Տեղեկատվական անվտանգության հիմնահարցերը

Տեղեկությունների հավաքագրման և տարածման գործընթացները հանգեցրին նոր ոլորտի ձևավորմանը, որը «տեղեկատվություն» և «հաղորդակցություն» տերմինների միավորմամբ ստացել է տեղեկատվական–հաղորդակցական անվանումը: Առավել պատկերավոր ներկայացնելու համար նշենք, որ վերջին 50 տարում տեղեկատվության արագությունը ավելացել է 300000 անգամ[1]:

Առօրյա գիտակցական մակարդակում «անվտանգություն» հասկացությունը բնորոշվում է որպես «վտանգի բացակայություն», «վիճակ, երբ վտանգ չի սպառնում»: «Վտանգ» հասկացությունն իր հերթին նշանակում է որևէ «վտանգի հնարավորություն, սպառնալիք»:

Տեղեկատվական անվտանգությունը, դա տեղեկատվության և նրան աջակցող ենթակառուցվածքների պաշտպանությունն է, պատահական, կամ կանխամտածված, բնական կամ արհեստական բնույթի ազդեցությանից, ինչը կարող է տեղեկատվական հարաբերությունների սուբյեկտներին հասցնել անընդունելի վնաս:

Հիմնահարցով զբաղվող արտասահմանյան գործակալություններում «Տեղեկատվական անվտանգությունը» դիտվում է որպես ընդհանուր անվտանգության առանձին բաժին այնպիսի հասկացությունների կողքին, ինչպիսիք են «համակարգչային անվտանգությունը, «ցանցի անվտանգությունը, հեռահաղորդակցության անվտանգությունը «տվյալների անվտանգությունը և այլն: Ուստի կարող ենք ասել, որ տեղեկատվական անվտանգությունը հասարակության տեղեկատվական միջավայրի պաշտպանվածությունն է և ավելի լայն հասկացություն է, քան միայն ցանցի կամ համակարգչի անվտանգությունը: Տարբեր է հասկացության բովանդակությունը նաև անգլալեզու, ռուսերեն ու հայերեն գրականության մեջ, ինչպես նաև հայեցակարգային փաստաթղթերում: Հասկացության մեկ այլ սահմանմամբ՝ «Տեղեկատվական անվտանգությունը»

տեղեկույթի և տեղեկատվական համակարգերի՝ չարտոնված մուտքից, օգտագործումից, հրապարակումից, փոփոխակումից կամ ոչնչացումից պաշտպանությունն է, որպեսզի ապահովված լինեն գաղտնիությունը, ամբողջականությունը և մատչելիությունը»: Այս իմաստով տեղեկատվական անվտանգության հոմանիշներն են «կիբեռանվտանգությունը» (Cyber- security) և համակարգչային անվտանգությունը(Computer security):

Տեղեկատվական անվտանգության հիմնարար հասկացությունները ներառում են մի շարք կարևոր բաղադրիչներ և սկզբունքներ, որոնք անհրաժեշտ են տեղեկությունների պաշտպանության և դրանց անխափանության ապահովման համար: Ահա դրանցից հիմնականները.

1. **Տեղեկատվության գաղտնիություն (Confidentiality):** Գաղտնիությունը նշանակում է, որ տեղեկատվությունը հասանելի է միայն լիազորված անձանց և արգելափակված է անօրինական հասանելիությունից: Տվյալների գաղտնիության ապահովումը պաշտպանում է անձնական և զգայուն տեղեկությունները չարտոնված մուտքից:
2. **Տվյալների ամբողջականություն (Integrity):** Տվյալների ամբողջականությունն ապահովում է, որ տեղեկությունները մնան ճշգրիտ և չփոփոխված չարտոնված փոփոխությունների արդյունքում: Սա կարևորվում է, որպեսզի տվյալները պահպանվեն այն տեսքով, ինչ դրանք մշակվել կամ փոխանցվել են:

Հասանելիություն (Availability): Հասանելիությունը նշանակում է, որ լիազորված օգտատերերը կարող են հասանելիություն ունենալ իրենց անհրաժեշտ տեղեկություններին, երբ դրա կարիքը ունեն: Սա ներառում է միջոցառումներ, որոնք պաշտպանում են տվյալների հասանելիությունը համակարգերի խափանումներից կամ կիբեռհարձակումներից:

3. **Հավաստիություն (Authenticity**): Հավաստիությունն ապահովում է, որ տեղեկատվության աղբյուրը իսկական է և չի կեղծվել: Սա վերաբերում է ինչպես տվյալների, այնպես էլ օգտատերերի նույնականացմանը:
4. **Հետևելիություն (Accountability):** Հետևելիությունն ապահովում է, որ բոլոր գործողությունները համակարգում հնարավոր լինի հետևել և համապատասխան պատասխանատվություն սահմանել: Սա ներառում է օգտագործողների

գործողությունների արձանագրում և մուտքագրումների հսկողություն:

5. **Չհրաժարում (Non-repudiation):** Չհրաժարումը նշանակում է, որ հաղորդագրության կամ գործողության հեղինակը չի կարող հրաժարվել կամ հերքել իր կատարած գործողությունը: Սա կարևոր է իրավաբանական իրավիճակներում, որտեղ անհրաժեշտ է հաստատել գործարքների կամ հաղորդակցությունների իսկությունը:
6. **Ռիսկի կառավարում (Risk Management):** Տեղեկատվական անվտանգության կարևոր բաղադրիչներից է ռիսկի վերլուծությունն ու կառավարումը, որը ներառում է հնարավոր սպառնալիքների և խոցելիությունների բացահայտումը, ինչպես նաև նրանց դիմակայելու միջոցների կիրառումը:
7. **Մուտքի կառավարում (Access Control):** Մուտքի կառավարումը նախատեսված է այն միջոցառումների համար, որոնք վերահսկում են, թե ով և ինչ պայմաններում կարող է հասանելիություն ունենալ տեղեկատվական համակարգերին:

Այս հասկացությունները միասին ապահովում են տեղեկությունների արդյունավետ պաշտպանությունը և օգնում են կազմակերպություններին և անձանց ապահովել իրենց տվյալների անվտանգությունը:

Տեղեկատվական անվտանգության հիմնահարցի ուսումնասիրության երկու հիմնական ուղղություն կարելի է առանձնացնել: **Առաջինի համաձայն՝** հասկացությունը կարելի է սահմանել որպես հենց տեղեկատվական ռեսուրսների՝ տեղեկատվության ու տեխնոլոգիաների անվտանգություն: Այս դեպքում տեղեկատվական անվտանգության ապահովման համար կարևոր են տեղեկատվական ենթակառուցվածքի անխափան գործունեության ապահովումը, այն կանխամտածված կամ պատահական ազդեցությունից պաշտպանելը: Այլ կերպ ասած՝ այս ուղղությունը հիմնականում շոշափում է տեխնիկական խնդիրները: **Երկրորդ ուղղությունն** ավելի լայն է և ընդգրկում է ընդհանուր անվտանգության ապահովման համար տեղեկատվական ռեսուրսների դերը, դրանց կիրառման արդյունավետությունը: Փաստորեն, այս դեպքում ուշադրություն են դարձվում ազգային անվտանգության ապահովման ժամանակ տեղեկատվական ռեսուրսների դերին ու նշանակությանը: Այսպիսով, տեղեկատվական անվտանգությունը

ուսումնասիրվում է նեղ և լայն առումներով: Առաջին դեպքում շեշտը դրվում է դրա տեխնիկական բաղադրիչի վրա, իսկ մյուս պարագայում ընդգրկվում են տեղեկատվական անվտանգության բոլոր սուբյեկտները: