Հավելված N 1
ՀՀ կառավարության 2011 թ.
դեկտեմբերի 22-ի նիստի N 50
արձանագրային որոշման

Կիբեռանվտանգության ընդհանուր շրջանակը
Հայաստանի Հանրապետության կառավարության 2010 թվականի փետրվարի 25-ի «Հայաստանի Հանրապետությունում էլեկտրոնային հասարակության ձևավորման հայեցակարգին հավանություն տալու մասին» N 7 արձանագրային որոշմամբ սահմանված աշխատանքներում

1. Կիբեռանվտանգության ապահովման օբյեկտներն են՝

1) պետական և տեղական ինքնակառավարման մարմիններում, կարևոր նշանակության օբյեկտներում և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպություններում՝ տեղեկատվական համակարգերը, հաղորդակցական և հեռահաղորդակցական, ցանցային և առցանցային համակցման միջոցները, սերվերները, համակարգային և կիրառական ծրագրային ապահովումը, տվյալների շտեմարանները և դրանց կառավարման համակարգերը, վերջնական օգտագործողների համակարգիչները, ստացվող/տրամադրվող էլեկտրոնային ծառայությունները, ինչպես նաև էլեկտրոնային ձևով մշակվող, շրջանառվող, պահպանվող և հրապարակվող տեղեկատվությունը.
2) էլեկտրոնային ծառայություններ մատուցող ոչ պետական կազմակերպություններում՝ մատուցվող էլեկտրոնային ծառայությունները և էլեկտրոնային ձևով մշակվող, շրջանառվող և պահպանվող, Հայաստանի Հանրապետության օրենսդրությամբ պաշտպանման ենթակա, սահմանափակ հասանելիության տեղեկատվությունը.
3) էլեկտրոնային ծառայություններ չմատուցող ոչ պետական կազմակերպություններում՝ պետական, տեղական ինքնակառավարման մարմինների և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպությունների կողմից տրամադրվող էլեկտրոնային ծառայությունները և էլեկտրոնային ձևով մշակվող, շրջանառվող և պահպանվող, Հայաստանի Հանրապետության

Կատարող՝ Էլինա Մկրտումովա
597142

օրենսդրությամբ պաշտպանման ենթակա, սահմանափակ հասանելիության տեղեկատվությունը.

4) բնակչության համար՝ պետական, տեղական ինքնակառավարման մարմինների և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպությունների կողմից տրամադրվող էլեկտրոնային ծառայությունները:

2. Կիբեռանվտանգության ապահովման ուղղություններն են՝

1) պետական և տեղական ինքնակառավարման մարմինների, հատուկ կարևորության օբյեկտների և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպությունների տեղեկատվական համակարգերի և հեռահաղորդակցական ցանցերի, ստացվող/տրամադրվող էլեկտրոնային ծառայությունների, ինչպես նաև էլեկտրոնային ձևով մշակվող, շրջանառվող և պահպանվող, Հայաստանի Հանրապետության օրենսդրությամբ պաշտպանման ենթակա, սահմանափակ հասանելիության տեղեկատվության պաշտպանությունը: Գործունեության շարունակականության ապահովումը վթարային և արտակարգ իրավիճակներում.

2) էլեկտրոնային ծառայություններ մատուցող ոչ պետական կազմակերպություններին մատուցվող էլեկտրոնային ծառայությունների և էլեկտրոնային ձևով մշակվող, շրջանառվող և պահպանվող, Հայաստանի Հանրապետության օրենսդրությամբ պաշտպանման ենթակա, սահմանափակ հասանելիության տեղեկատվության պաշպանությունը.

3) էլեկտրոնային ծառայություններ չմատուցող ոչ պետական կազմակերպություններին պետական, տեղական ինքնակառավարման մարմինների և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպությունների կողմից պաշտպանված և հուսալի էլեկտրոնային ծառայությունների տրամադրումը և այդ կազմակերպություններում էլեկտրոնային ձևով մշակվող, շրջանառվող և պահպանվող, Հայաստանի Հանրապետության օրենսդրությամբ պաշտպանման ենթակա, սահմանափակ հասանելիության տեղեկատվության պաշպանությունը.

4) բնակչությանը պետական, տեղական ինքնակառավարման մարմինների և էլեկտրոնային ծառայություններ մատուցող պետական կազմակերպությունների

կողմից պաշտպանված և հուսալի էլեկտրոնային ծառայությունների տրամադրման ապահովումը.

5) պետական պաշտոնական էլեկտրոնային տեղեկատվության պաշտպանությունը.
6) էլեկտրոնային հաղորդակցության միջոցներով ապատեղեկատվության հրապարակման և տարածման, հավաստի տեղեկատվության արգելափակման, մասնավորապես, ազգային, ռասայական և կրոնական թշնամանքի տարածման դեմ պայքարը
7) կիբեռգրոհների դեմ պաշտպանությունը.
8) կիբեռահաբեկչության դեմ պայքարը.
9) կիբեռհանցավորության դեմ պայքարը:

Հավելված N 2
ՀՀ կառավարության 2011 թ.
դեկտեմբերի 22-ի նիստի N 50
արձանագրային որոշման

ՑԱՆԿ

Հայաստանի Հանրապետության կառավարության 2010 թվականի փետրվարի 25-ի «Հայաստանի Հանրապետությունում էլեկտրոնային հասարակության ձևավորման հայեցակարգին հավանություն տալու մասին» N 7 արձանագրային որոշմամբ սահմանված աշխատանքներում, Հայաստանի Հանրապետության կառավարությունում տեղեկատվական անվտանգության իրավիճակի նախնական աուդիտի և ռիսկերի վերլուծության համար անհրաժեշտ տեղեկությունների

Գերատեսչության և նրան ենթակա կառույցների՝

1) յուրաքանչյուր տեղեկատվական համակարգի (այսուհետ՝ ՏՀ) նշանակությունը և մշակվող տվյալների բնյութը (գաղտնի, ծառայողական ընդհանուր և/կամ յուրահատուկ տվյալներ, աշխատակիցների և/կամ քաղաքացիների անհատական տվյալներ, գիտատեխնիկական, տնտեսական, արտադրական, ֆինանսական, ռազմական, քաղաքական տվյալներ և այլն).
2) ՏՀ-ներում գործող սերվերների, տվյալների բազաների նշանակությունը և քանակը, դրանց միացված համակարգիչների քանակը, միացման ենթակառուցվածքը (լոկալ ցանց, հեռավոր օգտվող, ինտերնետ) և եղանակները (լարային, ռադիոկապ, սեփական և/կամ վարձակալված կապուղիներ, հանրային օգտագործման ցանցեր), կիրառված ցանցային արձանագրությունները, օպերացիոն համակարգերի, տվյալների բազաների կառավարման համակարգերի և կիրառական ծրագրերի անվանումները.
3) առանձին (ՏՀ–ներում չընդգրկված) համակարգիչների քանակը և նշանակությունը, օպերացիոն համակարգերի և կիրառական ծրագրերի անվանումները: Եթե միացված են որևէ ցանցի, ապա դրա նպատակը (ցանցային տպիչից օգտվել, ինտերնետին միանալ և այլն).

4) ներքին ցանցային ենթակառուցվածքի ընդհանուր կառուցվածքը: Արտաքին ցանցերին, այդ թվում՝ ինտերնետին, համակցման ձևերը և նկարագրումը: Ցանցային և հեռահաղորդակցական սարքերի նշանակությունը և անվանումները դրանց համառոտ բնութագրերով (երթուղիչ, մոդեմ և այլն).
5) ինտերնետ մատուցող կազմակերպությունը և նրանից ստացվող ծառայությունները.
6) գերատեսչական ինտերնետային կայքերի հասցեները և դրանց տեղակայման համար սերվերային տարածք տրամադրած կազմակերպությունները: Կայքերը մշակող, կազմակերպությունների, կայքերի սպասարկում և շահագործում իրականացնողների տվյալները: Եթե կայքերը տեղակայված են գերատեսչական սերվերներում, ապա նաև սերվերների և կիրառված ծրագրային ապահովման բնութագրերը.
7) սեփական միջոցներով կազմակերպված և շահագործվող էլեկտրոնային ծառայությունների նկարագրումը և դրանց տեխնիկական և ծրագրային ապահովման բնութագրերը.
8) նշված բոլոր կետերին վերաբերող՝ տեղեկատվական անվտանգության ապահովման գծով իրականացված կազմակերպական և տեխնիկական միջոցառումների մասին, որոնք ուղղված են տեղեկատվության գաղտնիության, ամբողջականության և մատչելիության պահպանմանն, այդ թվում՝ վթարային և արտակարգ իրավիճակների դեպքերում: Մասնավորապես, պետք է ներկայացնել համառոտ տեղեկություններ հետևյալի մասին՝

   ա. տեղեկատվական ռեսուրսների պաշտպանության և դրանց անվտանգության վերահսկման համար կիրառվող տեխնիկական և ծրագրային միջոցները, դրանց նշանակությունը,

   բ. տեղեկատվական անվտանգության ապահովման համար նշանակված պատասխանատու ստորաբաժանման կամ աշխատակիցների առկայությունը,

   գ. տեղեկատվական անվտանգության ապահովմանը վերաբերող նախագծային, շահագործման և այլ ելային փաստաթղթերի առկայությունը,

   դ. տեղեկատվական անվտանգության քաղաքականության և դրանից բխող նորմատիվային և հանձնարարական փաստաթղթերի առկայությունը,

   ե. ադմինիստրատորների, ինժեներական և կիբեռանվտանգության անձնակազմի գործառնական պարտականությունների, օգտագործողների ձեռնարկների,

տեղեկատվական ռեսուրսներին առնչության սահմանափակումների կանոնների և ցուցակների, տեղեկատվական ռեսուրսների կարևորության և գաղտնիության դասակարգման առկայությունը,

զ. օգտվողների և սպասարկողների կազմակերպական կառուցվածքի և կառավարման մեխանիզմների առկայությունը,

է. տեղեկատվական ռեսուրսներին չթույլատրված առնչության փորձերի կանխարգել-մանը և արձագանքմանն ուղղված մշակված պլանների և գործողությունների առկայությունը,

ը. կիբեռհարձակումների հայտնաբերման և հակազդման միջոցների, դեպքերի գրանցման համակարգերի վերաբերյալ տվյալներ,

թ. ցանցային կառավարման և մոնիթորինգի հնարավորությունների մասին տվյալներ,

ժ. ՏՀ–ների, ցանցերի, կապուղիների, էլեկտրասնուցման և հողանցման կառուց-վածքային սխեմաների առկայությունը: Դրանց ֆիզիկական պաշպանության մասին տվյալներ,

ժա. կատարված աուդիտների (ներքին/արտաքին) և դրանց արդյունքների մասին տվյալներ,

ժբ. ցանցային համակցումների և տեղեկատվական համակարգերին առնչության վերաբերյալ էլեկտրոնային արձանագրությունների պահպանման մասին տվյալներ (ինչ տվյալներ են պահպանվում և ինչքան ժամանակով):