ՀՀ ԱՐԴԱՐԱԴԱՏՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ
ԳՈՐԾԱԿԱԼՈՒԹՅՈՒՆ

ՏԵՍԱՀՍԿՄԱՆ ՈՒՂԵՑՈՒՅՑ

ԵՐԵՎԱՆ, 2016

ՏԵՍԱՀՍԿՄԱՆ ՈՒՂԵՑՈՒՅՑ

Տեսահսկման ուղեցույցը մշակվել է Հայաստանի Հանրապետության Արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության կողմից: Ուղեցույցի նպատակն է ներկայացնել տեսահսկման հիմնական կանոններն ու սկզբունքները՝ ապահովելով մարդկանց անձնական տվյալների պաշտպանությունը:

Ուղեցույցը մշակվել է՝ առաջնորդվելով <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքի պահանջներով և տեսահսկման կարգավորման միջազգային չափանիշներով: Տեսահսկում իրականացնող յուրաքանչյուր անձ կամ կազմակերպություն պետք է առաջնորդվի <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքով և այս ուղեցույցով:

1.Տեսահսկման համակարգը և անձնական տվյալներ պարունակող տեսագրությունները

Տեսահսկման համակարգը տարածքի, միջոցառման, գործունեության կամ անձի տեսա/ձայնահսկումն է էլեկտրոնային սարքավորման միջոցով: Համակարգը կարող է աշխատել տեսագրման ռեժիմով (երբ տեսագրվում է) և իրական ժամանակում տվյալների փոխանցման եղանակով:

Տեսահսկման համակարգով կատարված տեսագրությունը համարվում է անձնական տվյալ, եթե՝

- հնարավոր է նույնականացնել տեսագրության մեջ երևացող անձի դեմքը (ուղղակի նույնականացում)

  կամ

- ահնար է նույնականացնել անձի դիմային առանձնահատկությունները, բայց տեսանկարահանված անձի ֆիզիկական կամ վարքագծային առանձնահատկություններն այլ տվյալի հետ համեմատելով՝ հնարավոր է նույնականացնել անձին (անուղղակի նույնականացում):

  Այսպիսով, մարդու տեսանկարն անձնական տվյալ է, որը թույլ է տալիս ուղղակի կամ անուղղակի նույնականացնել անձին: Հետևաբար, տեսախցիկի միջոցով իրականացվող տեսանկարահանումը և տեսահսկողությունը (այսուհետ՝ տեսահսկում), որպես անձնական տվյալի մշակում, նախատեսում է անձնական տվյալի մշակման, օգտագործման և պաշտպանության պահանջների և սկզբունքների ապահովում:

2. Տեսահսկման համակարգի տեղադրման և օգտագործման սկզբունքները

Տեսահսկումը տարածությունը և վարքագիծը մշտադիտարկելու/վերահսկելու միջոցներից մեկն է, բայց ոչ միակը: Քանի որ տեսահսկումն միջամտություն է անձնական կյանքին, տվյալներ մշակողը պետք է իրապես գնահատի սպառնալիքը և հիմնավորի նման համակարգի օգտագործման անհրաժեշտությունը: Մասնավորապես, պետք է գնահատել հետևյալը՝

- Տվյալներ մշակողի իրական անհրաժեշտությունը և նպատակը
- Համակարգի ազդեցությունը անձի մասնավոր կյանքի իրավունքի նկատմամբ
- Այլ միջոցներով նպատակին հասնելու հնարավորությունները

Տեսահսկման համակարգը պետք է տեղադրվի և շահագործվի օրինականության, համաչափության, թափանցիկության և անվտանգության սկզբունքների պահպանմամբ:

2.1 *Օրինականության սկզբունք:*

Տեսահսկումը պետք է իրականացվի միայն օրենքով նախատեսված նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով: Օրինակ, կրթական հաստատությունում գույքի պաշտպանությունը ապահովելու նպատակով տեղադրված տեսահսկման համակարգը արգելվում է օգտագործել վերահսկելու ուսումնական գործընթացը:

Տեսահսկման համակարգի տեղադրումը կարող է հետապնդել մեկից ավելի օրինական նպատակ: Օրինակ՝ առաջին օրինական նպատակը կարող է լինել հանցագործությունների հայտնաբերումը և կանխումը, իսկ երկրորդը՝ ճանապարհային երթևեկության անվտանգության ապահովումը:

2.2 *Համաչափության սկզբունք:*

Տվյալներ մշակողը պետք է տեսահսկման համակարգը օգտագործի միայն այն դեպքերում, երբ այլ եղանակներով անհնար է հասնել հետապնդվող նպատակին կամ պահանջվում է անհամաչափ ջանքեր:

Պետք է հավասարակշռություն լինի հետապնդվող նպատակի և նկարահանվող անձի մասնավոր կյանքի պաշտպանության միջև (Արդյո՞ք անհրաժեշտ է տեսախցիկ տեղադրել բժշկի սպասասրահում): Տեսահսկողը պարտավոր է տեսանկարները մշակել այն նվազագույն ծավալով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար: Տեսախցիկը պետք է տեղադրվի այնպես, որ նրա տեսադաշտը ճշգրտորեն մտնեն միայն այն պատկերները, որոնք համապատասխանում են հսկողության նպատակին (համաչափության սկզբունք): Օրինակ, բնակելի շենքի տեսահսկման դեպքում պետք է անհնար լինի տեսնել, թե ով որ բնակարանն է մտնում:

Տեսաձայնագրում իրականացնելիս տեսահսկողը պարտավոր է հիմնավորել տեսաձայնագրման անհրաժեշտությունը: Միաժամանակ, տեսաձայնային հսկողություն իրականացնող համակարգերի օգտագործման դեպքում տվյալներ մշակողը համաչափության սկզբունքին համապասխան պարտավոր է հիմնավորել ձայնային վերահսկման անհրաժեշտությունը:

Տեսահսկման արդյունքում հավաքված տվյալները (ներառյալ տեսագրությունները և նկարները) պետք է պահպանվեն հետապնդվող նպատակին հասնելու համար անհրաժեշտ ժամկետում: Տեսախցիկով գրանցված անձնական տվյալները պետք է ջնջվեն որոշակի ժամկետում: Մարդկանց և գույքի նկատմամբ կատարված հանցանքների արձանագրումը շատ դեպքերում տեղի է ունենում դրանց իրագործմանը հաջորդող ժամերում: Ուստի հետապնդվող նպատակի տեսանկյունից 24 ժամը բավարար է տվյալների պահպանման համար, քանի դեռ այդ ժամկետում չի արձանագրվել անձանց կամ գույքին վնաս պատճառելու դեպք: Սակայն օբյեկտիվ և կարևոր շարժառիթների առկայության դեպքում տվյալների պահպանման ժամկետը կարող է երկարաձգվել (համաչափության սկզբունք):

Որքան տվյալները ավելի երկար ժամկետով են պահպանվում, այդքան դրանց անվտանգության պահանջները խստացվում են:

2.3 Թափանցիկության սկզբունք

Թափանցիկության սկզբունքը ներառում է մի կողմից տեսահսկում իրականացնողի պարտականությունը տեղեկացնելու տեսահսկման իրականացման վերաբերյալ տեսահսկվող անձանց **(բարեխղճության սկզբունք),** իսկ մյուս կողմից՝ տեսահսկվող անձանց իրենց անձնական տվյալների վերաբերյալ տեղեկություններ ստանալու իրավունքը **(տեղեկատվության մատչելիության սկզբունքը):**

2.3.1 Բարեխղճության սկզբունք

Տեսահսկում իրականացնող սուբյեկտը տեսանելի նախազգուշացման միջոցով պետք է տեսախցիկների նկարահանման դաշտ մտնող բոլոր անձանց տեղեկացնի տեսահսկման մասին: Այն դեպքում, երբ այդ պատկերները ցանկացած ձևով տեսաձայնագրվում են, տեսանելի ծանուցումը պետք է պարունակի նաև տեղեկություն, թե ում մոտ նկարահանվող մարդիկ կարող են իրականացնել իրենց վերաբերյալ տեղեկատվության մուտքի իրավունքը: Օրինակ, բնակելի շենքում պետք է տեսահսկման վերաբերյալ նախազգուշացումը ակնհայտորոն տեսանելի լինի շենք մտնող յուրաքանչյուր անձի համար:

Եթե տեսահսկման տարածքն ընդարձակ է, տեսահսկողը կարող է ունենալ մի քանի նախազգուշացնող նշաններ կամ մեկ նշան՝ մուտքի դռան մոտ:

2.3.2 Տեղեկատվության մատչելիության սկզբունք

<<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքը սահմանում է, որ յուրաքանչյուրն ունի իր անձնական տվյալների մշակման մասին տեղեկություն ստանալու իրավունք: Սա վերաբերում է նաև տեսահսկման միջոցով անձնական տվյալներ մշակելուն: Օրենքի 15-րդ հոդվածի համաձայն՝ անձն իրավունք ունի ստանալ տեղեկություն իրեն տեսահսկելու եղանակների (օրինակ՝ տեսագրում կամ տեսաձայնագրում), հիմքերի և նպատակների, տեսահսկվող տվյալների ցանկի (սահմանների) և տեսագրությունը ձեռք բերելու աղբյուրների մասին, ինպես նաև այն անձանց շրջանակը, որոնց կարող է փոխանցվել իր տեսագրությունը:

Յուրաքանչյուր անձնական տվյալ մշակող՝ տեսահսկում իրականացնող պետական կամ մասնավոր մարմին պարտավոր է տեսահսկման սուբյեկտին հնարավորություն ընձեռել անվճար ծանոթանալու տեսահսկման սուբյեկտին վերաբերող տեսագրությանը (տեսաձայնագրությանը), իսկ եթե տեսահսկում իրականացնողը պահպանում է տեսագրությունը (այսինքն կա տեսագրությունը ձեռք բերելու աղբյուր), ապա տեսահսկման սուբյեկտը իրավունք ունի նաև ստանալ տեսագրության կրկնօրինակը (ձեռք բերել տեսագրությունը):

Տեսահսկում իրականացնողը տեղեկությունները պետք է տրամադրի հասանելի ձևով, իսկ այդ տեղեկությունները չպետք է պարունակեն այլ սուբյեկտների անձնական տվյալներ:

Հարկ է նշել, որ տեղեկությունները պետք է տրամադրվեն անվճար, եթե օրենքով այլ բան նախատեսված չէ: Տեսահսկման սուբյեկտը տեսագրությունը կարող է ստանալ նաև *իր* ներկայացրած կրիչով՝ կրկին անվճար: Եթե տեսահսկման սուբյեկտը չի նշել, թե ինչ կրիչով է ցանկանում ստանալ տեսագրությունը, ապա այն տրամադրվում է տեսահսկում իրականացնողի համար առավել ընդունելի կրիչով:

Կարևորագույն սկզբունք է, որ անձի մասին տեղեկությունները չպետք է վաճառվեն նրան, իսկ վճարելու անհրաժեշտությունը պետք է կապված լինի միմիայն տեսագրության տրամադրման համար տեսահսկողի կատարած ծախսերը փոխհատուցելու հետ:

Տեղեկությունները պետք է տրամադրվեն գրավոր հարցումը ստանալուց հետո՝ հինգ օրվա ընթացքում (օրենքի 20-րդ հոդված, 1-ին մաս):

Կարևոր է, որ տեսահսկում իրականացնողը սահմանի տեսահսկման և տեղեկությունների տրամադրման ներքին ընթացակարգեր, որվոհետև այդպիսով տեսահսկվողի համար պարզ են դառնում տեսահսկման կանոնները, այն պայմանները, թե ինչպես, պատասխանատու որ անձի միջոցով տեսահսկվողը կարող է ստանալ իրեն հետաքրքրող հարցերի պատասխանը, ում և ինչպես պետք է դիմի իր տեսագրության մասին տեղեկություններ կամ տեսագրության կրկնօրինակը ստանալու համար, ինչպես կարող է ծանոթանալ իր տեսագրությունը մշակելու պայմաններին, ում և ինչպես պետք է դիմի իր տեսահսկվողի մոտ պահվող տեսագրության անվտանգության ապահովման հարցերով և այլն: Ընթացակարգեր ունենալը խրախուսելի է, որը պետք է համապատասխանի <<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքին:

Տեսահսկողը պետք է ունենա նաև բողոքարկման ընթացակարգեր, ներքին վերանայման մեխանիզմներ, բողոքարկմանը լուծում տալու ժամկետներ և այլն

2.4 Անվտանգության սկզբունք:

1. Տեսահսկողական համակարգի պատասխանատուն պետք է կազմակերպական և տեխնիկական միջոցառումներ ձեռնարկի պաշտպանելու համար անձնական տվյալները չթույլատրված մշակումից (տվյալների անվտանգության սկզբունք):

Օրինակ, գրանցված տվյալները պետք է պահպանվեն հուսալի և բանալիով փակ վայրում: Տեսանկարների անվտանգությունն ապահովելու կարևոր պայմաններից է լավ պաշտպանված օպերացիոն կամ տեխնիկական, կազմակերպչական և ֆիզիկական համակարգերը: Համակարգերը լավ են պաշտպանված, եթե լիազորված աշխատակազմից բացի ուրիշ որևէ մեկը մուտք չունի համակարգ: Անհրաժեշտ է պարբերաբար ստուգել օպերացիոն համակարգերը, երաշխավորել տեսանկարների անվտանգությունը և գաղտնիությունը, կանխել դրանց կորուստը և անօրինական ձեռքբերումը:

Տեղեկատվական համակարգերում անձնական տվյալները մշակելու անվտանգությունն ապահովելուն ներկայացվող պահանջները, կենսաչափական անձնական տվյալների նյութական կրիչներին և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալները պահպանելու տեխնոլոգիաներին ներկայացվող պահանջները սահմանվում են Հայաստանի Հանրապետության կառավարության 2015 թվականի հոկտեմբերի 15-ի N 1175-Ն որոշմամբ:

Մշակողները կարող են կիրառել նաև <<Տեղեկատվության անվտանգության կառավարման>> ՀՍՏ ԻՍՈ/ԻԷԿ 27000 շարքի միջազգային չափանիշներն այնքանով, որքանով դրանք իրենց էությամբ կիրառելի են կենսաչափական անձնական տվյալների նյութական կրիչների և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալների պահպանման տեխնոլոգիաների նկատմամբ:

Ցանկացած տեսահսկման համակարգի նյութական կրիչ (օրինակ տեսախցիկ) պետք է ունենա եզակի նույնականացման համար և հաշվառված լինի մշակողի կողմից (ՀՀ կառավարության N 1175-Ն որոշում):

2. Գրանցված կամ ուղղակիորեն հաղորդված անձնական տվյալներ մուտք ունեցող անձանց թիվը պետք է հնարավորինս սահմանափակ լինի (տվյալների անվտանգության և համաչափության սկզբունք):

Օրինակ, դիսկոտեկայում միայն անվտանգության ապահովման համար լիազորված անձինք պետք է մուտք ունենան տեսախցիկների տվյալներ: Անձնակազմի մյուս անդամների մուտքը պետք է արգելվի:

Տեսահսկման համակարգի էկրանները պետք է այնպես շրջված լինեն, որ միայն թույլատրված/լիազորված անձը կարողանա տեսնել պատկերները: Հանրային էկրանները արգելված են:

3. Գրանցված տվյալները չպետք է հրապարակվեն, բացառությամբ, եթե տվյալներն այլ անձանց փոխանցվում են օրենքով նախատեսված դեպքերում:

Օրինակ, առևտրային կենտրոնը իրավունք չունի երրորդ անձանց հանձնել կամ վաճառել գրանցված պատկերները, ինչպես նաև դրանք տեղադրել ինտերնետում:

3. Տեսահսկման նպատակները

3.1 Տեսահսկումը հասարակական վայրերում

Հասարակական վայրերում (փողոցներ, մայթեր, հրապարակներ, խաղահրապարակներ, զբոսայգիներ, պուրակներ, հանրային տրանսպորտի կանգառներ և այլ հասարակական վայրեր) իրականացվող տեսահսկումը պետք է ունենա հստակ սահմանված իրավաչափ նպատակ կամ նպատակներ և պայմանավորված լինի խիստ անհրաժեշտությամբ: Այդպիսի իրավաչափ նպատակ և խիստ անհրաժեշտություն կարող են լինել՝

- ազգային անվտանգությունը
- հասարակական անվտանգությունը
- երկրի տնտեսական բարեկեցությունը
- հանցագործությունների և խռովությունների կանխումը
- առողջության կամ բարոյականության պաշտպանությունը
- այլոց իրավունքների և ազատությունների պաշտպանությունը
- տրանսպորտային երթևեկության կարգավորումը

Հասարակակական վայրերում տեսահսկումը կարող է իրականացվել նաև բնական և տեխնածին վտանգները կանխելու, անձանց արագ և դյուրին կերպով բուժօգնություն ցուցաբերելու նպատակով:

Փողոցների տեսահսկումն իրականացվում է նաև ճանապարհային երթևեկության անվտանգությունն ապահովելու նպատակով, մասնավորապես, ճանապարհային երթևեկության կանոնների խախտումները արձանագրելու շրջանակներում տեսագրությունները կամ տեսանկարները դրվում են վարորդներին վարչական պատասխանատվության ենթարկելու վարչական վարույթների հիմքում *(տես՝ <<Տեսանկարահանող կամ լուսանկարահանող սարքերով հայտնաբերված ճանապարհային երթևեկության կանոնների խախտումների վերաբերյալ գործերով իրականացվող վարչական վարույթի առանձնահատկությունների մասին>> ՀՀ օրենքը):*

Հասարակական վայրերում տեսահսկումը կարող է իրականացվել միայն հանրային իշխանությունների կողմից (օր՝ քաղաքապետարան, ոստիկանություն):

Հասարակական վայրերում տեղադրված տեսահսկման սարքերը չպետք է նկարահանեն բնակելի շենքերի մուտքը և ներսը, այդ թվում՝ պատուհանները և պատշգամբները:

3.2. Տեսահսկումը պետական և մասնավոր հաստատությունների շենքերում

Պետական կամ մասնավոր հաստատությունների (հանրային իշխանության մարմինների գործունեության իրականացման համար տրամադրված շենքեր, թանգարաններ, ռեստորաններ, սրճարաններ, խանութներ, մարզադահլիճներ, բնակելի շենքեր) շենքերում տեսահսկումն իրականացվում է՝

- անձանց և սեփականության անվտանգությունը ապահովելու
- գաղտնի տեղեկատվությունը պաշտպանելու
- անչափահասներին վնասակար ազդեցություններից պաշտպանելու

Նման հաստատություններում տեսախցիկները տեղադրվում են ընդհանուր օգտագործման վայրերում (շենքի մուտք, միջանցքներ, սանդուղքներ,ավտոկայանատեղի, անմիջական հարակից տարածք):

Պետական և մասնավոր հաստատությունների շենքերի աշխատասենյակներում, հանդերձարաններում, սանհանգույցներում, հանգստի սենյակներում, լողասենյակներում տեսահսկումն արգելվում է:

3.2.1. Տեսահսկումը աշխատավայրում

Աշխատավայրում տեսահսկման համակարգը տեղադրվում է բացառիկ դեպքերում, եթե դա անհրաժեշտ է անձանց անվտանգությունը և գույքը գողանալուց կամ այն վնասներից պաշտպանելու և նման արարքների հեղինակներին հայտնաբերելու, ինչպես նաև գաղտնի տեղեկատվությունը պաշտպանելու նպատակով, եթե այլ միջոցներով հնարավոր չէ հասնել այդ նպատակներին:

Աշխատավայրում տեսահսկման համակարգ տեղադրելուց առաջ տեսահսկողը պարտավոր է աշխատակազմին գրավոր տեղեկացնել համակարգի և աշխատողների իրավունքների մասին: Նախքան տեսահսկման համակարգ տեղադրելը աշխատակիցներին անհրաժեշտ է բացատրել տեսահսկման անհրաժեշտությունը, նպատակը և նրանց իրավունքները:

Տեսախցիկները կարող են նկարահանել աշխատավայրի շենքի մուտքը և ելքը, միջանցքները, ինչպես նաև թանկարժեք ապրանքների գտնվելու վայրերը և պահեստները: Տեսահսկման սարքերը չեն կարող նկարահանել աշխատողների աշխատասենյակները, բացառությամբ հատուկ հանգամանքների առկայության դեպքում (օր՝ աշխատողը, որն առնչվում է փողերի հետ, բայց այդ դեպքում պետք է

նկարվի դրամարկղը, ոչ թե գանձապահը, պահեստը, որտեղ աշխատում են բանվորները):

Ինչպես այլ վայրերում, այնպես էլ աշխատավայրում աշխատողները իրենց անձնական կյանքը հարգելու իրավունք ունեն: Տեսահսկումն արգելվում է աշխատողների **հանգստի և ընդմիջման սենյակներում, սանհանգույցներում և հանդերձարաններում:**

3.2.2. Տեսահսկումը բնակելի շենքերում և բնակարաններում, առանձնատներում

3.2.2.1. Բնակելի շենքերում տեսահսկման համակարգը տեղադրվում է **մարդկանց և գույքի անվտանգությունը ապահովելու նկատառումով:** Տեսահսկման համակարգը տեղադրելու համար պահանջվում է ձեռք բերել բնակարանների սեփականատերերի կեսից ավելիի գրավոր համաձայնությունը: Շենքի բոլոր բնակիչները պետք է տեղեկացված լինեն տեսահսկման համակարգ տեղադրված լինելու մասին:

Բնակելի շենքերում տեսախցիկները կարող են նկարել միայն **շենքի մուտքը և ընդհանուր օգտագործման տարածությունները** (ընդունարան, միջանցք, սանդուղք, վերելակի դռներ, ավտոկայանատեղի):

Արգելվում է տեսահսկել բնակարանների մուտքի դռները և պատշգամբները, բացառությամբ, եթե բնակարանի սեփականատերն ինքն է նման որոշում կայացրել կամ առկա է վերջինիս գրավոր համաձայնությունը:

Բնակելի շենքերում պետք է տեսահսկման վերաբերյալ նախազգուշացումն ակնհայտորեն տեսանելի լինի շենք մտնող յուրաքանչյուր անձի համար:

3.2.2.2. Անձը իր բնակարանում, առանձնատանը կարող է տեղադրել տեսախցիկներ իր անվտանգությունը ապահովելու համար[1]: Առանձնատան սեփականատերն իրավունք ունի տեսահսկել իր առանձնատունը և դրա այգին, բայց չի կարող իր հողամասի սահմաններից դուրս նկարահանել, եթե չունի համապատասխան հարևանի համաձայնությունը:

Տեսագրությունները, տեսախցիկի միջոցով գրանցված նկարները չեն կարող օգտագործվել այլ նպատակներով (նկարները համացանցում տարածել), քան բնակարանի անվտանգության պաշտպանությունն է: Դրանց օգտագործումը չպետք է վնաս պատճառի այլ անձանց իրավունքներին: Անձինք նախազգուշացնող նշանների միջոցով պետք է տեղեկացված լինեն տեսախցիկների առկայության մասին Մասնավոր նպատակով իրականացվող տեսահսկումը հնարավոր է միայն **սեփական տարածքում:**

Եթե անհատը իր տանը տեղադրում է տեսախցիկներ և նրա տանը կան լրիվ կամ ոչ լրիվ աշխատաժամանակով աշխատողներ, ապա պետք է հաշվի առնվեն որոշակի կանոններ: Այսպես, եթե աշխատողը տանը պահում է երեխաներին կամ, եթե

[1] Այս դեպքում տեսախցիկների իրավական կարգավորումը դուրս է Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքի կարգավորման դաշտից, և բնակարանի սեփականատերը կարող է առանց իրավասու մարմիններին տեղեկացնելու և թույլտվությունը ստանալու տեղադրել տեսախցիկներ, պայմանով, որպեսզի չխախտվեն հարևանների, այցելուների և անցորդների անձնական կյանքի իրավունքը:

յուրաքանչյուր օր բուժանձնակազմ է բնակարան գալիս հիվանդին խնամելու համար, ապա գործում են աշխատավայրում տեսահսկման իրավական կարգավորման կանոնները: Այդ անձինք պետք է տեղեկացված լինեն տեսախցիկների տեղադրման և դրանց նպատակների մասին: Արգելվում է տեսահսկել լրիվ աշխատաժամանակով աշխատող աշխատողներին իրենց մասնագիտական գործունեությունը կատարելիս:

3.2.3. Տեսահսկումը առևտրային հաստատություններում

Տեսախցիկները կարող են տեղադրվել հանրախանութներում, սուպերմարկետներում, ոսկերչական խանութներում, վարսավիրանոցներում, դեղատներում և այլն: Նման վայրերում տեսախցիկները տեղադրվում են **անձանց և գույքի անվտանգությունը ապահովելու նպատակով** (օրինակ՝ կանխելու գողությունը կամ ավազակային հարձակաումը և/կամ այդ արարքները կատարած անձանց): Այդ նպատակով տեսախցիկները կարող են տեղադրվել առևտրային հաստատությունների երթևեկելի գոտիներում և ապրանքների գտնվելու վայրերում:

Արգելվում է տեսախցիկներ տեղադրել հանդերձարանների և սանհանգույցների ներսում:

Տեսահսկման համակարգը չի կարող օգտագործվել որպես գործիք՝ ապահովելու անձնակազմի կողմից աշխատանքը պատշաճ կատարումը: Այնուամենայնիվ, այն կարող է օգտագործվել հայտնաբերելու դրամարկղից գողություն կատարող աշխատողին: Երբ որ աշխատողի աշխատանքը կախված է փողի գործածման հետ, ապա այդ դեպքում տեսախցիկը ավելի շատ պետք է նկարի դրամարկղը քան գանձապահին:

3.2.4. Տեսահսկումը կրթական հաստատություններում

Կրթական հաստատությունների ներսում տեսախցիկները կարող են տեղադրվել անձանց և գույքի պաշտպանության նկատառումով, ինչպես նաև պաշտպանելու անչափահասներին վնասակար ազդեցություններից (կանխելու աշակերտների միջև բռնությունը, գողությունները, պատերի և դռների վնասումը, հաստատության գույքը և այլն): Տեսախցիկները կարող են տեսանկարել նաև կրթական հաստատությունների շենքերի արտաքին կողմը՝ ուժեղացնելու անվտանգությունը դրա շրջակայքում (կանխելու՝ բռնությունները, կողմնակի անձանց մուտքը):

Կրթական հաստատություններում տեսախցիկները կարող են տեսանկարել հաստատության մուտքը/ելքը, սանդուղքը, միջանցքները: Բացառությամբ բացառիկ դեպքերի, արգելվում է տեսանկարել հաստատության ներքին բակը, դասասենյակները, ճաշարանը, կացարանները և մարզասրահները և այլն:

Անձանց և գույքի անվտանգության ապահովումը պետք է իրականացվի անձանց անձնական կյանք առավել նվազ ներխուժող եղանակներով: Տեսախցիկների օգտագործումը պետք է լինի սահմանափակ և հանդիսանա լրացուցիչ միջոց անվտանգության այլ միջոցառումների թվում:

Միայն բացառիկ հանգամանքներն (երբ կրթական հաստատությունները դառնում են հաճախակի կրկնվող հակաօրինական արարքների զոհ, օր. հաճախ տեղի են ունենում գողություններ) են հիմնավորում սովորողների և դասավանդողների շարունակական տեսանկարումը[2]:

4. Տեսահսկման չափանիշները

Տեսահսկման համակարգերը պետք է համապատասխանեն հետապնդվող նպատակին և բխեն համաչափության սկզբունքից: Այս առումով տեսահսկողը պետք է հաշվի առնի հետևյալը՝

Տեսախցիկների քանակը, դրանց գտնվելու վայրը և կետայնությունը (resolution) պետք է համապատասխանեն տեսահսկման նպատակին, կազմակերպության գործունեության առանձնահատկություններին, տարածքի ընդհանուր մակերեսին, սենյակի կառուցվածքին և այլն: Տեսահսկման համակարգը պետք է տեղադրվի այնպես, որ հնարավորինս քիչ տարածք վերահսկելով հնարավոր լինի հասնել հետապնդվող նպատակին: Եթե նպատակին կարելի է հասնել ավելի ցածր կետայնությամբ տեսախցիկների օգնությամբ, ապա պետք է օգտագործել դրանք՝ խուսափելով ավելորդ անձնական տվյալներ մշակելուց:

Տեսանկարներից պետք է պարզ լինի տեսահսկման ժամը, ամսաթիվը, և վայրը:

Ուղիղ, իրական ժամանակում/ռեժիմում տվյալների փոխանցմամբ աշխատող տեսահսկումը կարող են իրականացնել միայն հատուկ թույլատվություն ունեցող անձինք (օրինակ, անվտագության աշխատակիցները): Այս ռեժիմում աշխատող տեսահսկման համակարգի էկրանները պետք է այնպես շրջված լինեն, որ միայն թույլատրված/լիազորված անձը կարողանա տեսնել տեսապատկերները: Հանրային էկրաններն արգելվում են:

5. Պատասխանատվություն

<<Անձնական տվյալների պաշտպանության մասին>> ՀՀ օրենքը խախտելու, այդ թվում անձնական տվյալ մշակելու (այդ թվում տեսահսկման միջոցով) օրենքով սահմանված կարգը խախտելու կամ տեսահսկման սուբյեկտի պահանջով մշակողի կողմից տեղեկատվություն չտրամադրելու կամ տրամադրման կարգը խախտելու համար սահմանված է վարչական պատասխանատվություն: Քանի որ տեսահսկումը նույնպես անձնական տվյալների մշակում է, վարչական պատասխանատությունը վրա կհասնի նաև տեսահսկումն առանց օրենքով սահմանված հիմքերի, առանց օրինական նպատակի կամ օրենքով սահմանված կարգի խախտմամբ իրականացնելու դեպքում: Օրենքը խախտելու համար սահմանված է տուգանք, որի չափը տարբեր

[2] Միջազգային պրակտիկայում համայնքն է որոշում, թե արդյո՞ք մանկապարտեզներում և տարրական դպրոցներում անհրաժեշտ է տեղաքդրել տեսախցիկներ, թե ոչ:

խախտումների դեպքում տատանվում է 50.000 ՀՀ դրամից մինչև 500.000 ՀՀ դրամ (տես՝ Վարչական իրավախախտումների վերաբերյալ օրենսգիրք, հոդված 189.17):

Անձն ազատվում է վարչական պատասխանատվությունից, եթե լիազոր մարմնի որոշմամբ սահմանված ժամկետում կամ մինչև վարչական պատասխանատվության ենթարկվելու վերաբերյալ որոշում կայացնելը անձը վերացրել է թույլ տված խախտումը և լիազոր մարմին է ներկայացրել ապացույցներ այդ մասին: Սա վկայում է այն մասին, որ սահմանված պատասխանատվությունն ունի ոչ միայն պատժելու, այլ նաև անձնական տվյալների պաշտպանության իրավունքի խախտումները կանխարգելելու նպատակ: