգիաները,
13) *մասնագիտացում և պրոֆեսիոնալիզմ*. ՏԱ ապահովման միջոցների մշակման և համապատասխան միջոցառումների իրագործման նպատակով պետք է ներգրավվեն մասնագիտացված կազմակերպություններ և/կամ անձինք, որոնք տվյալ ասպարեզում ունեն գործնական փորձ և համապատասխան լիցենզիա (մասնագիտացված անձանց դեպքում՝ աշխատանքային փորձ) համապատասխան ծառայությունների մատուցման համար: Ադմինիստրատիվ միջոցների իրագործման և ՏԱ ապահովման միջոցների շահագործումը պետք է իրականացվի մասնագիտացված և համապատասխան կրթություն ստացած և/կամ աշխատանքային փորձ ունեցող մասնագետների կողմից,
14) *պարտադիր վերահսկողություն*. վերահսկողությունը պետք է կրի պարտադիր և արդիական/պարբերական բնույթ՝ պաշտպանության սահմանված կանոնների խախտման փորձերի հայտնաբերման և կանխարգելման արդյունավետ իրագործման նպատակով:

7. ՏԱ ապահովման նպատակով կազմվող փաստաթղթերը պետք է մշակվեն՝ հաշվի առնելով հետևյալ հիմնադրույթները.
   1) **Գաղտնիություն՝** տեղեկատվության հասանելիության ապահովում միայն համապատասխան իրավասություն ունեցող օգտագործողներին,
   2) **Ամբողջականություն՝** տեղեկատվության հուսալիության, ամբողջականության և մշակման մեթոդների ապահովություն,
   3) **Հասանելիություն՝** նույնականացված օգտագործողների համար անհրաժեշտ տեղեկատվության և դրա հետ կապված ակտիվների հասանելիության ապահովում,
   4) **Պատասխանատվության բաժանում/դերերի բաժանում,**
   5) **Հսկողություն:**
8. Տեղեկատվական տեխնոլոգիաների ռիսկի պատշաճ կառավարման և նվազեցման համար Կազմակերպությունները պետք է մշակեն առնվազն հետևյալ փաստաթղթերը.

1)Տեղեկատվական անվտանգության քաղաքականություն/ռազմավարություն,
2) Արտակարգ իրավիճակներում գործողությունների ծրագրեր,
3) Տեղեկատվական համակարգերում առկա ռիսկերի կառավարման կանոնակարգեր, կարգեր և/կամ կանոններ,
4) Գործարար ծրագրեր, ընթացակարգեր, ուղեցույցներ, պայմանագրեր:

Գլուխ 4. Տեղեկատվական անվտանգության քաղաքականություն/ռազմավարություն

9. Կազմակերպությունը պետք է ունենա ՏԱ քաղաքականության փաստաթուղթ, որը պետք է հաստատված լինի Կազմակերպության Ղեկավարության վերին օղակի կողմից:
10. ՏԱ քաղաքականությունը պետք է վերանայվի/թարմացվի առնվազն ամեն երեք տարին մեկ անգամ, ինչպես նաև՝ ՏԱ քաղաքականությունը հաստատած ղեկավար անձի կամ նրա իրավասությունների փոփոխության դեպքում:
11. ՏԱ քաղաքականությունը պետք է ընդգրկի Կազմակերպության կողմից տեղեկատվական տեխնոլոգիաների կիրառությամբ մշակվող, պահպանվող, ներկայացվող, ստացվող և փոխանցվող ամբողջ տեղեկատվությունը, համակարգերը, միջոցները, ծրագրերը, տվյալները, ցանցային համակարգերը, ֆիզիկական պաշտպանության համակարգերը և անձնակազմը՝ առանց բացառությունների:
12. Տեղեկատվական հարաբերությունների սուբյեկտներ են հանդիսանում.
    1) Կազմակերպությունը, որպես տեղեկատվական ռեսուրսների սեփականատեր,
    2) Բաժինները և կառուցվածքային ստորաբաժանումները,
    3) Պաշտոնատար անձինք և անձնակազմը,
    4) Տվյալ Կազմակերպությունում տեղեկատվական ռեսուրսների հետ առնչվող այլ անձինք,
    5) Համագործակցող կազմակերպության սույն կետի 1-4-րդ ենթակետերում նշված սուբյեկտները (հիմնական Կազմակերպության տեղեկատվության հետ առնչվելու չափով):

Գլուխ 5. Արտակարգ իրավիճակներում գործողությունների ծրագիր

13. Կազմակերպության գործարար գործընթացների անընդհատության ապահովման գործընթացի անբաժանելի մաս պետք է կազմի տեղեկատվական տեխնոլոգիաների անվտանգության ապահովման՝ արտակարգ իրավիճակներում գործողությունների ծրագիրը, որով պետք է սահմանվեն հետևյալ նվազագույն կետերը.
    1) Արտակարգ իրավիճակներում գործողությունները ղեկավարող աշխատանքային խումբը՝ պատասխանատվության շրջանակներով,

2) Խմբի անդամի անունը, ով իրավասու է հայտարարելու Արտակարգ իրավիճակ,
3) Արտակարգ իրավիճակի լինելու հավանականությունը,
4) Արտակարգ իրավիճակների դասակարգում՝ ըստ հավանական վնասի մեծության,
5) Յուրաքանչյուր իրավիճակի համար կանխատեսվող վերականգնման միջոցառումները և ժամանակը:

Գլուխ 6. Տեղեկատվական համակարգերում առկա ռիսկերի կառավարման կանոնակարգեր, կարգեր և /կամ կանոններ

14. ՏԱ ապահովման քաղաքականության իրագործման համար Կազմակերպության կողմից պետք է մշակվեն համապատասխան կանոնակարգեր, կարգեր և /կամ կանոններ, որոնցով կկարգավորվի ՏԱ ապահովման հետ կապված յուրաքանչյուր գործընթաց: Այդ կարգերով (կանոնակարգեր, կանոններ) պետք է սահմանվեն Կազմակերպության ծրագրային ապահովման և ավտոմատացված համակարգերի (տեխնիկածրագրային համակարգերի) հետևյալ կետերը.
    1) տեխնիկածրագրային համակարգերի ստեղծման նպատակների և հիմնավորումների սահմանման անհրաժեշտությունը և դրանց շահագործման ընթացակարգերը,
    2) տեխնիկածրագրային համակարգերի տարրերի տեղակայման վայրերը, դրանց կազմը, կառուցվածքը, այլ օբյեկտների հետ կապը,
    3) տեխնիկածրագրային համակարգերում շրջանառվող տեղեկատվության խմբերը, օգտագործման ընթացակարգերը և տեղեկատվության հասանելիության մակարդակները,
    4) տեխնիկածրագրային համակարգերում շրջանառվող տեղեկատվության խմբերի պաշտպանության կազմակերպման կանոնները:

15. Սույն կարգի 14-րդ կետի 1-4-րդ ենթակետերով սահմանված կետերը պետք է անդրադառնան հետևյալ խնդիրներին.
    1) տեխնիկածրագրային համակարգերի ստեղծման նպատակների և հիմնավորումների սահմանման անհրաժեշտությունը և դրանց շահագործման ընթացակարգերը. Այս հատվածում ներկայացվում է տեխնիկածրագրային համակարգերի կիրառության նպատակները. որտեղ և ինչ եղանակներով են դրանք օգտագործվելու, կիրառման անհրաժեշտությունը և այլն: Տեխնիկածրագրային համակարգերը պետք է կիրառվեն/ստեղծվեն այս կամ այն գործընթացների որակական հատկանիշների բարձրացման, հսկողության, արագագործության, ժամանակի խնայողության, վերլուծության

և կանխատեսման նպատակներով, որոնք իրենց հերթին կկրճատեն ծախսերը և հետևաբար կմեծացնեն Կազմակերպության եկամտաբերությունը;

2) *տեխնիկածրագրային համակարգերի տարրերի տեղակայման վայրերը, դրանց կազմը, կառուցվածքը, այլ օբյեկտների հետ կապը*. Այս մասում նկարագրվում է տեխնիկածրագրային համակարգերի գործունեության յուրահատկությունները, այսինքն՝ ինչ կապեր կան տեխնիկածրագրային համակարգերի տարբեր բաղադրիչների միջև, ինչպիսի տեխնիկական միջոցներ են կիրառվում, առկա է արդյոք կապ այլ կազմակերպությունների հետ և ինչպես է դա իրականացվում, ինչ կապուղիներ են օգտագործվում, ինչ ծրագրային ապահովում է անհրաժեշտ տեխնիկածրագրային համակարգերի գործունեության համար:

3) *տեխնիկածրագրային համակարգերում շրջանառվող տեղեկատվության խմբերի պաշտպանության կազմակերպման կանոնները*. Այստեղ պետք է նկարագրվի, թե գաղտնիության ինչպիսի մակարդակներ են կիրառվում, ինչ տեսակի փաստաթղթեր են շրջանառվում տեխնիկածրագրային համակարգերում, որ տեղեկատվությունն է ենթակա պաշտպանության և ինչ նորմատիվային/կարգավորիչ ակտերի հիման վրա:

4) *տեխնիկածրագրային համակարգերում շրջանառվող տեղեկատվության խմբերի պաշտպանության կազմակերպման կանոնները*. Պետք է նկարագրվեն տեխնիկածրագրային համակարգերում շրջանառվող տեղեկատվական ռեսուրսների օգտագործողների խմբերը և այս խմբերի իրավասությունների շրջանակները:

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 տեխնիկածրագրային 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:

(16-րդ կետը խմբ. 17.03.17թ. թիվ 66Ն)

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:
(17-րդ կետը խմբ. 17.03.17թ. թիվ 66Ն)

18. Սույն կարգի 17-րդ կետում նշված բնութագրիչները ներկայացվում են չորս հիմնական խմբերով՝
    1) Օգտագործողների բնութագրիչներ. Ընդհանուր առմամբ օգտագործողի ցանկացած բնութագրիչ կարող է կիրառվել (սեռը, տարիքը, ծննդավայրը և այլն): Կանոնակարգիչ փաստաթղթերով առնվազն պետք է սահմանվեն հետևյալ բնութագրիչները.
    ա. Հասանելիության մակարդակ. Այս կետը սահմանվում է ՀՀ օրենքների, միջազգային պայմանագրերի, Կենտրոնական բանկի նորմատիվ ակտերի պահանջների, որոնք վերաբերում են գաղտնի համարվող տեղեկատվության պաշտպանության (պետական, բանկային, առևտրային, անձնական և այլ գաղտնիք համարվող տեղեկատվություն) և տվյալ տեղեկատվական ռեսուրսի դասակարգման մակարդակի հիման վրա:
    բ. Անհրաժեշտ է իմանալ (need - to - know). Այս բնութագրիչը պետք է կցվի այն աշխատակիցներին, անձանց, որոնք աշխատանքային պարտականություններից ելնելով, պետք է ունենան հասանելիության իրավասություններ այս կամ այն տեղեկատվական ռեսուրսին:
    գ. Դերերի բաժանում. Օրինակ՝ օգտագործողին կարող է տրվել «սովորական օգտագործող» բնութագրիչը, իրեն համապատասխան իրավասություններով: Դերերը կարող են տրամադրվել ըստ Կազմակերպությունում զբաղեցրած պաշտոնների և/կամ իրականացվող գործառույթների:
    դ. Խմբային պատկանելիություն. Այս բնութագրիչը կարող է ներառել օգտագործողի ազգությունը, երկիրը, կազմակերպությունը և այլն:

2) Օբյեկտների բնութագրիչներ (տեղեկատվական ռեսուրսների բնութագրիչներ). Իրավասությունների տրամադրման որոշման կայացման համար պետք է կիրառվեն նաև օբյեկտների բնութագրիչները: Այդ բնութագրիչներն են.

ա. Զգայունության աստիճան. Ցանկացած տեղեկատվություն պետք է դասակարգվի ըստ բացահայտման նկատմամբ զգայունության աստիճանի (չդասակարգվող, փակ (կոնֆիդենցիալ), գաղտնի կամ հույժ գաղտնի): Պետք է սահմանվեն հասանելիության ընթացակարգերը՝ ըստ համապատասխան դասակարգման աստիճանների:

բ. Տեղեկատվության նույնականացուցիչներ. Պետք է կիրառվեն տեղեկատվության նույնականացուցիչներ, օրինակ՝ տեղեկատվության սկզբնաղբյուրը կամ տեղեկատվության ստեղծողը, տեղեկատվության սեփականատերը և փաստաթղթի համարը;

գ. Հասանելիության կառավարման ցուցակ. Պետք է թվարկվեն այն անձիք, ովքեր հասանելիության իրավասություններ ունեն տվյալ տեսակի տեղեկատվությանը: Տեղեկատվության սեփականատերը կարող է նշել իրեն պատկանող տեղեկատվության օգտագործողներին:

3) Արտաքին պայմաններ. ՏԱ ապահովման համար մշակված փաստաթղթերով սահմանված որոշ կետեր պետք է ներկայացնեն արտաքին պայմանների բնութագրիչները, ինչպիսիք են աշխարհագրական դիրքը, ժամանակը և նմանատիպ այլ տեղեկություններ: Մեծ ուշադրություն պետք է դարձվի փոփոխվող բնութագրիչներին, մասնավորապես.

ա. Աշխարհագրական դիրք. Հասանելիության իրավասություններ պետք է տրամադրվեն՝ այդ թվում նաև հիմք ընդունելով աշխարհագրական վայրը (օրինակ՝ տվյալ տեղեկատվությունը հասանելի է միայն գլխամասից կամ մասնաճյուղից):

բ. Ժամանակ. Որոշակի տեսակի տեղեկատվությանը հասանելիության իրավասությունները կարող են տրամադրվել կոնկրետ ժամերին:

4) Տվյալների բովանդակություն. Հասանելիության իրավասությունները պետք է տրամադրվեն ելնելով տեղեկատվության արժեքավորության աստիճանից:

(18-րդ կետը փոխ. 17.03.17թ. թիվ 66Ն)

Գլուխ 7. Գործարար ծրագրեր, ընթացակարգեր, ուղեցույցներ, պայմանագրեր

19. Կազմակերպությունը՝ իր տեղեկատվական անվտանգության ապահովման համար պետք է մշակի որոշակի գործարար ծրագրեր, ընթացակարգեր, ուղեցույցներ, պայմանագրեր, որոնք պետք է նկարագրեն տեղեկատվական ռեսուրսների պաշտպանության ապահովման նպատակների իրագործման ձևերը, ուղիները, տեղեկատվության պաշտպանության համակարգի հիմնական խնդիրների լուծումները: Նշված փաստաթղթերով պետք է սահմանվեն հետևյալ խնդիրների լուծման ուղիները.
    1) Դասակարգված տեղեկատվություն պարունակող փաստաթղթերի օգտագործում, պահպանում և ոչնչացում, այդ թվում՝ կոդերի, էլեկտրոնային բանալիների ցուցակների կամ դրանց պատճենների ոչնչացում,
    2) Գաղտնաբառերի օգտագործում և պահպանում,
    3) Օգտագործողների նույնականացում և իրավասությունների տրամադրում,
    4) Օգտագործողներին նույնականացման (իդենտիֆիկացիայի) և իրավասությունների (աուտենտիֆիկացիա) հաստատման համար կիրառվող/կիրառվելիք միջոցների ցանկը և տվյալ գործընթացը բնութագրող ընթացակարգը,
    5) Տեղեկատվական պաշտպանության գործընթացների նկատմամբ մոնիտորինգի իրականացում,
    6) Էլեկտրոնային նույնականացուցիչ ֆայլերի օգտագործում և պահպանում,
    7) Օգտագործողների գրանցում և հեռացում,
    8) Տեխնիկածրագրային համակարգերի և տեղեկատվության ինվենտարիզացիա (տեղեկատվության սեփականատերերի սահմանում),
    9) Արտաքին կրիչների օգտագործում և պահպանում,
    10) Հակավիրուսային համակարգերի կիրառություն,
    11) Աշխատակիցների պարտականությունների տարանջատում և դասակարգում,
    12) Արտաժամյա աշխատանքների իրականացում,
    13) Սխալների բացահայտման, անվտանգության կանոնների խախտման դեպքերի քննման, մեղավորների պատժման և աշխատանքների մշտական վերահսկման ընթացակարգեր,
    14) Պահուստային կրկնօրինակում, պահպանում և վերականգնում,
    15) Արխիվների հետ աշխատանք, պահպանման ժամկետներ, պաշտպանության միջոցներ, օգտագործողների ցանկ, հասանելիության մակարդակ, արխիվացված տեղեկատվության վերականգնում,
    16) Կիրառվող ծրագրային համակարգերի դասակարգում,
    17) Հնարավոր սպառնալիքների մոդելների կառուցում,
    18) Կիրառվող ծրագրային փաթեթների թեստավորում,
    19) «Գործառնական օր» Ծրագրային համակարգի և այլ ծրագրային համակարգերի բացում/փակում,
    20) Տեխնիկական առաջադրանքների կազմում,

21) Կազմակերպության կողմից շահագործվող ծրագրերի վերջնական տարբերակի ծրագրային կոդերում փոփոխությունների նախաձեռնում, իրականացում, թեստավորում և վերահսկում,
22) Հիմնական սերվերների օգտագործում, կառավարում և վերականգնում,
23) Ցանցերի կառավարման, ցանցային անվտանգության համար՝
ա. Տեղեկատվության ֆիլտրացման պահանջներ,
բ. Ներքին տեղեկատվական ցանցի ենթակառուցվածքի ֆիզիկական և տրամաբանական ճարտարապետությունը,
գ. Ներքին տեղեկատվական ցանցի պաշտպանության մեխանիզմներ, ցանցային սարքավորումների կարգաբերումներ:
24) Հեռակա աշխատանքների իրականացման համար՝
ա. Հեռակա ադմինիստրավորման համակարգեր,
բ. Հեռակա աշխատանքների իրականացման պահանջներ,
գ. Հեռակա աշխատանքների իրականացման նպատակները և դեպքերը:
25) Անլար ցանցի կիրառման համար՝
ա. Անլար միացումների նպատակները և անլար միացումները թույլատրող սարքերի կարգաբերումները;
բ. Անլար միացումների համար կիրառվող անվտանգության միջոցները և միջոցառումները:
26) Էլ-փոստի և համացանցի օգտագործման պահանջներ,
27) Պատահարների գրանցման և մոնիտորինգի իրականացման պահանջներ,
28) Վճարային պրոցեսների անվտանգության պահանջներ,
29) Անընդհատության ապահովման միջոցառումներ,
30) Տեխնիկական սարքավորումների (միջոցների) ֆիզիկական ամբողջականության ապահովման արդյունավետ միջոցների կիրառություն,
31) Կազմակերպության իրավաբանական պաշտպանության կազմակերպում՝ այլ ընկերությունների հետ փոխհարաբերությունների (պատվիրակում, տեղեկատվության փոխանակում և այլն) ընթացքում, վերջիններիս սպասարկող անձնակազմի կողմից ոչ միտումնավոր կամ չարամիտ (անթույլատրելի) գործողությունների բացասական հետևանքներից,
32) Անձնակազմի ուսուցման և համալրման հետ կապված չափանիշները և մոտեցումները,
33) Կիրառվելիք կրիպտոգրաֆիկական և այլ պաշտպանական միջոցները,
34) ՏԱ ապահովման համակարգի արդյունավետության հսկողության իրականացման հիմնադրույթները,
35) Կազմակերպության գործունեության տարածքից դուրս (մոռացված) թողնված տեղեկատվության կրիչների ապօրինի տիրապետումը կողմնակի անձանց կողմից,

36) Տեխնիկածրագրային համակարգերի նախագծման փուլում կազմակերպության աշխատակիցների կողմից թույլ տրված սխալների, աշխատանքային կանոնների խախտման կամ ոչ պատշաճ կատարման արդյունքում՝ ՏԱ ապահովման համակարգի վրա բացասական ազդեցությունը,
37) Պատահարների վերաբերյալ տվյալների հավաքագրման, գրանցման և մշակման համակարգի գործարկում,
38) Տեխնիկածրագրային համակարգերի միջոցով մշակվող և ցանցի միջոցով փոխանցվող տեղեկատվության ծածկագրում,
39) Հիմնական սերվերից պահուստային սերվերին և հակառակը անցման սկզբունքները,
40) Սերվերային սենյակի մուտքի և ելքի, սերվերային սենյակում միաժամանակ գտնվող մարդկանց քանակի, սերվերային սենյակներում աշխատանքների իրականացման ժամանակ ուղեկցող անձանց վերաբերյալ կանոնները, ընթացակարգը,
41) Սերվերային սենյակի պարամետրերը կանոնակարգող փաստաթղթի մշակում (ջերմաստիճան, խոնավություն, լուսավորություն, ֆիզիկական անվտանգություն և այլն),
42) Տվյալների շտեմարաններում պահվող դասակարգված տվյալների ծածկագրում կամ համարժեք անվտանգության միջոցառման նախաձեռնում,
43) Ծրագրային համակարգերի տեղադրման, կարգաբերման վերաբերյալ կանոնները, ընթացակարգը:
44) Սույն կետով սահմանված բոլոր կանոնակարգիչ փաստաթղթերում պետք է նշվեն՝
    ա. փաստաթղթի վերանայման (թարմացման) ամսաթիվը,
    բ. փաստաթղթի ընդունման համապատասխան որոշման համարը,
    գ. փաստաթղթի պատասխանատուի անունը, ազգանունը և պաշտոնը,
    դ. փաստաթղթի համարը (նույնականացուցիչը):
45) Սույն կետով սահմանված բոլոր կանոնակարգիչ փաստաթղթերում պետք է.
    ա. սահմանված լինեն փաստաթղթում տեղ գտած տերմինները: Որոշ հասկացություններ, հատկապես տեղեկատվական տեխնոլոգիաներին վերաբերող, կարող են ունենալ այլ իմաստային նշանակություն, որոնք պետք է բացատրվեն տվյալ փաստաթղթի նպատակների տեսանկյունից:
    բ. ներկայացվեն այն անձինք (աշխատատեղերը/պաշտոնները), ում (որոնց) վերաբերում է կարգավորիչ փաստաթուղթը: Օրինակ՝ որոշ փաստաթղթեր կարող են վերաբերել միայն ամբողջ կամ կես դրույքով աշխատող աշխատակիցներին, ինչպես նաև կարող են վերաբերել ցերեկային կամ գիշերային հերթափոխով աշխատող աշխատակիցներին:

գ. մշակված լինեն մատչելի լեզվով, հակիրճ ձևակերպված պահանջներով և չլինեն երկիմաստ:

46) (46-րդ ենթակետը ուժը կորցրել է 17.03.17թ. թիվ 66Ն)

47) Կազմակերպության կողմից կիրառվող թղթային գրանցամատյանների վարման ընթացակարգեր:

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:

(19-րդ կետը փոխ., լրաց, 17.03.17թ. թիվ 66Ն)

Գլուխ 8. Գործարար գործընթացների անընդհատության ապահովում և թեստավորման կազմակերպում

20. Կազմակերպությունը առնվազն երեք տարին մեկ անգամ, ինչպես նաև արտակարգ իրավիճակներում գործողությունների նոր ծրագրի մշակման դեպքում պետք է իրականացնի արտակարգ իրավիճակների սցենարների փորձարկումներ՝ հաշվարկելով արտակարգ իրավիճակների հետևանքների վերացման համար անհրաժեշտ ժամանակը և ռեսուրսները:

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 ՔՐԵՍԹ 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:

(20.1-20.7 ենթակետերը լրաց. 17.03.17թ. թիվ 66Ն)

21. Կազմակերպության կողմից սահմանված ժամկետներում, մասնավորապես՝ առնվազն կիսամյակը մեկ անգամ, իսկ տեխնիկական անձնագրերում վեց ամսից

քիչ սահմանված ժամանակահատվածներում դրանց համապատասխան, պետք է ստուգվեն սարքավորումների աշխատունակությունը:

22. Կազմակերպության ցանցային սարքավորումները և անվտանգության բոլոր համակարգերը պետք է ապահովված լինեն անխափան էլեկտրասնուցման համակարգերով:
23. Անխափան էլեկտրասնուցման աղբյուրներ պետք է ունենան նաև առնվազն այն համակարգիչները, որոնք ապահովում են Կազմակերպության բնականոն գործունեությունը և առօրյա աշխատանքը:
24. Կազմակերպության էլեկտրասնուցման համակարգը պետք է կազմակերպված լինի այնպես, որ ապահովի տեխնիկածրագրային համակարգերի անխափան բնականոն աշխատանքը:
25. Կազմակերպությունը պետք է ապահովի կարևոր սարքավորումների և ծրագրային փաթեթների հնարավորինս կարճ ժամանակահատվածում փոխարինելիությունը:
26. Կազմակերպության կողմից առնվազն «Գործառնական օր» Ծրագրային համակարգերի վրա կատարվող պրոֆիլակտիկ աշխատանքների իրականացումը պետք է իրականացվի Կազմակերպության աշխատանքային ժամերից դուրս և ավարտվի մինչև Կազմակերպության աշխատանքային օրվա սկիզբը:
27. Կազմակերպության բոլոր տարածքային ստորաբաժանումներում պետք է առկա լինի գործող գեներատոր-շարժիչ կամ այլընտրանքային հոսանքի աղբյուր:

Գլուխ 9. Պահուստավորում և արխիվացում

28. Կազմակերպության կողմից օգտագործվող առնվազն այն ծրագրային համակարգերում, որտեղ շրջանառվում են Կազմակերպության հաճախորդների և/կամ ֆինանսական գործառնությունների վերաբերյալ որևէ տեղեկատվություն, պետք է առկա լինեն պահուստային կրկնօրինակման հնարավորություն:
29. Կազմակերպության կողմից սահմանված պարբերականությամբ պետք է իրականացվի օգտագործվող ծրագրային համակարգերի, և դրանց տեղեկատվական բազաների պահուստային կրկնօրինակում և արխիվացում:
30. Պահուստային կրկնօրինակները և արխիվները պետք է պահպանվեն տեղեկատվության գաղտնիության աստիճանի դասակարգմանը համապատասխան:
31. Կազմակերպության բոլոր պահուստային կրկնօրինակները և արխիվները չեն կարող պահպանվել բաց տեքստով:
32. Կազմակերպության պահուստային կրկնօրինակները և արխիվները պետք է վարվեն տարբեր ֆիզիկական կրիչների կամ համակարգիչների վրա:

33. Կազմակերպության բոլոր ընթացիկ և/կամ պահուստային կրկնօրինակները Կազմակերպության կողմից սահմանված պարբերականությամբ պետք է փորձարկվեն և ուսումնասիրվեն:
34. Կազմակերպության կողմից սահմանված որոշակի պարբերականությամբ պետք է իրականացվի «Գործառնական օր» Ծրագրային համակարգի պահուստային տարբերակին անցման-վերականգնման գործողությունը:
35. Կազմակերպության պահուստային (ռեզերվային) սերվերները իր կողմից կանխորոշված պարբերականությամբ պետք է փորձարկվեն:
36. Համապատասխան սերվերային համակարգերի «տաք» և «սառը» ռեզերվների ընտրությունը իրականացվում է Կազմակերպության ղեկավարության վերին օղակի կողմից համապատասխան հիմնավոր որոշմամբ:

Գլուխ 10. Հիմնական ռիսկերը

37. Կազմակերպությունը պետք է մշակի համապատասխան փաստաթուղթ, որտեղ մանրամասն նկարագրված են ՏԱ ռիսկերի հնարավոր մոդելները և դրանց աղբյուրները, տվյալ ռիսկերի իրագործման եղանակները, տեղեկատվության արտահոսքի ուղիները, պետք է տրվեն «միտումնավոր անթույլատրելի գործողություններ» հասկացողության սահմանումը: Այս փաստաթուղթը հանդիսանում է գաղտնի և պետք է հասանելի լինի միայն արտոնագրված օգտագործողներին:
38. Նշված փաստաթղթում առաջին հերթին պետք է նկարագրվի Կազմակերպության համար նշանակալից համարվող ռիսկերի տեսակները և դրանց իրագործման հնարավոր ճանապարհները: Ընդ որում, ռիսկերի տեսակները պետք է բաժանվեն առնվազն հետևյալ խմբերի.
    1) գաղտնիության խախտում (գաղտնի տեղեկատվության հրապարակում, արտահոսք և այլն),
    2) աշխատունակության խախտում (գործարար գործընթացների ապակազմակերպում),
    3) ամբողջականության խախտում (տեղեկատվության խեղաթյուրում, փոփոխում, հափշտակում, ոչնչացում և այլն),
    4) տեղեկատվության հասանելիության խախտում:
39. Ռիսկերի հնարավոր աղբյուրները պետք է դասակարգվեն ըստ *ներքին (տվյալ Կազմակերպության) ռիսկերի և արտաքին ռիսկերի:*
(39-րդ կետը փոխ. 17.03.17թ. թիվ 66Ն)

40. Կազմակերպությունը պետք է հատուկ ընթացակարգեր սահմանի իր անձնակազմի և երրորդ անձանց ՏԱ ապահովման կանոնների ուսուցման կամ ծանոթացման նպատակով՝ նշված անձանց կողմից Կազմակերպության գաղտնի տեղեկատվության միտումնավոր կամ ոչ միտումնավոր արտահոսքը (այլ անձանց բացահայտումը) կանխելու համար: Նշված կանոնները պետք է

վերաբերվեն նաև բանավոր կերպով անձնակազմին և/կամ երրորդ անձանց տրամադրվող (հայտնի դարձած) դասակարգված տեղեկատվության անվտանգության ապահովմանը:

41. Կազմակերպությունը պետք է նկարագրի «խախտողի մոդելը», պետք է տրվի խախտողի սահմանումը և նա դասակարգվի ըստ հետևյալ խմբերի.
    1) անփորձ օգտագործող,
    2) զեղծարար,
    3) արտաքին կամ ներքին խախտող:
42. Կազմակերպության կողմից պետք է սահմանվեն վնասի այն չափը, որոնք կարող են պատճառել սույն կարգի 41-րդ կետում նշված խմբի անձինք իրենց գործողություններով:
43. Սույն կարգի 41-րդ կետում նշված խմբերը սահմանելուց պետք է հաշվի առնվի աշխատանքից ազատված անձանց ենթախումբը, որոնք կարող են օգտագործել իրենց գիտելիքները Կազմակերպության ներքին գործընթացների վերաբերյալ, Կազմակերպությունում կիրառվող պաշտպանության միջոցների և միջոցառումների, հասանելիության իրավասությունների տրամադրման ընթացակարգերի վերաբերյալ՝ պաշտպանված տեղեկատվության հափշտակման և նմանատիպ այլ անթույլատրելի գործողությունների նպատակով (տեղեկատվական անվտանգության տեսանկյունից՝ այս անձինք, ինչպես նաև տվյալ Կազմակերպության անձնակազմը, հանդիսանում են առավել վտանգավոր խմբերը):

Գլուխ 11. Կազմակերպչական կառուցվածք

44. Կազմակերպությունը պետք է ունենա Տեղեկատվական անվտանգության հիմնախնդիրներով զբաղվող ստորաբաժանում (այսուհետև՝ ՏԱ ստորաբաժանում) կամ անձ: ՏԱ ստորաբաժանման կամ անձի բացակայության դեպքում պետք է առկա լինի տվյալ գործառույթների պատվիրակման պայմանագիր ՏԱ ապահովման ոլորտում մասնագիտացված ընկերության հետ:
45. Կազմակերպության Տեղեկատվական տեխնոլոգիաների ստորաբաժանման աշխատակիցների պարտականությունները պետք է բաշխված լինեն ըստ սույն կարգի Հավելված 1-ում նշված տիպային պարտականությունների անհամադրելիության մատրիցին համապատասխան:
46. Կազմակերպության ադմինիստրատորները չպետք է ունենան որևէ ֆինանսական գործարք կատարելու իրավասություն: Ֆինանսական գործարք է համարվում նաև գործառնական օրվա բացման/փակման իրականացումը:
47. Կազմակերպության և բոլոր աշխատակիցների միջև պետք է ստորագրվի տեղեկատվության գաղտնիության պահպանման (չբացահայտման) համաձայնագիր:

48. Կազմակերպությունում ֆինանսական գործարքների, օգտագործողների գրանցման ու իրավասությունների տրամադրման բոլոր աշխատանքները պետք է կազմակերպված լինեն կիրառելով երկակի վերահսկման մեխանիզմը, այսինքն՝ մուտքագրումը, ստուգումը և հաստատումը պետք է կատարվեն տարբեր աշխատակիցների կողմից: Պետք է հնարավորինս բացառված լինեն ցանկացած գործողության միանձնյա իրականացումը, այսինքն՝ գործողության նախաձեռնողը, ստուգողը և հաստատողը պետք է լինեն տարբեր՝ առնվազն երկու աշխատակից, ընդ որում թույլատրելի է միայն ստուգման և հաստատման գործընթացի համատեղումը: Սույն կետում նշված պահանջները, բացառությամբ՝ օգտագործողների գրանցման ու իրավասությունների տրամադրման, կարող են չկատարվել Կազմակերպության կողմից միայն հստակ և գրավոր ձևով պատճառաբանված հիմնավորման առկայության դեպքում:
49. Կազմակերպության օգտագործողներին տրված իրավասությունները պետք է համապատասխանեն տվյալ աշխատակցի աշխատատեղի նկարագրին:
50. Կազմակերպության յուրաքանչյուր աշխատակից մեկ համակարգում պետք է ունենա միայն մեկ օգտագործողի միջոցով աշխատելու հնարավորություն, իսկ պահանջի կատարման անհնարինության դեպքում անհրաժեշտ է Կազմակերպության ղեկավարության վերին օղակի կողմից հաստատված հստակ հիմնավորման առկայություն, աշխատակցին տրամադրված յուրաքանչյուր հաջորդ օգտագործողը չպետք է ունենա հիմնական օգտագործողի հետ խաչվող կամ հիմնական օգտագործողի գործողությունների երկակի վերահսկման մեխանիզմը խախտող իրավասություն:
51. Կազմակերպության կողմից կիրառվող բոլոր «Գործառնական օր» ծրագրային համակարգերը, հերթական և արտահերթ ձևափոխությունները, թարմացումները և կամայական այլ փոփոխությունները հիմնական կիրառումից առաջ պետք է փորձարկվեն և հիմնական աշխատանքի տեղափոխվեն միայն փորձարկման դրական եզրակացության դեպքում:
52. Կազմակերպության ներքին տեղեկատվական ցանցից դուրս գտնվող կամայական աշխատակայանից յուրաքանչյուր հեռակա միացում պետք է իրականացվի բացառապես Կազմակերպության ղեկավարության վերին օղակի թույլտվությամբ, նախօրոք արտոնագրված օգտագործողների կողմից: Արտաքին մուտքերի անհրաժեշտության դադարման դեպքում տվյալ մուտքերը անմիջապես ապաակտիվացում են:
53. Կազմակերպության համապատասխան աշխատակիցների կողմից պարբերաբար պետք է իրականացվեն Կազմակերպության առնվազն «Գործառնական օր» ծրագրային համակարգի և այլ կարևոր և հույժ կարևոր դասակարգված ծրագրային համակարգերի էլեկտրոնային գրանցամատյանների, հեռակա աշխատանքների հատուկ գրանցամատյանների, ինչպես նաև հեռացված, մերժված և/կամ փոփոխված գործարքների/փաստաթղթերի

մոնիտորինգ, որոնց արդյունքները առնվազն եռամսյակը մեկ պետք է ներկայացվեն գործադիր ղեկավարությանը:

54. Կազմակերպությունում պետք է իրականացվի Կազմակերպության տեղեկատվական կայքի անվտանգության և ամբողջականության պարբերական ուսումնասիրություն:
55. Կազմակերպությունում պետք է իրականացվի միջազգային տեղեկատվական ցանցում (համացանցում) Կազմակերպության մասին հրապարակումների ուսումնասիրություն:
56. Կազմակերպությունում հեռակա աշխատանքների (հեռակա փորձարկումների) իրականացման դեպքում՝
    1) նախապես որոշվում են հեռակա աշխատանքների իրականացման համար անհրաժեշտ և հասանելի շրջանակները, պլանավորվում և համաձայնեցվում Կազմակերպության ղեկավարության վերին օղակի հետ,
    2) ստեղծվում (տրամադրվում) են առանձին օգտագործողներ անհատական և սահմանափակ արտոնություններով՝ կախված կանխորոշված աշխատանքի տեսակից,
    3) իրականացված հեռակա աշխատանքների վերաբերյալ տվյալները գրանցվում են հատուկ գրանցամատյաններում:

Գլուխ 12. Տեղեկատվական անվտանգություն պահանջներ

57. Կազմակերպության տեղեկատվական անվտանգության հարցերով զբաղվում է ՏԱ պատասխանատուն, ՏԱ ստորաբաժանումը կամ Կազմակերպությանը համապատասխան պատվիրակման ծառայություններ մատուցող երրորդ անձը:
58. Կազմակերպության գաղտնագրման բանալիները պետք է փոփոխվեն առնվազն վեց ամիսը մեկ անգամ, եթե Կազմակերպության համար ՀՀ կենտրոնական բանկի կողմից սահմանված այլ իրավական ակտերով ավելի երկար ժամանակ նախատեսված չէ:
59. Կազմակերպությունը, ՏԱ ապահովմանն ուղված փաստաթղթերի, ընթացակարգերի, կանոնների և այլ կանոնակարգիչ փաստաթղթերի մշակման ժամանակ, պետք է հիմնվի, այդ թվում նաև «Արգելված է ամեն ինչ, բացի ...» սկզբունքի վրա:
60. Կազմակերպության կողմից կիրառվող բոլոր «Գործառնական օր» ծրագրային համակարգերի, տեղեկատվական բազաների, ցանցային համակարգերի կառավարման գլխավոր օգտագործողը (ադմինիստրատորները)՝ առկայության դեպքում, պետք է կասեցվեն, իսկ գաղտնաբառերը փակ և պատասխանատու աշխատակիցների կողմից կնքված ծրարներով պետք է պահպանվեն Կազմակերպության անվտանգության հարցերով զբաղվող ստորաբաժանման չհրկիզվող պահարանում: Այդ գաղտնաբառերը պետք է կիրառվեն միայն խիստ անհրաժեշտության, Կազմակերպության կողմից սահմանված դեպքերում և

միայն գործադիր ղեկավարության գրավոր հրամանի առկայության պարագայում:

61. ՏԱ պատասխանատու անձը, ստորաբաժանումը կամ երրորդ անձը առնվազն պետք է իրականացնի՝
    1) համակարգչային ցանցերի և ավտոմատացված համակարգերի անվտանգության միջոցառումների պահպանման վերահսկում, վերլուծությունների իրականացում,
    2) Կազմակերպության ներքին ցանցի խոցելիության թեստերի կազմակերպում (իրականացում) և ցանցի օգտագործողների ակտիվության մոնիտորինգ,
    3) տվյալների բազաների հասանելիության մոնիտորինգ,
    4) արտակարգ իրավիճակների վերահսկում և վերլուծությունների իրականացում,
    5) ավտոմատացված համակարգերի օգտագործողների գրանցման և/կամ հեռացման հաստատում,
    6) համակարգչային ցանցերի և ավտոմատացված համակարգերի օգտագործողների գործողությունների և հասանելիությունների վերլուծություն,
    7) Կազմակերպության էլեկտրոնային գրանցամատյանների վերլուծություն,
    8) նոր ձեռք բերվող կամ մշակվող կիրառական ծրագրերի համար անհրաժեշտ անվտանգության միջոցառումների սահմանում և ներկայացում համապատասխան ստորաբաժանմանը,
    9) մասնակցություն նոր ձեռք բերվող կամ մշակվող կիրառական ծրագրերի թեստավորմանը,
    10) տեղեկատվության անվտանգության պահանջների վերաբերյալ աշխատակիցների ուսուցում, համապատասխան ձեռնարկների մշակում,
    11) Կազմակերպության կողմից սահմանված պարբերականությամբ հաշվետվությունների ներկայացում Կազմակերպության ղեկավարության վերին օղակին:

62. Կազմակերպության կողմից առնվազն գաղտնի և հույժ գաղտնի (կրիտիկական) դասակարգված էլեկտրոնային տեղեկատվությունը պետք է պահպանվի առնվազն գաղտնագրված եղանակով:
    (62-րդ կետը խմբ. 17.03.17թ. թիվ 66Ն)

63. Կազմակերպությունում պետք է առկա լինի դասակարգված տեղեկատվության օգտագործողների ցուցակ (արտոնագրված օգտագործողների ցուցակ)՝ համապատասխանեցված Կազմակերպության Անվտանգության քաղաքականության հետ: Նշված պահանջը պետք է արտացոլվի Կազմակերպության համապատասխան աշխատակիցների Աշխատատեղի նկարագրում:

64. Կազմակերպության տեղեկատվական համակարգերում շրջանառվող դասակարգված տեղեկատվությունը պետք է արտապատկերվի էլեկտրոնային գրանցամատյաններում:
65. Դասակարգված տեղեկատվության վերաբերյալ էլեկտրոնային գրանցամատյանները հանդիսանում են գաղտնիք պարունակող փաստաթղթեր, որոնք պետք է հասանելի լինեն միայն արտոնագրված օգտագործողներին:

Գլուխ 13. Ցանցային անվտանգություն

66. Կազմակերպության ցանցի կառուցվածքը հաստատվում է Կազմակերպության ղեկավարության վերին օղակի կողմից:
67. Կազմակերպության ցանցերի հետ կապված փաստաթղթերը հանդիսանում են գաղտնի և պետք է հասանելի լինեն միայն արտոնագրված օգտագործողներին:
68. Կազմակերպության ցանցը պետք է կառուցված լինի այնպես, որ ցանցին կամայական արտաքին հարցում անցնի առնվազն մեկ միջցանցային էկրանի միջով:
69. Կազմակերպության համապատասխան աշխատակցի կողմից պետք է մշակվի և պարբերաբար վերանայվի ցանցերում տեղեկատվության հոսքի ֆիլտրացման կանոնները:
70. Կազմակերպության ներքին ցանցին միացված համակարգիչները համացանցին կարող են միանալ միայն Կազմակերպության ինտերնետային պրովայդերների միջոցով օգտագործելով միայն Կազմակերպության ներքին տեղեկատվական ցանցը: Արգելվում է Կազմակերպության ներքին ցանցի համակարգիչների ուղիղ միացումը համացանցին, օրինակ՝ տարբեր տեսակի շարժական մոդեմների կիրառմամբ:
71. Կազմակերպության կողմից սահմանված պարբերականությամբ պետք է ուսումնասիրվեն ցանցի աշխատունակությունը գերծանրաբեռնված ռեժիմներում:
72. Կազմակերպության կողմից պետք է դիտարկվեն միջցանցային էկրանների համար Կազմակերպության կողմից սահմանված բոլոր նախազգուշական ցուցումները:
73. Կազմակերպության կողմից պետք է բացահայտվեն ներքին ցանցի բոլոր վտանգավոր կետերը, ներքին ցանցին արտաքին ցանկացած միացման հնարավոր տեղերը:
74. Կազմակերպության տարածքային ստորաբաժանումների միջև տեղեկատվական ցանցերով շրջանառվող տեղեկատվությունը պետք է լինի առնվազն ծածկագրված:

Գլուխ 14. Ծրագրային անվտանգություն

75. Մշակող կազմակերպության ստեղծած՝ գլխավոր ադմինիստրատորի գաղտնաբառը ծրագրի վերջնական գործարկումից և ծրագրի ընդունման-հանձնման ակտը ստորագրելուց անմիջապես հետո պետք է փոխվի, իսկ փոխված գաղտնաբառը փակ ծրարի միջոցով պետք է հանձնվի Կազմակերպության գործադիր ղեկավարին, իսկ գլխավոր ադմինիստրատոր օգտագործողի միջոցով ծրագրային համակարգի ադմինիստրատոր օգտագործող ստեղծելուց անմիջապես հետո գլխավոր ադմինիստրատոր օգտագործողը պետք է կասեցվի:
76. Կազմակերպությունում ցանկացած ծրագրային ապահովման ներդրումը պետք է իրականացվի համապատասխան փորձարկումներից հետո: Ընդ որում՝ փորձարկման ժամանակ արգելվում է օգտագործել Կազմակերպության իրական հաճախորդների տվյալները:
77. Կազմակերպության ծրագրային կարգաբերումների կամայական նորացումները և թարմացումները նույնպես պետք է ներդրվեն միայն փորձարկումներից հետո:
78. Արգելվում է կամայական չարտոնված մուտքի հնարավորության առկայությունը:
79. Արգելվում է այլ անձի կողմից օգտագործվող անունով համակարգ մուտք գործելը, բացառությամբ արտակարգ իրավիճակներում, միայն Կազմակերպության ղեկավարության վերին օղակի թույլտվության առկայության դեպքում:
80. «Գործառնական օր» ծրագրային համակարգի ինքնուրույն մշակման դեպքում Կազմակերպությունում պետք է առկա լինեն՝
    1) մշակված տեխնիկական առաջադրանքը,
    2) ծրագրային համակարգի մշակմանը մասնակցած հիմնական և/կամ ժամկետային պայմանագրով աշխատող աշխատակիցների ցուցակը, որտեղ պետք է նշվեն նաև նրանց զբաղեցրած պաշտոնները,
    3) ծրագրի մշակման լեզուն և ինտերֆեյսը,
    4) ծրագրի վերջնական շահագործվող տարբերակի ծրագրային կոդերը կրող սկավառակների գտնվելու վայրը,
    5) ծրագրերի թեստավորման մասնակիցների ցուցակը, մասնակիցների մասնագիտական որակավորումը, Կազմակերպությունում զբաղեցրած պաշտոնը,
    6) յուրաքանչյուր թեստավորման արձանագրությունը, թեստավորող խմբի մասնակիցների եզրակացությունը, գործադիր տնօրենի և մասնակիցների ստորագրությունները,
    7) ծրագիրը օգտագործող ստորաբաժանումների աշխատակիցների կողմից թեստավորմանը մասնակցելու մասին փաստաթղթերը,
    8) ծրագրի վերջնական շահագործվող տարբերակի ծրագրային կոդերի մեջ փոփոխություններ կատարելու հնարավորություններ ունեցող աշխատակիցների ցուցակը,

9) ծրագրի օգտագործողների ուղեցույցը կամ այլ ուղղորդող ձեռնարկներ, փաստաթղթեր:

(80-րդ կետը փոխ. 17.03.17թ. թիվ 66Ն)

81. «Գործառնական օր» Ծրագրային համակարգը որևէ մշակող ընկերությանը պատվիրակելու դեպքում Կազմակերպությունում պետք է առկա լինեն՝
    1) ծրագրային համակարգի վերաբերյալ Կազմակերպության և մշակող ընկերության միջև կնքված պայմանագիր.
    2) մշակող ընկերությանը ներկայացված տեխնիկական առաջադրանքը և պահանջները.
    3) նոր մշակված ծրագրային ապահովման թեստավորման արձանագրությունը և այլ փաստաթղթեր, որոնք պարունակում են թեստավորման արդյունքները, թեստավորող խմբի մասնակիցների եզրակացությունը, ղեկավարության վերին օղակի և մասնակիցների ստորագրությունները,
    4) Կազմակերպության և մշակող ընկերության կողմից ստորագրված ընդունման-հանձնման ակտը,
    5) մշակող ընկերության տեղեկատվական տեխնոլոգիաների վերաբերյալ հեղինակավոր աուդիտորական կազմակերպության եզրակացությունը.
    6) մշակող ընկերության՝ միջազգային ընդունված չափանիշներին համապատասխանությունը հավաստող վկայագիր կամ միջազգային հավաստագրման որևէ կազմակերպության կողմից թողարկված վկայագիր կամ որևէ ապահովագրական ընկերությունում ծրագրային համակարգի ապահովագրված լինելը հավաստող փաստաթուղթ,
    7) Կազմակերպության, մշակող ընկերության և Էսքրոու (Escrow) ծառայություններ մատուցող երրորդ ընկերության միջև «Գործառնական օր» ծրագրային համակարգի ծրագրային կոդերի պահուստային պահպանման և համապատասխան արտակարգ իրավիճակում Կազմակերպությանը հանձնման վերաբերյալ պայմանագիր:
82. «Գործառնական օր» ծրագրային համակարգի նոր կամ թարմացված տարբերակը ներդրվում է միայն այն դեպքում, երբ այն՝
    1) անցել է թեստավորման բոլոր փուլերը և առկա է թեսթավորող հանձնաժողովի դրական եզրակացությունը,
    2) ընդունվել է համակարգի պատվիրատուի (օգտագործողի) կողմից՝ ընդունման – հանձնման ակտի ստորագրմամբ:
83. Կազմակերպությունը պետք է ձեռք բերի միայն արտոնագրված ծրագրային համակարգեր:
84. Կազմակերպությունը պետք է կատարի ծրագրային ապահովումների պարբերական թարմացումներ:

85. Կազմակերպության «Գործառնական օր» Ծրագրային համակարգի թեստավորումների հետ կապված փաստաթղթերը հանդիսանում են գաղտնի և պետք է հասանելի լինեն միայն արտոնագրված օգտագործողներին:

Գլուխ 15. Ֆիզիկական անվտանգություն

86. Կազմակերպության Սերվեր հանդիսացող համակարգիչները պետք է պահպանվեն համապատասխան առանձնացված (սերվերային) սենյակներում:
87. Սերվերային սենյակը պետք է համապատասխանի հետևյալ չափանիշներին.
    1) լինի առանձնացված հարակից տարածքներից ոչ թափանցիկ նյութերից (օրինակ՝ չլինի ապակուց) պատրաստված պատերով,
    2) սերվերային սենյակի դուռը պետք է հանդիսանա միակ ճանապարհը այնտեղ մուտք գործելու կամ դուրս գալու համար,
    3) ունենա հակահրդեհային պաշտպանության համակարգ,
    4) ունենա շարժման գրանցման/հայտնաբերման համակարգ և/կամ տվիչներ,
    5) ունենա համակարգիչների բնականոն աշխատանքն ապահովելու համար անհրաժեշտ ջերմաստիճանը, օդի խոնավությունը կարգավորող և պահպանող համակարգ, ինչպես նաև օդափոխության համակարգ,
    6) ունենա տեսահսկման համակարգ, որը պետք է տեղադրված լինի այնպես, որ հնարավորություն լինի հսկելու սերվերային սենյակում տեղի ունեցող ցանկացած իրադարձություն,
    7) ունենա դռան ինքնաբերաբար փակման համակարգ,
    8) ունենա սերվերային սենյակի մուտքի/ելքի գրանցման համակարգ (առնվազն պետք է գրանցվի մուտք/ելք գործողի անուն-ազգանունը, մուտքի/ելքի ժամը և ամսաթիվը),
    9) սերվերային սենյակը պետք է ունենա անխափան էլեկտրասնուցման համակարգեր, որը պետք է ապահովի ինչպես սերվերների անխափան աշխատանքը այնպես էլ այս գլխում նշված տեսահսկման, հակահրդեհային պաշտպանության, շարժման գրանցման և հայտնաբերման, ջերմաստիճանը պահպանող, օդափոխության համակարգերի անխափան աշխատանքը, առնվազն հիմնական սերվերներից այլ վայրում գտնվող պահուստային սերվերներին անցնելու ժամանակահատվածում,
    10) եթե սերվերային սենյակը ունի պատուհան, ապա այն պետք է լինի դրսից ճաղապատ և միշտ լինի փակ և կարող է բացվել միայն Կազմակերպության ղեկավարության վերին օղակի գրավոր որոշման և հստակ պատճառաբանության առկայության դեպքում:

    (87-րդ կետը փոխ. 17.03.17թ. թիվ 66Ն)
88. Կազմակերպության բոլոր տեխնիկական սարքավորումները պետք է հողանցվեն:

89. Կազմակերպության տեխնիկածրագրային սարքավորումները պետք է ունենան նույնականացուցիչներ:
90. Ցանցային միացման կետերը պետք է ֆիզիկապես պաշտպանված լինեն:

Գլուխ 16. Ներքին Աուդիտ

91. Եթե Կազմակերպությունը ունի ներքին աուդիտի ստորաբաժանում, ապա դրա կազմում պետք է ներառվի տեղեկատվական տեխնոլոգիաների աուդիտում մասնագիտացված և տեղեկատվական տեխնոլոգիաների աուդիտ իրականացնող աշխատակից:
92. Եթե Կազմակերպությունը չունի ներքին աուդիտի ստորաբաժանում, ապա Կազմակերպությունը պետք է ունենա տեղեկատվական տեխնոլոգիաների աուդիտ իրականացնելու պարտականություններով օժտված աշխատակից:
93. Կազմակերպությունում տեղեկատվական տեխնոլոգիաների աուդիտով զբաղվող ստորաբաժանում կամ աշխատակցի առկայությունը պարտադիր չէ, եթե Կազմակերպությունը տեղեկատվական տեխնոլոգիաների ներքին աուդիտի իրականացումը պատվիրակում է երրորդ անձի:

Գլուխ 17. Պատվիրակում

94. Կազմակերպությունը կարող է մասնակիորեն կամ ամբողջությամբ պատվիրակել տեղեկատվական տեխնոլոգիաների ենթակառուցվածքի աշխատանքները, հաշվի առնելով համապատասխան ՀՀ օրենքներով և նորմատիվ իրավական այլ ակտերով սահմանված սահմանափակումները:

Հայաստանի Հանրապետության
կենտրոնական բանկի խորհրդի
2013 թվականի հուլիսի 9-ի թիվ 173 Ն որոշմամբ հաստատված

«Տեղեկատվական անվտանգության ապահովման վերաբերյալ» կարգի

Հավելված 1

Տիպային պարտականությունների անհամադրելիության մատրից

	Ծրագրավորողներ	Օգնության Ծառայություն	Տվյալների հենքի ադմինիստրատոր	Ցանցային ադմինիստրատոր	Համակարգերի ադմինիստրատոր
Ծրագրավորողներ			X	X	X
Օգնության Ծառայություն					
Տվյալների հենքի ադմինիստրատոր	X			X	X
Ցանցային ադմինիստրատոր	X		X		X
Համակարգերի ադմինիստրատոր	X		X	X	