ՏԻՄ-երում անձնական տվյալների մշակման գնահատում

Շուշան Դոյդոյան

Դավիթ Սանդուխչյան

Երևան 2020

Բովանդակություն

Ներածություն

Տեղական ինքնակառավարման մարմինների (ՏԻՄ) կողմից անձնական տվյալների մշակման գնահատումն իրականացվել է Գերմանիայի միջազգային համագործակցության ընկերության՝ ԳՄՀԸ-ի (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH) աջակցությամբ:

Ուսումնասիրման նպատակն է ընտրված չորս ՏԻՄ-երում.

ա) գնահատել անձնական տվյալների մշակման համապատասխանությունը ՀՀ օրենսդրությանը և միջազգային լավագույն փորձին,

բ) գնահատել անձնական տվյալների անվտանգության ապահովման միջոցները,

գ) գնահատել անձնական տվյալների մշակման օրենսդրական պահանջների վերաբերյալ ՏԻՄ-երի աշխատակիցների իրազեկման մակարդակը և համապատասխան ուսուցման և գործիքակազմի անհրաժեշտությունը,

դ) ներկայացնել առաջարկներ ուղղված ՏԻՄ-երի կողմից անձնական տվյալների մշակման գործընթացի բարելավմանը և կատարելագործմանը:

Ուսումնասիրման առարկան մասնավորապես 3 խոշորացված համայնքներում՝ Ջերմուկում, Դիլիջանում եւ Սիսիանում ներդրված Համայնքային կառավարման տեղեկատվական համակարգի (այսուհետ՝ ՀԿՏՀ), Քաղաքացիների սպասարկման գրասենյակների (այսուհետ՝ ՔՍԳ) միջոցով մատուցվող վարչական ծառայությունների, ինչպես նաեւ Աբովյանի համայնքապետարանի կողմից մանկապարտեզների առցանց գրանցման համակարգի գործարկման նպատակով անձնական տվյալների մշակման գործընթացի ստուգումն է:

Գնահատումն իրականացրել են անձնական տվյալների պաշտպանության (այսուհետ՝ ԱՏՊ) ոլորտում 20 և ավելի տարիների փորձ ունեցող փորձագետները՝ իրավաբան, նախկինում ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալության պետ, բ.գ.թ. Շուշան Դոյդոյանը և տեղեկատվական իրավունքի և համակարգչային անվտանգության մասնագետ, փաստաբան Դավիթ Սանդուխչյանը:

Գնահատումն անցկացվել է փորձագետների կողմից մշակված մեթոդաբանության հիման վրա (տես՝ Հավելված 1): Մեթոդաբանության հիմքում դրված են եղել «Անձնական տվյալների մասին»[1] ՀՀ օրենքի պահանջները, ինչպես նաև միջազգային, մասնավորապես ԵՄ համապատասխան չափանիշները, ինչպիսիք են ISO/IEC 27001 տեղեկատվական անվտանգության ստանդարտները [2] և Եվրամիության Տվյալների պաշտպանության համընդհանուր կարգավորումը (General Data Protection Regulation կամ GDPR):[3]

[1] https://www.arlis.am/documentview.aspx?docid=98338

[2] https://www.iso.org/isoiec-27001-information-security.html

[3] https://gdpr-info.eu/

Գնահատումը բաղկացած է հետևյալ վեց բաժիններից.

1. Ամփոփ եզրակացություն, որտեղ ներկայացված են բացահայտված հիմնական խնդիրներն ու ըստ առանձին նպատակների տրված ընդհանուր գնահատականը,
2. Գնահատման նպատակների, ծավալի ու մեթոդաբանության նկարագրություն,
3. Անձնական տվյալների պաշտպանության օրենսդրության համապատասխանության գնահատման արդյունքներ,
4. Անձնական տվյալների մշակման անվտանգության միջոցների գնահատման արդյունքներ,
5. Անձնական տվյալների պաշտպանության օրենսդրական պահանջների մասին ՏԻՄ աշխատակիցների իրազեկման մակարդակի գնահատման արդյունքներ,
6. Փորձագիտական եզրակացություն և առաջարկություններ:

Ուսումնասիրման տվյալները հավաքվել են 2020թ. օգոստոս-սեպտեմբեր ժամանակահատվածում:

1. Ամփոփ եզրակացություն

Ամփոփ եզրակացության մեջ ներկայացվում են ՏԻՄ-երի կողմից անձնական տվյալների մշակման գործընթացում փորձագետների կողմից բացահայտած հիմնական խնդիրները և ընդհանուր գնահատականն ըստ նախանշված նպատակների:

1.1 ՏԻՄ-երի կողմից անձնական տվյալների մշակման համապատասխանությունը ՀՀ օրենսդրությանը և միջազգային լավագույն փորձին և չափանիշներին

Ուսումնասիրությունը ցույց տվեց, որ ՏԻՄ-երում գործարկվող երկու էլեկտրոնային համակարգերի և քաղաքացիների սպասարկման գրասենյակների կողմից ծառայությունների մատուցման ընթացքում անձնական տվյալների մշակման գործընթացն իրականացվում է **օրինականության սկզբունքին համապատասխան**: **ՏԻՄ-երի կողմից մարդկանց անձնական տվյալները մշակվում են օրինական եւ որոշակի նպատակներով:** ՏԻՄ-երը մշակում են բացառապես ոլորտային օրենքներով նախատեսված անձնական տվյալներ օրենքով իրենց տրված լիազորությունների շրջանակում:

- Միաժամանակ, պետք է արձանագրենք, որ անձնական տվյալների մշակում նախատեսող օրենսդրությունը բավարար չափով «որակյալ» չէ. նկատի ունենք, որ թեեւ ոլորտային օրենքները նախատեսում են ՏԻՄ-երի՝ այս կամ այն անձնական տվյալներ մշակելու լիազորությունները, սակայն լայն իմաստով օրենքներում օրենքների թարմացվածությունը (օգտագործվող տերմինաբանությունը, բառակազմը, հստակությունը), օրենքներում էլեկտրոնային գործիքների կիրառման առանձնահատկությունների (ներառյալ՝ անձնական տվյալների անվտանգության

ապահովման միջոցների) նկարագրությունը եւ փոխկապակցված այլ ոլորտների օրենսդրության (այդ թվում՝ արխիվացման) հետ ներդաշնակությունը բավարար մակարդակի չեն:

- Որոշ խնդիրներ են բացահայտվել անձնական տվյալների մշակման **համաչափության սկզբունքի համապատասխանության առումով**: Որոշ դեպքերում արձանագրվել է համաչափության սկզբունքի բաղադրիչի՝ սուբյեկտների նվազագույն ներգրավման պահանջի ոչ բավարար համապատասխանություն: Առկա չի եղել հստակ ներքին ընթացակարգային եւ վարչական տարանջատում, թե ՏԻՄ որ աշխատակիցը անձնական տվյալների ինչպիսի շրջանակի հետ գործ ունի:
- Ուսումնասիրված ՏԻՄ-երի կողմից բավարար չափով չի իրականացվում ԱՏՊ մշակման օրինական նպատակի համար ոչ պիտանի անձնական տվյալները բացահայտելու և սահմանված ժակետի ավարտից հետո վերացնելու կամ ջնջելու գործընթաց: Առկա չէ նաեւ հստակ գործընթաց օրինական նպատակին հասնելու համար ոչ անհրաժեշտ անձնական տվյալները բացահայտելու, վերացնելու, ոչնչացնելու կամ ուղեփակելու նպատակով: Առկա չէ նաեւ այս գործընթացների կարգավորում: Որոշ շեղումներ են բացահայտվել նաեւ **հավաստիության սկզբունքի** համապատասխանության առումով. առկա չէ տվյալների վերանայման, ստուգման որեւէ մեխանիզմ և մշակված ընթացակարգ:

1.2 ՏԻՄ-երի կողմից անձնական տվյալների մշակման անվտանգության կանոնների ապահովումը

Տեղական ինքնակառավարման մարմինների անձնական տվյալներ պարունակող համակարգերը սպասարկող կազմակերպության կողմից ներդրվել և կիրառվում են որոշակի միջոցներ: Այնուամենայնիվ, համակարգերի անվտանգության մակարդակը չի կարելի համարել լիարժեք բավարար: Անձնական տվյալների մշակման համակարգերի պաշտպանության բացահայտված հիմնական թերություններն են.

- Տեղեկատվական անվտանգության կանոնների բացակայությունը և աշխատակիցների համակարգչային անվտանգության հմտությունների սկզբնական մակարդակը: Բացակայում են տեղեկատվական անվտանգության մասնագետների հաստիքները կամ ՏԻՄ-ի հետ մշտապես համագործակցող համապատասխան փորձագետները, որոնց մասնակցությունը ընդհանուր տեղեկատվական, ցանցային և ծրագրային անվտանգության պատշաճ համակարգեր ստեղծելու համար չափազանց կարևոր է:

- Լիարժեք ապահովված չէ անձնական տվյալներ պարունակող ֆիզիկական կրիչների գաղտնագրումը՝ համաձայն «Անձնական տվյալների պաշտպանության» ՀՀ օրենքի 19-րդ հոդվածի 2-րդ մասի պահանջների: Հեռահար աշխատանքի և առցանց հարցումների անվտանգությունը ապահովելու նպատակով հարկավոր է կիրառել լրացուցիչ անվտանգութան գործիքներ, այդ թվում վիրտուալ մասնավոր ցանցեր և բազմակի նույնականացման միջոցներ:

- Մեծի մասամբ բացակայում են ծրագրային անվտանգության ապահովման համապատասխան միջոցառումները՝ հակավնասակար (antivirus, antimalware)

ծրագրերի կիրառումը, համակարգերի ու ծրագրերի կանոնավոր թարմացումը (system and software update) և անվտանգության բացերի վերածումը (vulnerabilities patching): Համատարած խնդիր է չարտոնագրված օպերացիոն համակարգերի եւ ծրագրերի օգտագործումը:

1.3 Անձնական տվյալների մշակման օրենսդրական պահանջների վերաբերյալ ՏԻՄ-երի աշխատակիցների իրազեկման մակարդակը

Ուսումնասիրությունից պարզ է դարձել, որ ընտրված ՏԻՄ-երից ոչ մեկի աշխատակիցները վերապատրաստման կամ ուսուցման չեն մասնակցել անձնական տվյալների պաշտպանության ոլորտում, որպեսզի կարողանան ճանաչել անձնական տվյալների անվտանգության խախտումները և պատշաճ իրականացնեն տվյալների մշակման գործընթացը:

Անձնակազմը տեղյակ չէ նաեւ, թե ինչպես է անհրաժեշտ վարվել մշակման նպատակի համար ոչ անհրաժեշտ տվյալների հետ, ինչպես դրանք բացահայտել և ջնջել կամ փոփոխել: Անձնակազմը տեղյակ չէ նաեւ, թե երբ, ում և ինչ ընթացակարգով է պետք հաղորդել ՏԻՄ-ում անձնական տվյալների անվտանգության խախտումների և արտահոսքերի մասին, ինչպես նաեւ կենսաչափական տվյալներ մշակելու գործընթացի մասին:

Անձնակազմի գիտելիքն ու հմտությունները հիմնված են բացառապես աշխատանքային փորձի վրա, որը տարբեր ՏԻՄ-երի, անգամ ստորաբաժանումների դեպքում, տարբեր է:

Անձնական տվյալների պաշտպանության առանձին մասնագիտական խնդիրները մանրամասն քննարկվում են սույն փաստաթղթի 4-րդ բաժնում, իսկ ըստ մեթոդաբանության չափանիշների գնահատման արդյունքները, բացահայտված բացերը և առաջարկությունները՝ հաշվետվության եզրափակիչ մասում:

2. Գնահատման նպատակը, ծավալը և մեթոդաբանությունը

Անձնական տվյալների մշակման գնահատման հիմնական նպատակն է որոշել, թե որքանով է տվյալների հավաքագրման, պահպանման և մշակման գործընթացը համապատասխանում իրավական և նորմատիվ օրենսդրական պահանջներին: Գնահատման նպատակն է նաեւ ստուգել տվյալների պաշտպանության օրենսդրության պահանջներին համապատասխանությունը, ինչպես նաև բացահայտել այն առանցքային հարցերը, որոնք ներկայումս սահմանված չեն ՀՀ օրենսդրությամբ, սակայն հայտնի են որպես լավագույն փորձ և կարևոր են անձնական տվյալների պաշտպանության պատշաճ մակարդակի ապահովման տեսանկյունից:

Տեղական ինքնակառավարման մարմինների կողմից անձնական տվյալների մշակման ծավալի և գործընթացների համապատասխանատվությունը ՀՀ օրենսդրությանը գնահատվել է «Անձնական տվյալները պաշտպանության մասին» ՀՀ օրենքով սահմանված պահանջներին ուղղակի համեմատելու միջոցով: Մեթոդաբանության այս բաժինը կազմված է երեք մասից.

- Անձնական տվյալների մշակման հիմքերի, նպատակի ծավալի օրինականությունը,
- Անձնական տվյալների մշակման ընթացքում սուբյեկտների՝ քաղաքացիների իրավունքների պաշտպանության ապահովումը,
- Անձնական տվյալներ մշակելու համար սահմանված կամ փաստացի գործող ընթացակարգերի համապատասխանությունը օրենսդրությանը:

Անձնական տվյալների մշակման գործընթացը ստուգվել է փորձետների կողմից մշակված 62 չափանիշների հիման վրա: Գնահատման չափանիշները մանրամասն ներկայացված են Հավելված 2-ում:

Անձնական տվյալների պաշտպանության գնահատման ծավալը ներառում է միայն այն համակարգերը և գործառույթները, որոնք առնչվում են անձնական տվյալներ մշակելուն, մասնավորապես 3 խոշորացված համայնքներում՝ Ջերմուկում, Դիլիջանում եւ Սիսիանում ներդրված Համայնքային կառավարման տեղեկատվական համակարգը, Քաղաքացիների սպասարկման գրասենյակների միջոցով մատուցվող ծառայությունները, ինչպես նաեւ Աբովյանի համայնքապետարանի կողմից մանկապարտեզների առցանց գրանցման համակարգը: ՏԻՄ-երի կողմից շահագործվող տեղեկատվական համակարգչային սարքերը և համակարգերը դիտարկվել ու գնահատվել են միայն այն ծավալով, որը այս կամ այն կերպ կարող է ազդել անձնական տվյալների պաշտպանվածության վրա:

Մեթոդաբանության այն մասը, որը վերաբերում է անձնական տվյալների պաշտպանվածությանը, մշակվել է՝ հիմք ընդունելով միջազգային ու Եվրոպական ստանդարտները (GDPR և ISO 27001) և համապատասխան աուդիտորական մեթոդները: Տեղեկատվական անվտանգության գնահատումն անցկացվել է ՏԻՄ-երում առկա կազմակերպչական (վարչական), ֆիզիկական և տեխնիկական միջոցների ստուգման միջոցով (security controls check):

Քանի որ գնահատման ծավալը չի ենթադրել տեղեկատվական անվտանգության խորացված աուդիտ և սահմանափակված էր միայն անձնական տվյալների պաշտպանության գնահատմամբ, մեթոդաբանությունը մշակելիս ընտրվել են ISO 27001-ի ստուգման այն միջոցները, որոնք վերաբերելի են անձնական տվյալների պաշտպանության գնահատմանը՝ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 19-րդ հոդվածի իմաստով:

ՏԻՄ-երի աշխատակազմի կողմից անձնական տվյալների օրենսդրական պահանջների մասին իրազեկ լինելու աստիճանը գնահատվել է ուղղակի հարցման միջոցով: Գնահատման մեթոդաբանության համապատասխան մասը նպատակ ուներ պարզել՝ որքանով են աշխատակիցները տեղեկացված անձնական տվյալների պաշտպանության օրենսդրության մասին, առկա է արդյոք պաշտոնական հրահանգում (համայնքային ծառայողի անձնագրում) համապատասխան պարտականություններ և գիտեն արդյոք՝ ինչպես արձագանքել անձնական տվյալներին հետ կապված միջադեպերին (արտահոսք, ապօրինի փոփոխում կամ ոչնչացում):

Գնահատումն իրականացնելու նպատակով իրականացվել են առցանց հարցազրույցներ ընտրված ՏԻՄ-երի գլխավոր քարտուղարների, սոցիալական աշխատակիցների, սիստեմ ադմինիստրատորների, համակարգչային սպասարկման պատասխանատուների հետ:

Առցանց հարցազրույցներն անց են կացվել Հավելված 2-ում ներառված հարցաշարի հիման վրա):

3. ՏԻՄ-երի կողմից անձնական տվյալների մշակման գործընթացի՝ օրենսդրությանը համապատասխանության գնահատման արդյունքներ

Անձնական տվյալների պաշտպանության իրավունքը սահմանադրական իրավունք է: ՀՀ Սահմանադրության 34-րդ հոդվածի 1-ին մասի համաձայն՝ «Յուրաքանչյուր ոք ունի իրեն վերաբերող տվյալների պաշտպանության իրավունք»: Նույն հոդվածի 2-րդ մասի համաձայն՝ «Անձնական տվյալների մշակումը պետք է կատարվի բարեխղճորեն, օրենքով սահմանված նպատակով, անձի համաձայնությամբ կամ առանց այդ համաձայնության՝ օրենքով սահմանված այլ իրավաչափ հիմքի առկայությամբ»:
Համաձայն ՀՀ Սահմանադրության 6-րդ հոդվածի՝ ՏԻՄ-ը իրավասու է կատարել միայն այնպիսի գործողություններ, որոնց համար լիազորված է Սահմանադրությամբ կամ օրենքներով: Այսպիսով, ՏԻՄ-երի կողմից անձնական տվյալների մշակումը հնարավոր է բացառապես օրենքով սահմանված նպատակով և նախատեսված դեպքերում: Անձնական տվյալների մշակումն ու մշակման պայմանները նույնպես նախատեսվում են օրենքով:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 3-րդ հոդվածի 1-ին մասի 1-ին կետի համաձայն՝ անձնական տվյալ է «(…) ֆիզիկական անձին վերաբերող ցանկացած տեղեկություն, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը»:

ՏԻՄ-երի կողմից անձնական տվյալների մշակումը՝ անձնական տվյալների հավաքումը, ամրագրումը, մուտքագրումը, համակարգումը, կազմակերպումը, պահպանումը, օգտագործումը, վերափոխումը, վերականգնումը, փոխանցումը, ուղղումը, ուղեփակումը, ոչնչացումը, կամ դրանց հետ այլ գործողությունները կարող են կատարվել բացառապես օրենքներով ուղղակիորեն սահմանված դեպքերում եւ կարգով: ՏԻՄ-երը անձնական տվյալների մշակման գործընթացն իրականացնում են հետեւյալ իրավական նորմերի հիման վրա.

- Անձնական տվյալների պաշտպանության մասին ՀՀ օրենք,
- «Տեղական ինքնակառավարման մասին» ՀՀ օրենքի 38-րդ հոդվածի 1-ին մասի 3-րդ կետ, 40-րդ, 46-րդ եւ 48-րդ հոդվածները, անուղղակիորեն 4-րդ հոդվածի 2-րդ մաս,
- «Գույքահարկի մասին» ՀՀ օրենքի 10-րդ, 14-րդ եւ 23-րդ հոդվածներ,
- «Հողի հարկի մասին» ՀՀ օրենքի 8-րդ, 14-րդ, 15-րդ եւ 17-րդ հոդվածներ,
- «Սոցիալական աջակցության մասին» ՀՀ օրենքի 2-րդ, 6-րդ 24-րդ, 31-րդ, 34-րդ, 36.2-րդ, 40-րդ եւ 42-րդ հոդվածներ,
- «Աղբահանության և սանիտարական մաքրման մասին» ՀՀ օրենքի 14-րդ եւ 19-րդ հոդվածներ,
- «Հանրակրթության մասին» ՀՀ օրենքի 16-րդ եւ 32-րդ հոդվածներ,
- «Նախադպրոցական կրթության մասին» ՀՀ օրենքի 15-րդ եւ 17-րդ հոդվածներ,
- Վարչարարության հիմունքների եւ վարչական վարույթի մասին ՀՀ օրենք,
- Համայնքային ծառայության մասին ՀՀ օրենքը:

ՏԻՄ-երի կողմից մշակվում են երկու խումբ քաղաքացիների անձնական տվյալներ՝ համայնքապետարանների աշխատակիցների անձնական տվյալները աշխատանքային հարաբերությունների շրջանակում եւ քաղաքացիների անձնական տվյալները՝ վերջիններիս ծառայություններ մատուցելու համատեքստում: ՏԻՄ-երի կողմից քաղաքացիների անձնական տվյալների մշակումն իրականացվում է երկու համակարգերի միջոցով՝ էլեկտրոնային՝ Համայնքային կառավարման տեղեկատվական համակարգի (այսուհետ՝ ՀԿՏՀ) և պաշտոնական կայքերում առկա էլեկտրոնային ծառայությունների շտեմարանի միջոցով՝ ներառյալ մանկապարտեզների առցանց հերթագրման համակարգը, ինչպես նաև ֆիզիկական՝ քաղաքացիների միասնական սպասարկման կենտրոնների կողմից:

ՏԻՄ-երը կիրառում են Տեղեկատվական համակարգերի զարգացման եւ վերապատարաստման կենտրոն (ՏՀԶՎԿ) ՀԿ-ի մշակած ու գործարկած էլեկտրոնային փաստաթղթաշրջանառության Համայնքային կառավարման տեղեկատվական համակարգը (այսուհետ՝ ՀԿՏՀ) ներքին փաստաթղթաշրջանառության ապահովման նպատակով: Համակարգը մշակվել և ներկայում նույնպես սպասարկվում է հասարակական կազմակերպության կողմից, վերջինիս մշակած գործիքակազմով:

Նախքան ԱՏՊ օրենսդրության առանձին սկզբունքներին և կարգավորումներին համապատասխանության հարցին անդրադառնալը դիտարկենք մի կարեւոր հանգամանք: ՏԻՄ-երի էլեկտրոնային համակարգերի մշակումը և գործարկումը պատվիրակված է մասնավոր սեկտորին, որն էլ իրականացնում է նաեւ սպասարկման ողջ գործընթացը: Պատվիրակված կազմակերպությունը հանդես է գալիս ԱՏՊ օրենքի իմաստով (հոդված 14-րդ) որպես տվյալներ մշակողի առաջադրանքով անձնական տվյալներ մշակող լիազորված անձ, ինչը նշանակում է, որ պետք է լինի տվյալների մշակման առաջադրանք: Տվյալ դեպքում լիազորված կազմակերպությունը (ՏՀԶՎԿ) իր առջեւ դրված խնդիրներն իրականացնում է ՏԻՄ-երի հետ կնքած պայմանագրի հիման վրա: Լիազորված անձի միջոցով տվյալների մշակման կանոնները պետք է պահպանվեն, իսկ առաջադրանքը պետք է խստորեն համապատասխանի ԱՏՊ օրենքի պահանջներին: Այսպիսով, գնահատման խնդիրն էր նաեւ պարզել, թե արդյոք պահպանվել են լիազորված անձի միջոցով տվյալներ մշակելու օրենքի պահանջները: Մեր գնահատմամբ՝ անհրաժեշտություն կա վերանայելու ՏԻՄ-երի եւ լիազորված կազմակերպության միջեւ կնքված պայմանագրերը՝ դրանք համապատասխանեցնելով ԱՏՊ օրենքի 14-րդ հոդվածով սահմանված կանոններին: Մասնավորապես, ՏԻՄ և ՏՀԶՎԿ միջեւ կնքված պայմանագրում պետք է հստակ արտացոլվեն հետեւյալ դրույթները.

- պետք է շարադրված լինեն անձնական տվյալներ մշակելու իրավական հիմքերը եւ պայմանները,
- անձնական տվյալներ մշակելու նպատակը,
- մշակման ենթակա անձնական տվյալների ցանկը,
- տվյալների սուբյեկտների շրջանակը,
- այն անձանց շրջանակը, որոնց կարող են փոխանցվել անձնական տվյալները,

- անձնական տվյալների պաշտպանության տեխնիկական եւ կազմակերպչական միջոցառումները եւ գործընթացի համար անհրաժեշտ այլ տեղեկություններ:

Ստորեւ ներկայացվում են ՏԻՄ-երի կողմից անձնական տվյալներ մշակելու պրակտիկայի համապատասխանությունը ԱՏՊ օրենքին գնահատման արդյունքները՝ համաձայն ԱՏՊ օրենսդրությամբ սահմանված սկզունքների:

3.1 Օրինականության սկզբունք

Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքի 4-րդ հոդվածի համաձայն՝

1. Անձնական տվյալներ մշակողը պարտավոր է հետեւել եւ ապահովել, որ տվյալները մշակվեն օրենքի պահանջների պահպանմամբ:

2. Անձնական տվյալները մշակվում են օրինական եւ որոշակի նպատակներով եւ առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով:

Ինչպես նաեւ, ԱՏՊ օրենքի 8-րդ հոդվածի համաձայն՝ տվյալների մշակումն օրինական է, եթե.

1) տվյալները մշակվում են օրենքի պահանջների պահպանմամբ,

2) Տվյալները մշակվում են օրինական և որոշակի նպատակներով և առանց տվյալների սուբյեկտի համաձայնության չեն կարող օգտագործվել այլ նպատակներով,

3) Տվյալների սուբյեկտը տվել է իր համաձայնությունը:

Ուսումնասիրությունը ցույց տվեց, որ ՏԻՄ-երի կողմից անձնական տվյալների մշակման գործընթացն էլեկտրոնային համակարգերի և ՔՍԳ-ի միջոցով իրականացվում է ընդհանուր առմամբ օրինականության սկզբունքին համապատասխան: ՏԻՄ-երի կողմից մարդկանց անձնական տվյալները մշակվում են օրինական եւ որոշակի նպատակներով: ՏԻՄ-երը մշակում են բացառապես ոլորտային օրենքներով նախատեսված անձնական տվյալներ, որոնք անհրաժեշտ են օրենքով իրենց տրված լիազորություններն իրականացնելու եւ քաղաքացիներին պատշաճ ծառայություններ մատուցելու նպատակով:

Օրինականության սկզբունքի համապատասխանության առումով արձանագրված միակ բացն այն է եղել, որ կարգավորված չէ անձի (աշխատակցի կամ քաղաքացու) համաձայնության ստացման հարցը: Եթե անհրաժեշտություն է առաջանում օրենքով սահմանված ՏԻՄ որեւէ լիազորություն իրականացնելու գործընթացում մշակել աշխատակիցների կամ քաղաքացների լրացուցիչ անձնական տվյալներ, քան նախատեսված է օրենքով, ուստի այս տվյալները պետք է մշակվեն բացառապես անձի համաձայնության հիման վրա: Նման անհրաժեշտություն կարող է առաջանալ, օրինակ, ՏԻՄ տարածքում տեսահսկման համակարգի տեղադրման կամ լրատվամիջոցից ՏԻՄ աշխատակիցների պարգեւավճարների վերաբերյալ ստացված հարցմանը պատասխանելու ժամանակ եւ այլն:

Համաձայնությունը պետք է համապատասխանի օրենքով սահմանված հետեւյալ չափանիշներին: «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 9-րդ հոդվածի 7-րդ մասի համաձայն՝ «Տվյալների սուբյեկտի համաձայնությունը տրվում է

գրավոր կամ էլեկտրոնային եղանակով՝ հաստատված էլեկտրոնային թվային ստորագրությամբ, բանավոր համաձայնության դեպքում՝ այնպիսի հավաստի գործողությունների միջոցով, որոնք ակնհայտորեն կվկայեն տվյալների սուբյեկտի՝ անձնական տվյալները օգտագործելու համաձայնության մասին»: Նույն հոդվածի 8-րդ մասի համաձայն՝ «Տվյալների սուբյեկտի համաձայնությունը ստանալու փաստն ապացուցելու (...) պարտականությունը կրում է մշակողը»:

Համաձայնություն է 1) «ցանկացած կամահայտնություն, որով տվյալների սուբյեկտը տալիս է իր հավանությունը» եւ այն պետք է լինի 2) «ազատ տրված», 3) «որոշակի» եւ 4) «տեղեկացված»: Ընդ որում, «ցանկացած կամահայտնություն, որով տվյալների սուբյեկտը տալիս է իր հավանությունը» չափանիշից բխում է, որ սկզբունքորեն չկան սահմանափակումներ, թե համաձայնությունն ինչ ձեւով պետք է վերցվի, սակայն այն պետք է լինի կամահայտնություն: Համաձայնությունը կարող է տրվել գրավոր՝ հաստատված ստորագրությամբ, բանավոր, գործողության միջոցով, որն ակնհայտ վկայում է համաձայնության մասին: Թեեւ համաձայնությունը կարող է տրվել ցանկացած ձեւով, սակայն այն պետք է հստակ արտացոլի տվյալների սուբյեկտի կամքը իր անձնական տվյալների մշակման վերաբերյալ: Այսինքն, համաձայնությունը պետք է լինի «միանշանակ»: Սա նշանակում է, որ չպետք է որեւէ կասկած մնա, որ տվյալների սուբյեկտի համաձայնությունն ուղղված է հենց անձնական տվյալների մշակմանը: Այլ կերպ ասած՝ տվյալների սուբյեկտի կամահայտնությունը, որով նա տալիս է իր հավանությունն անձնական տվյալների մշակման վերաբերյալ, պետք է միանշանակորեն վկայի տվյալների սուբյեկտի մտադրության վերաբերյալ, իսկ եթե կա տվյալների սուբյեկտի մտադրության վերաբերյալ ողջամիտ կասկած, ապա համաձայնությունը չի կարող համարվել միանշանակորեն տրված:

Համաձայնության՝ «ազատ տրված» լինելու չափանիշը նշանակում է, որ համաձայնությունը կարող է վավեր համարվել, եթե տվյալների սուբյեկտը համաձայնությունը տվել է իր իրական ընտրությամբ (ազատ, կամավոր որոշմամբ), առանց խաբեության, սպառնալիքի, հարկադրանքի կամ համաձայնություն չտալու դեպքում իր համար բացասական հետեւանքի: Եթե համաձայնություն տալ կամ չտալու հետեւանքները խաթարում են անձի ազատ ընտրությունը (freedom of choice), ապա համաձայնությունը չի համարվի ազատ տրված: Համաձայնության՝ «որոշակի» լինելու չափանիշը նշանակում է, որ համաձայնությունը կարող է վավեր համարվել, եթե այն կոնկրետ է: Այլ կերպ ասած, ընդհանուր համաձայնությունը, առանց անձնական տվյալի ճշգրիտ նպատակը մանրամասնելու, ընդունելի չէ: Համաձայնությունը պետք է լինի հասկանալի, այսինքն, այն պետք է վերաբերի անձնական տվյալների մշակման հստակ եւ ճշգրիտ շրջանակի:

Վերջապես, համաձայնության՝ «տեղեկացված» լինելու չափանիշից բխում է, որ անձնական տվյալների սուբյեկտի համաձայնությունը պետք է հիմնված լինի անձնական տվյալների մշակման հանգամանքները եւ հետեւանքները գիտակցելու եւ հասկանալու, անձնական տվյալների մշակման (մշակվող տվյալների, մշակման նպատակի, այլն անձանց հնարավոր փոխանցման, տվյալների սուբյեկտի իրավունքների եւ այլնի) վերաբերյալ ճշգրիտ եւ լիարժեք տեղեկությունների վրա: Ընդ որում, տեղեկությունները պետք է հասանելի, հասկանալի եւ տեսանելի լինեն տվյալների սուբյեկտի համար, այլ ոչ թե «հասանելի ինչ-որ տեղ»:

Այսպիսով, ուսումնասիրված բոլոր ՏԻՄ-երում էլկետրոնային համակարգերի միջոցով անձնական տվյալները մշակվում են օրինականության սկզբունքին համապատասխան: Այստեղ արձանագրված միակ կարիքն այն է, որ բոլոր այն դեպքերում, երբ քաղաքացիների անձնական տվյալները մշակվում են անձի համաձայնության հիման վրա, դրանք պետք է լինեն բացառություններ եւ ուղղակի նախատեսված օրենքով: Միաժամանակ, անձի համաձայնությունը պետք է ստացվի վերոնշյալ կանոների պահպանմամբ:

3.2 Համաչափության սկզբունք

Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքի 5-րդ հոդվածը սահմանում է համաչափության սկզունքը.

1. Տվյալների մշակումը պետք է հետապնդի օրինական նպատակ, դրան հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ եւ չափավոր:

2. Անձնական տվյալներ մշակողը պարտավոր է անձնական տվյալները մշակել այն նվազագույն քանակով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար:

3. Արգելվում է այնպիսի անձնական տվյալների մշակումը, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար կամ անհամատեղելի են դրա հետ:

4. Արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով:

5. Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:

Գնահատմամբ որոշ խնդիրներ են ի հայտ եկել անձնական տվյալների մշակման **համաչափության սկզբունքի բաղադրիչներից մեկի՝ սուբյեկտների նվազագույն ներգրավման առումով:** Ուսումնասիրված ՏԻՄ-երում առկա չէ ներքին ընթացակարգային եւ վարչական տարանջատում, թե ՏԻՄ որ աշխատակիցը անձնական տվյալների ինչպիսի շրջանակի հետ գործ ունի: Գործընթացում ներգրավված աշխատակիցների ցանկը հստակ չէ, թե ովքեր ունեն հասանելիություն մշակված տվյալներին, ովքեր ունեն անմիջական մասնակցություն տվյալների հավաքագրման և/կամ համակարգ մուտքագրման, տվյալների և տվյալների բազաների համակարգման, վիճակագրական և անձնական տվյալներ պարունակող տվյալների բազաների օգտագործմամբ այլ հաշվետվությունների մշակման գործընթացներում:

Համաչափության սկզբունքի մյուս բաղադրիչն այն է, որ **անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար:** Ուսումնասիրությունը ցույց է տվել, որ ՏԻՄ-երի կողմից չի իրականացվում ոչ պիտանի անձնական տվյալները սահմանված ժակետի ավարտից հետո բացահայտելու,վերացնելու կամ ջնջելու գործընթաց՝ հանգեցնելով համաչափության սկզբունքի 5-րդ բաղադրիչի խախտման:

Չկան ընդունված կանոնակարգեր և ընթացակարգեր ուղղված նշվյալ գործընթացի իրականացմանը: Օրինակ, ՏԻՄ աշխատակցի հետ աշխատանքային պայմանագիրը լուծելուց հետո գործատուն պարտավոր է ոչնչացնել կամ ապանձնավորել աշխատողի բոլոր այն անձնական տվյալները, որոնց մշակման նպատակները սպառվել են, բացառությամբ այն տվյալների որոնց պահպանման ժամկետները նախատեսված են օրենքով: Սա մի կողմից կարող է պայմանավորված լինել ՏԻՄ-ի լիազորությունների շրջանակում անձնական տվյալների մշակում նախատեսող օրենսդրության եւ արխիվային ոլորտը կարգավորող օրենսդրության ներդաշնակության բացակայության հետ: Մյուս կողմից, ակնհայտորեն, առկա է օրենսդրության թարմացվածության խնդիր այն առումով, որ սահմանված չեն էլեկտրոնային եղանակով մշակվող անձնական տվյալների արխիվացման եւ պահպանման կանոնները:

«Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 13-րդ հոդվածով սահմանվում են կենսաչափական անձնական տվյալներ մշակելու առանձնահատկությունները՝ կենսաչափական անձնական տվյալներ մշակվում են միայն տվյալների սուբյեկտի համաձայնությամբ, բացառությամբ օրենքով նախատեսված դեպքերի, եւ եթե օրենքով հետապնդվող նպատակը հնարավոր է իրականացնել միայն այդ կենսաչափական տվյալները մշակելու միջոցով:

Թեեւ ԱՏՊ օրենքը սահմանում է որոշակի խումբ անձնական տվյալների (ներառյալ հատուկ կատեգորիայի [4] եւ կենսաչափական անձնական տվյալներ [5]) մշակման որոշակի առանձնահատկություններ, սակայն ուսումնասիրված ՏԻՄ-երում առկա չէ տարբերակված մոտեցում և մշակվող անձնական տվյալները չունեն առանձնացված կարգավիճակներ: Միաժամանակ, տարբեր կատեգորիայի անձնական տվյալների մշակման և պահպանման գործընթացում առկա չեն պաշտպանության տարբեր մակարդակներ եւ հաշվի չեն առնված մշակման առանձնահատկությունները, չեն կիրառվում լրացուցիչ երաշխիքներ:

Ինչպես նաեւ պարզ դարձավ, որ ՏԻՄ-երը ԱՏՊ օրենքով սահմանված կարգով երբեւէ ծանուցում չեն ներկայացրել ՀՀ ԱՆ ԱՏՊ գործակալություն կենսաչափական տվյալներ մշակելու վերաբերյալ: Գործակալությունը նաեւ չի տեղեկացվել տվյալների արտահոսքերի մասին, թեեւ ՏԻՄ-երից մեկում բավական ծավալուն արտահոսք է գրանցվել:

3.3 Թափանցիկության սկզբունք

Թափանցիկության սկզբունքից է բխում այն, որ անձն ունի անձնական տվյալների մշակման վերաբերյալ տեղեկատվություն ստանալու իրավունք: Անձն իրավունք ունի իր մասին անսահմանափակ տեղեկություն ստանալ անձնական տվյալներ մշակողից.

---

[4] Հատուկ կատեգորիայի անձնական տվյալներ՝ անձի ռասայական, ազգային պատկանելությանը կամ էթնիկ ծագմանը, քաղաքական հայացքներին, կրոնական կամ փիլիսոփայական համոզմունքներին, արհեստակցական միությանն անդամակցությանը, առողջական վիճակին ու սեռական կյանքին վերաբերող տեղեկություններ:

[5] Կենսաչափական տվյալ - կենսաչափական անձնական տվյալներ՝ անձի ֆիզիկական, ֆիզիոլոգիական եւ կենսաբանական առանձնահատկությունները բնութագրող տեղեկություններ:

- Նա իրավունք ունի ստանալ մշակվող անձնական տվյալների պատճենները (ինչպես ֆիզիկական այնպես էլելեկտրոնային եղանակով),

-ստանալու տեղեկություններ իր անձնական տվյալները մշակելու հիմքերի և նպատակների,

-տվյալները մշակողի, նրա գտնվելու վայրի մասին,

-ինչպես նաև այն անձանց շրջանակի մասին, որոնց կարող են փոխանցվել անձնական տվյալները,

- անձնական տվյալների մշակման մասին անձին հարցման հիման վրա տվյալները պետք է տրամադրվեն 5-օրյա ժամկետում:

Միաժամանակ, անձն ունի իր մասին սխալ, ոչ ճշգրիտ տեղեկության ճշգրտման իրավունք:

Այս սկզբունքի ապահովման առումով կարող ենք արձանագրել, որ առկա է քաղաքացիների իրազեկման ցածր մակարդակ: Նրանք տեղյակ չեն ԱՏՊ օրենքով սահմանված հնարավորության եւ ընթացակարգերի մասին: Բոլոր ՏԻՄ-երի գլխավոր քարտուղարները նշել են, որ քաղաքացիներն իրենց չեն դիմել այս բովանդակությամբ հարցմամբ, միաժամանակ քաղաքացիների տեղեկություն ստանալու հարցումներին ընթացք է տրվում սահմանված կարգով՝ 5-օրյա ժամկետում:

Այսպիսով, թեեւ անձնական տվյալների մշակման մասին **սուբյեկտի տեղյակ լինելու իրավունքի** իրացումն իրականացվում է Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքով սահմանված 5-օրյա ժամկետում, սակայն, առկա է քաղաքացիներին (տվյալների սուբյեկտներին) իրենց տեղեկություն ստանալու իրավունքի մասին հանրային իրազեկում իրականացնելու անհրաժեշտություն:

Սուբյեկտի տեղյակ լինելու իրավունքից բխում նաեւ այն, որ որ համայնքների պաշտոնական կայքերը օգտատերերին չեն ծանուցում «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 10-րդ հոդվածի 2-րդ մասի բոլոր 8 կետերով սահմանված տեղեկությունների վերաբերյալ: Այստեղ տեղադրված չեն նաեւ անձնական տվյալների մշակման եւ անվտանգության քաղաքականությունները, որոնք պետք է սահմանեն ՏԻՄ-ի կողմից անձնական տվյալների մշակման իրավական հիմքերը, նպատակները, ինչպես նաեւ անձնական տվյալների հետ կատարման ենթակա գործողությունների ցանկը, այն անձանց շրջանակը, որոնց կարող են փոխանցվել քաղաքացիների անձնական տվյալները:

Այսպիսով, տվյալների մշակման թափանցիկության սկզբունքի ապահովումը բավարար մակարդակով չի իրականացվում: Անհրաժեշտություն կա մշակելու եւ հանրայնացնելու անձնական տվյալների մշակման եւ անվտանգության քաղաքականությունները (privacy policy), որոնք պետք է սահմանեն ՏԻՄ-ի կողմից անձնական տվյալների մշակման իրավական հիմքերը, նպատակները, ինչպես նաեւ անձնական տվյալների հետ կատարման ենթակա գործողությունների ցանկը, մշակվող տվյալների սպառիչ ցանկը եւ այլն):

3.4 Հավաստիության սկզբունք

Այս սկզբունքից է բխում այն, որ մշակվող անձնական տվյալները պետք է լինեն ամբողջական, լիարժեք եւ հնարավորինս թարմացված: Թեեւ չի արձանագրվել ոչ ճշգրիտ կամ թերի տվյալի առկայություն համակարգում, սակայն պետք է արձանագրել, որ ՏԻՄ-երում առկա չեն ընթացակարգային լուծումներ ուղղված այս հարցի կարգավորմանը: ԱՏՊ օրենքը սահմանում է, որ տվյալներ մշակողը պարտավոր է ոչ ամբողջական, ոչ ճշգրիտ, հնացած, անօրինական ճանապարհով ձեռք բերված կամ մշակելու նպատակներին հասնելու համար ոչ անհրաժեշտ անձնական տվյալների դեպքում դրանք ամբողջացնել, թարմացնել, ուղղել կամ ոչնչացնել:

Ուսումնասիրությունը ցույց է տվել, որ առկա են բացթողումներ հավաստիության սկզբունքի համապատասխանության առումով. առկա չէ տվյալների վերանայման, ստուգման որեւէ մեխանիզմ և մշակված ընթացակարգ: ՏԻՄ-երը բավարար ռեսուրսներ ու ջանքեր չեն ներդնում բացահայտելու հնացած կամ թերի տվյալները և օրենքով սամանված ժամկետներում դրանք ամբողջացնելու, թարմացնելու, ուղղելու կամ ոչնչացնելու նպատակով:

Որեւէ գործընթաց կամ ընթացակարգ առկա չէ ուղղված այն տվյալների վերացմանը, ոչնչացմանը կամ ուղեփակմանը, որոնք անհրաժեշտ չեն օրինական նպատակին հասնելու համար:

Այսպիսով, թեեւ անձնական տվյալների մշակման գործընթացը հիմնականում իրականացվում է օրինականության սկզբունքին համապատասխան, սակայն անհրաժեշտ է բարեփոխումներ իրականացնել համաչափության, հավաստիության, թափանցիկության սկզբունքների ապահովման, տվյալների սուբկյետի համաձայնության պատշաճ ստացման, տարբեր կատեգորիաների տվյալների պաշտպանության ապահովման ուղղությամբ, ինչպես նաեւ անհրաժեշտ է մշակել եւ ընդունել վերոնշյալ հարցերը կարգավորող ներքին ընթացակարգեր և քաղաքականություններ: Որոշ կարգավորումներ պետք է սահմանվեն նաեւ ՏԻՄ աշխատակիցների պաշտոնների անձնագրերում:

4. Անձնական տվյալների պաշտպանության անվտանգության միջոցների վերլուծություն

Ցանկացած տեղեկատվական համակարգի անվտանգության գնահատում պետք է իրականացվի վարչական, ֆիզիկական և տեխնիկական ապահովման միջոցների (administrative, physical and technical security controls) առկայության ու դրանց արդյունավետության տեսակետից: Այս դասական մոտեցումը կիրառելի է ցանկացած համակարգերի անվտանգությունը գնահատելու համար՝ անկախ համակարգի չափերից, նրանում պահպանվող տեղեկատվության ծավալներից ու բնույթից:

Կազմակերպչական/վարչական միջոցները ներառում են տեղեկատվական անվտանգության քաղաքականության և համապատասխան կանոնների առկայությունը, ինչպես նաև աշխատակազմի կողմից այդ քաղաքականության ու կանոնների իմացությունը ու կիրառումը: Տեղեկատվական անվտանգության ֆիզիկական միջոցները ներառում են համակարգչային տեխնիկայի ամինջական հասանելիության սահմանափակումներ, ինչպես նաև աշխատանքային տարածքներ վերահսկողությունը:

Ու վերջապես, տեխնիկական անվտանգության միջոցները ներառում են տարբեր ծրագրային միջոցներ ու սարքավորումներ: Անվտանգության տեխնիկական միջոցները սահմանում են տվյալների բազաներ մուտք գործելու կանոնները, տվյալների հասանելիության սահմանափակումները, ինչպես նաև վնասակար ծրագրերի բացահայտումն ու դրանց վերացումը:

4.1 Անվտանգության քաղաքականություն և կանոններ

Նախքան տեղական ինքնակառավարման մարմինների կողմից մշակվող անձնական տվյալների պաշտպանվածության գնահատմանն անցնելը ուսումնասիրվել է կազմակերպչական և տեղեկատվական համակարգի կառուցվածքը և տեղեկատվական հոսքերի քարտեզը (կցված է որպես հավելված 3): Ուսումնասիրության արդյունքում պարզվել են անձնական տվյալների պահպանությանն առնչվող համակարգերի կառավարման սկզբունքները, պաշտպանության միջոցները և աշխատակիցների պատասխանատվությունը:

Նախքան տեղական ինքնակառավարման մարմինների կողմից մշակվող անձնական տվյալների պաշտպանվածության գնահատման անցնելը ուսումնասիրվել է կազմակերպչական և տեղեկատվական համակարգի կառուցվածքները (կցված է որպես Հավելված 3): Ուսումնասիրության արդյունքում պարզվել էին անձնական տվյալների պահպանությանն առնչվող համակարգերի կառավարման սկզբունքները, պաշտպանության միջոցները և աշխատակիցների պատասխանատվությունը:

Ընտրված բոլոր ՏԻՄ-երում իրականացված ուսումնասիրության արդյունքում պարզվել է, որ տեղեկատվական անվտանգության որևէ քաղականություն, կանոն կամ ընթացակարգ բավակայում է: Չնայած տեղեկատվական համակարգերի կառավարման համար պատասխանատու աշխատակազմն ունի բավարար գիտելիք ու որակավորում այդ համակարգերի պատշաճ շահագործումն ապահովելու համար, անվտանգության կանոնների և փորձի մասին իրազեկումը բավարար համարել չի կարելի:

Ինչպես արդեն նշվել է սույն փաստաթղթի այլ բաժիններում, անձնական տվյալների մշակման համակարգերը սպասարկվում են լիազորված կազմակերպության կողմից՝ «Տեղեկատվական համակարգերի զարգացման և վերապատրաստման կենտրոն» հասարակական կազմակերպության (ՏՀԶՎԿ), որը եղել է համայնքների տեղեկատվական կայքերի ստեղծման և էլեկտորանային կառավարման ծառայություններ մատուցելու նախաձեռնողն ու իրականացնողը:

Պետք է նշել, որ ՏՀԶՎԿ-ի կողմից կատարվել է բավական ծավալուն և բարդ աշխատանք, որը դժվար է թերագնահատել: Կարելի է իհարկե քննարկել ՏՀԶՎԿ-ի կողմից նախագծված ու իրագործված լուծումները, սակայն դա մոտեցումների հարց է, ինչպես նաեւ դուրս է սույն գնահատման շրջանակներից:

ՏՀԶՎԿ-ի կողմից համակարգերի սպասարկումն իրականացվում է ՏԻՄ-երի հետ կնքված պայմանագրի հիման վրա, որը նաև նախատեսում է անվտանգության որոշակի կանոններ: Դրանք վերաբերում եմ ՏՀԶՎԿ-ի ու ՏԻՄ-երի համակարգերի սպասարկման պատասխանատու աշխատակիցների (SS մասնագետ, համակարգը տնօրինող) միջև տեղեկատվական համակարգի անվտանգ սպասարկման գործընթաց: Ընդհանուր առմամբ, կանոնները համապատասխանում եմ ISO-27001 անվտանգության սկզբունքներին, այդ թվում սպասարկող կազմակերպության կողմից համակարգ մուտք գործելու իրավասությունների վերահսկման պարագայում:

Մի թերություն, որն անհրաժեշտ է նշել ՏԻՄ-սպասարկող կազմակերպություն համագործակցության ձեւաչափում. դա սպասարկող կազմակերպության կողմից մուտք գործելու ու աշխատանքներ կատարելու ընթացքում մշտադիտարկման և համագործակցության արձանագրության բացակայությունն է (interaction protocol and monitoring): Նշված բացը կարելի է լրացնել՝ SS մասնագետի (համակարգի տնօրինողի) կողմից սպասարկող անձի մուտք գործելուց հետո մշտադիտարկում իրականացնելու պարտավորություն սահմանելը և համագործակցությունն արձանագրելը:

Հեռահար ու շարժական աշխատանքի կանոններ

Բոլոր համայնքներում, որտեղ անցկացվել էր անձնական տվյալները պաշտպանվածության գնահատումը, առկա է հեռահար աշխատանք կատարելու հնարավորություն: Համայնքների գլխավոր քարտուղարներից ստացված տեղեկությունների համաձայն՝ հեռահար աշխատանքի կազմակերպման անհրաժեշտությունը ծագել է նոր տեսակի կորոնավիրուսի COVID-19 համավարակի պայմաններում աշխատանքներն առավել անվտանգ կազմակերպելու անհրաժեշտությունից: Հեռահար աշխատանքների կազմակերպման անհրաժեշտությունը ծագում է նաև ժամանակ առ ժամանակ հեռավոր բնակավայրերում գտնվող աշխատակիցների համար դեպի համակարգ մուտքը կազմակերպելու նպատակով:

Ստանալով աշխարհում ավելի ու ավելի լայն տարածում՝ հեռահար աշխատանքը միշտ եղել է համակարգչային հարձակման լայնորեն տարածված ուղղություններից մեկը (cyber attack vector). Ավելին, գնահատման պահին երեք համայնքներից երկուսի կայքերը շահագործվում են անպաշտպան արձանագրության կիրառմամբ (non-secure protocol), ինչն առանձին քննարկվում է այս փաստաթղթի հաջորդ բաժիններում: Հեռահար աշխատանքի կանոններ ընդունելն անհրաժեշտ է իրականացնել անվտանգության քաղաքականության և/կամ կանոններ ընդունելուն զուգահեռ կամ նույնիսկ մինչ այդ:

ՏԻՄ ցանցային անվտանգության պատասխանատու աշխատակիցները հեռահար աշխատանքների անվտանգության կազմակերպման համար կիրառում են որոշակի միջոցներ, ինչպիսիք են միայն որոշակի IP հասցեներից մուտք ապահովելը, աշխատանքի մշտադիտարկումը: Այնուամենայնիվ, թվարկված միջոցները չի կարելի համարել բավարար: Հառահար աշխատանք կազմակերպելու համար առնվազն պետք է կիրառվի մասնավոր վիրտուալ ցանցեր (VPN) և բազմակի նույնականացման միջոցներ (multi factor authentication):

Հասանելիության և գաղտնաբառերի կանոնները և կառավարումը (access and password management).

Անվտանգության քաղաքականության և կանոնների հետ կապված անհրաժեշտ է նաև նշել, որ մուտք գործելու և գաղտնաբառի կառավարման կանոնները (access and password managment rules) կիրառվում են MS Windows Server խմբերի օգտագործմամբ, ինչը լայնորեն ընդունված պրակտիկա է: Սակայն, պետք է նշել, որ մուտք գործելու իրավունքն առանձին կանոններով սահմանված չէ: Ըստ համայնքապետարանի SS մասնագետների՝ իրավունքները որոշում են իրենք՝ համայնքային ծառայողի անձնագրին համապատասխան:

Սակայն, իրավունքների հետ կապված ստույգ չափանիշներ և մուտք գործելու իրավունք շնորհելու գործընթացը սահմանված չէ: Ուսումնասիրված բոլոր ՏԻՄ-երում բացակայում էին գաղտնաբառի կանոններ՝ թե պարբերությամբ փոփոխելու, թե բարդության պահանջներ կիրառելու: Սիսիանի համայքապետարանը միակն էր, որտեղ գաղտնաբառի բարդության, երկարության ու պարբերականության սկզբունքները կիրառվում են, սակայն կրկին՝ կանոնները բացակայում են:

Ֆիզիկական անվտանգությունը և պահուստային արխիվացումը (backup)

Անձնական տվյալներ պարունակող սարքավորման (սերվերի) ֆիզիկական անվտանգության և պահուստային արխիվացման կանոնները սահմանվել են սպասարկող կազմակերպության (ՏՎԶՎԿ) կողմից և համապատասխանում են անվտանգության ստանդարտներին: Համակարգը տեղադրված է փակ տարածքում իսկ պահուստային արխիվացումը իրականացվում է կանոնավոր՝ շաբաթը մեկ անգամ: Արխիվացման գործընթացն ավտոմատիզացված չէ, կատարվում է ՏԻՄ-երի SS մասնագետների կողմից: Նման մոտեցումը կարելի էր համարել ընդունելի համապատասխան կանոնների առկայության դեպքում, սակայն կանոնները բացակայում են:

Բոլոր ՏԻՄ-երում բացակայում են տեղեկատվական վթարներին արձագանքելու ընթացակարգերը (incident management protocols)՝ այդ թվում կիբեր գրոհներին արձագանքելու ուղեցույցը (cyber attacks response guide). Հաշվի առնելով, որ աշխարհում կտրուկ աճել է պետական կառույցներից սովորաբար ավելի թույլ պաշտպանված ՏԻՄ-երի դեմ ուղղված կիբեր հարձակումների ծավալը, այս խնդիրը պահանջում է շուտափույթ լուծում:

4.2 Տվյալների պաշտպանության միջոցներ, ներառյալ ցանցային անվտանգություն

Տվյալների բազայի գաղտնագրումը

Անձնական տվյալների պաշտպանության համար տեխնիկական միջոցների կիրառման պահանջը ամրագրված է ոչ միայն մի շարք միջազգային սանդարտներով (ISO/IEC-27001, ISO/IEC-27701 NIST Cyber Security Framework, NIST Privacy Framework), այլ նաև «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի 19-րդ հոդվածով:

Օրենքի 19-րդ հոդվածի 2-րդ մասը սահմանում է, որ «անձնական տվյալները մշակելու ընթացքում մշակողը պարտավոր է օգտագործել գաղտնագրման միջոցներ՝ անձնական տվյալներ պարունակող տեղեկատվական համակարգերի պաշտպանվածությունը պատահական կորստից, տեղեկատվական համակարգեր անօրինական մուտք գործելուց, անձնական տվյալների անօրինական օգտագործումից, ձայնագրումից, ոչնչացումից, վերափոխումից, ուղեփակումից, կրկնօրինակումից, տարածումից և այլ միջամտությունից ապահովելու համար»:

Կարելի է վստահաբար փաստել, որ տեխնիկական միջոցների օգտագործմամբ անձնական տվյալների պաշտպանվածության գնահատման արդյունքում բացահայտված ամենալուրջ բացը անձնական տվյալներ պարունակող էլեկտրոնային կրիչների և համակարգերի գաղտնագրման բացակայություն է:

Անձնական տվյալների բազաների՝ այդ թվում շարժական կրիչների (removableand handled media) գաղտնագրումը խիստ անհրաժեշտ միջոց է, որը պարտադիր պետք է կիրառվի անձնական տվյալներ պարունակող և մշակող բոլոր համակարգերում: Սակայն, այդ խնդիրը սովորաբար լուծվում է համակարգի նախագծման փուլում: Միշտ չէ, որ այն հնարավոր է շտկել արդեն իսկ ստեղծված ու շահագործվող համակարգերում:

Քանի որ համակարգի նախագծման (system architecture) հարցը գնահատման ծավալից դուրս է և պահանջում է առանձին ծավալուն աշխատանք, անցկացրած գնահատման արդյունքում կարելի է առաջարկել համակարգի վերանախագծման կամ փոփոխման դեպքում անդրադառնալ անձնական տվյալների բազաների գաղտնագրման հարցին: Այս պահին առաջնային քայլերը պետք է ուղղված լինեն ցանցային անվտանգությունը հզորեցնելու ուղղությամբ:

Ցանցային անվտանգությունը

ԱՆձնական տվյալների համակարգը սպասարկող կազմակերպությունը (ՏՀՉՎԿ) և ՏԻՄ-ի ՏՏ մասնագետները ձեռնարկել են որոշ միջոցներ համակարգ կողմնակի ներթափանցման վտանգները նվազեցնելու և ներքին ցանցը պաշտպանելու համար: Ցանցի պարագծային պաշտպանությունն իրականացվում է մեկուսացման սարքով (firewall), իսկ մուտքը դեպի սերվեր սահմանափակված է ներքին IP հասցեներով:

Հաշվի առնելով, որ ներկա ժամանակ (չի բացառվում, որ նաև ապագայում) ՏԻՄ-երում թույլատրված է հեռահար աշխատանքը՝ առանց վիրտուալ մասնավոր ցանցերի (ՎՄՑ - virtual private network - VPN) օգտագործման (բացառություն է Ջերմուկի համայնքը), չի կարելի բացառել նաև միջնորդային գրոհները (man in the middle attack): ՎՄՑ կիրառումը հեռահար աշխատանքներ կատարելիս պետք է լինի պարտադիր և ամրագրվի հեռահար

աշխատանքի կանոններում, որը ցանկալի է մշակել և ընդունել հնարավորինս կարճ ժամկետներում:

Առանձին պետք է անդրադառնալ էլեկտրոնային կրիչների վրա ու անձնական համակարգիչներում պահպանվող անձնական տվյալների բազաներին: Ինչպես պարզվել է ՏԻՄ աշխատակիցների հետ հարցազրույցների ընթացքում, գնահատման պահին քաղաքացիների ռեգիստրի թարմացումը կատարվում էր կամ էլեկտրոնային փոստի (Դիլիջան) կամ ֆիզիկապես՝ արտաքին հիշողության միջոցով (USB solid state drive). Ռեգիստրի տվյալները հաղորդվում են առանց գաղտնագրության, ինչը հակասում է թե ISO/IEC 270001 սկզբունքներին:

Առավել մտահոգիչ է սոցիալական աշխատողների կողմից անձնական տվյալներ պարունակող բազաների օգտագործումը: Համաձայն սոցիալական աշխատողների կողմից տրամադրված տեղեկության՝ տվյալները պաշտպանված են գաղտնաբառով և օգտագործվում են բացառապես իրենց ու իրենց տարածքային ղեկավարների կողմից: Անկախ սոցիալական աշխատողների կողմից օգտագործվող իրավական հիմքերից, որոնք քննարկվում են փաստաթղթի այլ բաժիններում, զուտ տեղեկատվական անվտանգության տեսանկյունից տվյալների տնօրինումը անհրաժեշտ է կանոնակարգել թե պաշտպանության միջոցները կիրառելու, թե անվտանգության կանոնները պահպանելու առումով:

Էլեկտրոնային կրիչների վրա պահպանվող՝ ՏԻՄ-երի և ՏՀԶՎԿ-ի տնօրինվող համակարգից դուրս պահպանվող անձնական տվյալների պահպանման թերությունները կարելի է և անհրաժեշտ է արագորեն շտկել՝ էլեկտրոնային կրիչների վրա փոխանցվող տվյալները պարտադիր գաղտնագրելով արդի որակյալ միջոցներով: Հետագայում անվտանգության կանոնները մշակելիս անհրաժեշտ է նախատեսել շարժական կրիչների (removable and handled media) օգտագործման կանոններ, այդ թվում՝ դրանց գաղտնագրման և օգտագործման պահանջները:

Ցանցի մշտադիտարկում

Ցանկացած արժեքավոր տվյալ պարունակող տեղեկատվական համակարգում անհրաժեշտ է իրականացնել անդադար մշտադիտարկում՝ հնարավոր կասկածելի գործողությունները կամ գործընթացները (suspicious activities and actions) ժամանակին հայտնաբերելու և անհրաժեշտության դեպքում կանխելու նպատակով: Ուսումնասիրված ՏԻՄ-երի անձնական տվյալների համակարգերում գործարկված է մուտքերի գրանցման (access logs) համակարգ, որը հնարավորություն է տալիս պարբերաբար ստուգել աշխատակիցների գործունեությունը համակարգում:

Այնուամենայնիվ, մուտքերի գրանցումը ավտոմատիզացված չէ, ինչպես նաև ցանցային հոսքերի մշտադիտարկումը: Ժամանակակից ներթափանցման բացահայտման (intrusion detection) և ներթափանցման կանխարգելման (intrusion prevention) համակարգերը ոչ միայն բավականին թանկ են, այլ նաև բարդ շահագործման տեսակետից: Սակայն, հետագայում ցանկալի է դիտարկել առնվազն կասկածելի զանգվածային հոսքերը կանխող համակարգեր և գրոհներ շեղող ծրագրեր (honey pots):

4.3 Համացանցային ինտերֆեյսի անվտանգությունը

Համացանցային կայքի անվտանգության համար մեթոդաբանությամբ հատուկ չափանիշներ չեն նախատեսված և կայքի անվանգությունը գնահատվել է ծրագրային ապահովման, ցանցային անվտանգության, ինչպես նաև անվտանգության կանոնների ընդհանուր սկզբունքներին համապատասխան: Օգտագործողի ինտերֆեյսն (user interface) ամբողջությամբ իրագործվում է բրաուզերի միջոցով, իսկ բազան՝ MS SQL սերվերի: Այդ պարագայում համացանցային ինտերֆեյսի անվտանգությունը չափազանց կարևոր է:

Ինչպես արդեն նշվել էր անձնական տվյալներ մշակող համակարգը հնարավորություն ունի աշխատակիցներին մուտք գործել համակարգ հեռահար՝ աշխատանքային տարածքից դուրս: Առհասարակ անվտանգությունը այս դեպքում իրագործված է միայն որոշակի IP հասցեների համար սերվերի մեկուսացման սարքն (firewall) օգտագործելու միջոցով: Հեռահար աշխատանքի դեպքում մուտքն ապահովվում է SS մասնագետի մշտադիտարկման միջոցով՝ աշխատակցի հետ ուղղակի կապ հաստատելու միջոցով: Նման մոտեցումը ապահովում է անվտանգության որոշակի մակարդակ, սակայն համարվում է ռիսկային:

Կարևոր է նշել, որ համացանցայի կայքի միջոցով բազմաթիվ ծառայություններ հասանելի են նաև բնակիչներին: Ընդ որում, բնակիչները ծառայություններից օգտվելիս հաղորդում են իրենց անձնական տվյալները: Գնահատման պահին չորս ՏԻՄ-երից երկուսի կայքերի հետ կապը իրագործվում էր առանց անվտանգ արձանագրությունների (secure protocols) օգտագործմանբ և չունեին անվտանգության սերտիֆիկատներ:

Առանց անվտանգ արձանագրությունների (SSL/TLS) համացանցային ինտերֆեյսի օգտագործումը չափազանց ռիսկային է, քանի որ հեշտացնում է ներթափանցողի համար տվյալներ որսալու գրոհ անցկացնելու հնարավորությունը:

Նշված թերությունը հնարավոր է շտկել բավականին կարճ ժամկետում ու չափազանց կարևոր է այն իրագործել բոլոր ՏՄԻ-երում: Տեղեկատվական անվտանգության կանոնները մշակելիս անհրաժեշտ է ամրագրել անվտանգ արձանագրությունների (secure protocols) կիրառման և անվտանգության սերտիֆիկատների արդիության պահպանման պայմանները:

4.4 Ծրագրային ապահովման անվտանգությունը

Ծրագրային ապահովման (համակարգչային ծրագրերի) անվտանգության հարցը միշտ եղել է առանցքային: Այսօր համակարգչային ծրագրերի կիրառման ոլորտը ընդլայնվում է և ծրագրային անվտանգության հարցերին պետք է հատուկ ուշադրություն դարձնել: Անհրաժեշտ է նշել, որ բոլոր ՏԻՄ-մ այդ հարցը լուրջ բարելավում է պահանջում:

Առաջին հերթին պետք է նշել, որ ուսումնասիրված ՏԻՄ-ի համակարգերի մեծ մասը ունի լիեցենզիաներ միայն Ձերմուկի համայքապետարանում (90%): Անձնական տվյալներ պարունակող հարգային տվյալների բազաները (գույքի և հողի հարկի տվյալներ) օգտագործվում են MS Windows 7 և նույնիսկ MS WIndows XP համակարգերը, որոնք այլևս անվտանգության թերությունների վերացման թարմացումներ (security patching) չեն ստանում.

Անհրաժեշտ է նշել, որ աշխատանքային համակարգիչներում բացակայում են անվտանգության և հակավնասակար (anti-virus/malware protection) ծրագրերը: Անշուշտ հակավնասակիր ծրագրերը բավական թանկ են, և դրանց ձեռքբերումը անհրաժեշտ անվտանգության միջոցների հետ մեկտեղ կարող է ՏԻՄ-երի համար լինել բավական ծանր բեռ: Սակայն պաշտպանիչ ծրագրեր չօգտագործելու հետևանքները կարող են լինել շատ ավելի թանկ:

Բոլոր ՏԻՄ-երում, որտեղ անցկացվել է անձնական տվյալների պաշտպանության գնահատումը, աշխատակիցները կամ հնարավորություն ունեն համացանցից ներբեռնելու համակարգչային ծրագրեր, կամ այդ հնարավորությունը տրամադրվում է ըստ պահանջի՝ առանց անվտանգությունը գնահատելու և անհրաժեշտությունը հաստատելու ընթացակարգի: Նման պրակտիկան, մանավանդ հակավնասակար ծրագրերի բացակայության պայմաններում, պարունակում է լուրջ ռիսկեր և պետք է կասեցվի, իսկ հետագայում կանոնակարգվի անվտանգության կանոնների օգնությամբ:

5. Անձնական տվյալների մշակման օրենսդրական պահանջների վերաբերյալ ՏԻՄ աշխատակիցների իրազեկման մակարդակը

Ուսումնասիրությունից պարզ է դարձել, որ ընտրված ՏԻՄ-երից ոչ մեկի աշխատակիցները երբեւէ վերապատրաստման կամ ուսուցման չեն մասնակցել անձնական տվյալների պաշտպանության ոլորտում, որպեսզի կարողանան ճանաչել անձնական տվյալների անվտանգության խախտումները և պատշաճ իրականացնեն տվյալների մշակման գործընթացը: Անձնակազմը տեղյակ չէ նաեւ, թե ինչպես է անհրաժեշտ վարվել մշակման նպատակի համար ոչ անհրաժեշտ տվյալների հետ, ինչպես ջնջել կամ դադարեցնել այս կամ այն տվյալի մշակումը:

Անձնակազմը տեղյակ չէ նաեւ, թե երբ, ում և ինչ ընթացակարգով է պետք հաղորդել ՏԻՄ-ում անձնական տվյալների անվտանգության խախտումների և արտահոսքերի մասին: Նրանց գիտելիքն ու հմտությունները հիմնված են բացառապես աշխատանքային փորձի վրա, որը տարբեր ՏԻՄ-երի դեպքում տարբեր է:

Առանձին պետք է անդրադառնալ համակարգը շահագործող ու կառավարող աշխատակազմի որակավորմանը, տեղեկատվական անվտանգության ոլորտում ժամանակակից մեթոդների կիրառման, ինչպես նաև անձնական տվյալների պաշտպանության օրենսդրությամբ սահմանված պահանջների մասին իրազեկ լինելուն: Այն ՏԻՄ-երում, որտեղ անցկացվել էր գնահատումը, աշխատակիցներն ունեն համակարգերի անվտանգությունը ապահովելու համար բավարար մասնագիտական գիտելիք ու աշխատանքային փորձ: Սակայն, տվյալների պաշտպանությանը վերաբերող առանձնահատուկ գիտելիքի մակարդակը բավարար չէ, ինչը հնարավոր է արագ լրացնել կազմակերպելով համապատասխան կարճատև ուսուցում: ՏԻՄ-երի բոլոր աշխատակիցների համար պարբերաբար պետք է կազմակերպվեն իրազեկման միջոցառումներ՝ տեղեկատվական անվտանգության տարրական գիտելիքի բացերը լրացնելու նպատակով:

Անհրաժեշտ է նշել, որ թե անվտանգության քաղաքականություն և կանոններ մշակելու, թե այդ քաղաքականությունը և կանոնները կյանքի կոչելու տեսակետից լավագույն ու նախընտրելի լուծումը տեղեկատվական անվտանգության մասնագետի հաստիք ունենալն

է: Ընդ որում, հաշվի առնելով ՏԻՄ-երի սահմանափակ ֆինանսական հնարավորությունները, նույնանման խնդիրները և աշխատանքի համեմատաբար փոքր ծավալը (համեմատելով մեծ առևտրային ընկերությունների կամ նախարարությունների հետ) հնարավոր է ունենալ տեղեկատվական անվտանգության մասնագետի մեկ հաստիք մի քանի համայնքի համար:

6. Փորձագիտական եզրակացություն և առաջարկություններ

Ուսումնասիրությունը ցույց տվեց, որ ՏԻՄ-երում գործարկվող երկու էլեկտրոնային համակարգերի և քաղաքացիների սպասարկման գրասենյակների կողմից ծառայությունների մատուցման ընթացքում անձնական տվյալների մշակման գործընթացն իրականացվում է **օրինականության սկզբունքին համապատասխան**: **ՏԻՄ-երի կողմից մարդկանց անձնական տվյալները մշակվում են օրինական եւ որոշակի նպատակներով:** ՏԻՄ-երը մշակում են բացառապես ոլորտային օրենքներով նախատեսված անձնական տվյալներ օրենքով իրենց տրված լիազորությունների շրջանակում: Սակայն ուսումնասիրությունը բացահայտել է որոշ խնդիրներ կապված օրենսդրության որակի, համաչափության, հավաստիության, թափանցիկության սկզբունքների համապատասխանության, տվյալների սուբյեկտի համաձայնության պատշաճ ստացման, տարբեր կատեգորիաների տվյալների պաշտպանության ապահովման առումներով:

Կարծում ենք, խնդիրների մեծ մասը հնարավոր է լուծել որոշակի ներքին ընթացակարգային կանոններ մշակելու եւ ընդունելու շնորհիվ կարճ ժամանակում՝ միաժամանակ սահմանելով նաեւ կարգավորումներ ՏԻՄ աշխատակիցների պաշտոնների անձնագրերում: Միաժամանակ, անհրաժեշտ է պարբերաբար թարմացնել անձնական տվյալների մշակում նախատեսող օրենսդրությունը եւ ապահովել դրա ներդաշնակությունը փոխկապակցված այլ ոլորտների օրենսդրության հետ:

Բոլոր ՏԻՄ-երում անձնական տվյալների մշակման համար օգտագործվող համակարգերի և համապատասխան համակարգչային սարքերի և ցանցերի անվտանգության մակարդակը գրեթե նույն է: Ըստ առաջարկված մեթոդաբանության, բոլոր ՏԻՄ-ում ուսումնասիրության արդյունքներով տվյալների մշակման համակարգերի պաշտպանվածությունը կարելի է գնահատել «ոչ բավարար», ինչը պահանջում է հրատապ միջոցառումներ:

Աբովյան քաղաքի համայնքի մանկապարտեզի գրանցման համակարգը ըստ էության ներառված է համայնքային տեղեկատվական համակարգում: Հետևաբար, բոլոր ընդհանուր բնույթի դիտարկումները նույն կերպ վերաբերում են նաև այդ համակարգին: Առանձին հարցերը, որոնք վերաբերվում են Աբովյան քաղաքի մանկապարտեզների գրանցման համակարգին, նշված են համապատասխան մասում:

Ստորև բերված է գնահատման արդյունքներն ըստ մեթոդաբանությամբ սահմանված յուրաքանչյուր չափանիշի, ինչպես նաև գնահատման պարզաբանումը և բարելավմանն ուղղված առաջարկությունները:

Առաջարկներ ուղղված ներքին ընթացակարգերի եւ քաղաքականության բարելավմանը, ինչպես նաեւ ԱՏՊ օրենսդրությանը համապատասխանեցնելու նպատակով

1. Ուսումնասիրված բոլոր ՏԻՄ-երում անձնական տվյալները մշակվում են օրինականության սկզբունքին համապատասխան: Բոլոր այն դեպքերում, երբ քաղաքացիների անձնական տվյալները մշակվում են անձի համաձայնության հիման վրա, դրանք պետք է լինեն բացառություններ եւ նախատեսված օրենքով:

2. Անձնական տվյալների մշակում նախատեսող օրենսդրությունը բավարար չափով «որակյալ» չէ: Նկատի ունենք, որ թեեւ ոլորտային օրենքները նախատեսում են ՏԻՄ-երի՝ այս կամ այն անձնական տվյալներ մշակելու լիազորությունները, սակայն լայն իմաստով օրենքների թարմացվածությունը (օգտագործվող տերմինաբանությունը, բառակազմը, հստակությունը), օրենքներում էլեկտրոնային գործիքների կիրառման առանձնահատկությունների (ներառյալ՝ անձնական տվյալների անվտանգության ապահովման միջոցների) նկարագրությունը եւ փոխկապակցված այլ ոլորտների օրենսդրության (այդ թվում՝ արխիվացման) հետ ներդաշնակությունը բավարար մակարդակում չեն: Ուստի առաջարկում ենք քարտեզագրել օրենսդրության մեջ առկա բացերը անձնական տվյալների մշակման գործընթացը լավագույն փորձին համապատասխանեցնելու նպատակով եւ օրենսդրական փոփոխությունների առաջարկների փաթեթ մշակել՝ ակտիվորեն համագործակցելով ՀՀ ԱՆ ԱՏՊ գործակալության հետ:

3. Ուսումնասիրված ՏԻՄ-երում բացակայում են տվյալներ մշակելու ներքին բավարար ընթացակարգերը: Օրինակ, անհրաժեշտ ծավալով չի իրականացվում ԱՏՊ մշակման օրինական նպատակի համար ոչ պիտանի անձնական տվյալները բացահայտելու և սահմանված ժակետի ավարտից հետո դրանք վերացնելու կամ ջնջելու գործընթացը: Առկա չէ նաեւ գործընթաց օրինական նպատակին հասնելու համար ոչ անհրաժեշտ անձնական տվյալները բացահայտելու, վերացնելու, ոչնչացնելու կամ ուղեփակելու նպատակով: Ուստի, անհրաժեշտ է մշակել եւ ընդունել ՏԻՄ-երի կողմից անձնական տվյալների մշակման ներքին քաղաքականություն եւ ընթացակարգ, որով կսահմանվեն, օրինակ, անձնական տվյալների սուբյեկտների շրջանակը, տվյալների մշակման նպատակները, մշակող անձանց շրջանակը, տվյալների մշակման ժամկետները և պայմանները և այլ ոլորտային կարեւոր հարցեր: Անհրաժեշտ է նաեւ սահմանել հատուկ ընթացակարգ ոչ պիտանի անձնական տվյալները սահմանված ժակետի ավարտից հետո վերացնելու կամ ջնջելու գործընթացը կարգավորելու նպատակով:

4. Ուսումնասիրված ՏԻՄ-երից ոչ մեկում առկա չէ որոշակի ընթացակարգ անձնական տվյալների ճշգրտությունն ու թարմությունը ապահովելու համար: Առկա չէ թերի կամ ոչ ճշգրիտ կամ հնացած տվյալները հայտնաբերելու կամ տվյալների սուբյեկտի կողմից դիմում ստանալուց հետո անհապաղ կամ նման հնարավորության բացակայության դեպքում երեք աշխատանքային օրվա ընթացքում դրանք ամբողջացնելու, թարմացնելու, ուղղելու կամ ոչնչացնելու հարցերի կանոնակարգում: Այս հարցում իրավիճակը գնահատվել է ոչ բավարար: ՏԻՄ-երը պետք է հնարավորինս սեղմ ժամկետում մշակեն եւ ընդունեն այս հարցերը կանոնակարգող ներքին ընթացակարգ:

5. Ուսումնասիրված ՏԻՄ-երից ոչ մեկում առկա չէ մշակված ընթացակարգ, թե ինչպես պետք է ՏԻՄ-ը բացահայտի, հայտնաբերի եւ լիազոր մարմնին տեղեկացնի անձնական տվյալների արտահոսքի կամ այլ ռիսկերի դեպքում: Անհրաժեշտ է սեղմ ժամկետում մշակել եւ ընդունել այս հարցերի ներքին կանոնակարգ: Անհարժեշտ է նաեւ սեղմ ժամկետում ԱՏՊ գործակալություն ներկայացնել ծանուցում կենսաչափական տվյալներ մշակելու վերաբերյալ:

6. Ուսումնասիությունը ցույց է տվել, որ ՏԻՄ-երում առկա չէ որեւէ գործընթաց կամ ընթացակարգ ուղղված այն տվյալների վերացմանը, ոչնչացմանը կամ ուղեփակմանը, որոնք անհրաժեշտ չեն օրինական նպատակին հասնելու համար: Չկա ընթացակարգ նաեւ թերի, ոչ ամբողջական տվյալներն ուղղելու փոփոխելու հետ կապված: Ինչպես նաև, բավարար ռեսուրսներ ու ջանքեր չեն ներդնում բացահայտելու հնացած կամ թերի տվյալները և օրենքով սամանված ժամկետներում դրանք ամբողջացնելու, թարմացնելու, ուղղելու կամ ոչնչացնելու նպատակով: Այս հարցում ՏԻՄ փորձը գնահատվել է ոչ բավարար:

7. Անհրաժեշտ է մշակել եւ ընդունել անձնական տվյալներ մշակելու վերաբերյալ սուբյեկտի համաձայնության օրինակելի ձեւ, որը կօգտագործվի քաղաքացիների կամ ՏԻՄ աշխատակիցների տվյալները մշակելու նպատակով: Մասնավորապես, համաձայնության օրինակելի ձևում հստակ կնշվի մշակվող տվյալների շրջանակը, մշակման նպատակը, այն գործողությունները, որոնք պետք է կատարվեն այդ տվյալների հետ, այն անձանց շրջանակը, ում հասու են դառնալու տվյալները, այն ժամկետը, որի սահմաններում պահպանելու են տվյալները եւ այլ կարեւոր ենթահարցեր:

8. Ընթացակարգային հարցերից է նաեւ լիազորված կազմակերպության ՏՀՁՎԿ-ի եւ ՏԻՄ-երի միջեւ կնքված պայմանագրերի վերանայումը: Մասնավորապես, անհրաժեշտ է պայմանագրերը համապատասխանեցնել ԱՏՊ օրենքի 14-րդ հոդվածով սահմանված կանոններին: ՏԻՄ և ՏՀՁՎԿ միջեւ կնքված պայմանագրում պետք է հստակ արտացոլվեն հետեւյալ դրույթները.

    - պետք է շարադրված լինեն անձնական տվյալներ մշակելու իրավական հիմքերը եւ պայմանները,
    - անձնական տվյալներ մշակելու նպատակը,
    - մշակման ենթակա անձնական տվյալների ցանկը,
    - տվյալների սուբյեկտների շրջանակը,
    - այն անձանց շրջանակը, որոնց կարող են փոխանցվել անձնական տվյալները,
    - անձնական տվյալների պաշտպանության տեխնիկական եւ կազմակերպչական միջոցառումները եւ անհրաժեշտ այլ տեղեկություններ:

9. Անհրաժեշտ է բարեփոխել ՏԻՄ աշխատակիցների աշխատանաքային պայմանագրերը եւ աշխատանքի նկարագրությունները՝ պատշաճ ապահովելով դրանցում ԱՏՊ իրավահարաբերությունների լիարժեք արտացոլումը:

10. Անհրաժեշտություն կա նաև մշակելու եւ հանրայնացնելու անձնական տվյալների մշակման եւ անվտանգության քաղաքականությունները (privacy policy), որոնք պետք է սահմանեն ՏԻՄ-երի կողմից անձնական տվյալների մշակման իրավական հիմքերը, նպատակները, ինչպես նաեւ անձնական տվյալների հետ կատարման

ենթակա գործողությունների ցանկը, տվյալների սպառիչ ցանկը եւ այլն): Մշակված քաղաքականությունները կարող են հրապարակվել նաեւ ՏԻՄ պաշտոնական կայքերում:

11. Ուսումնասիրված ՏԻՄ-երից ոչ մեկում նշանակված չէ ԱՏՊ պատասխանատու անձ: Անհրաժեշտ է սեղմ ժամկետում նշանակել ԱՏՊ պատասխանատու անձ, ում լիազորությունը կլինի ՏԻՄ-ում անձնական տվյալների պաշտպանությունն ու անվտանգության ապահովումը: Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձը պետք է.

    - ապահովի «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով սահմանված՝ անձնական տվյալներ մշակողի պարտականությունների կատարումը,
    - ապահովի պետական մարմնի կապն անձնական տվյալների պաշտպանության լիազոր մարմնի հետ, այդ թվում՝ կազմակերպի անձնական տվյալների մշակման վերաբերյալ խորհրդատվության ստացումը,
    - կազմի և անձնական տվյալների պաշտպանության լիազոր մարմին ներկայացնի անձնական տվյալների պաշտպանության վերապատրաստման՝ պետական մարմինիներկայացուցիչների ցուցակը,
    - ինչպես նաև ԱՏՊ օրենքով սահմանված այլ լիազորություններ:

Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձի հետ կապ հաստատելու տվյալները (էլեկտրոնային փոստի հասցեն, հեռախոսահամարը) պետք է հրապարակվեն ՏԻՄ-ի պաշտոնական կայքում: Անհրաժեշտ է իրականացնել մեկից վեց ամսվա ընթացքում:

Առաջարկներ ուղղված տվյալների մշակման համակարգերի պաշտպանվածության և անվտանգության ապահովմանը

1. Անվտանգության քաղաքականությունը ու կանոնների առկայությունը բացակայում է բոլոր ՏԻՄ-երում: Իրավիճակը գնահատվել է որպես ոչ բավարար, սակայն ոչ ծայրահեղ: Անհրաժեշտ է շտկել մեկից վեց ամսվա ընթացքում:

2. Շարժական ու հեռահար աշխատանքների կանոնների առկայություն բացակայում է բոլոր ՏԻՄ-երում: Իրավիճակը գնահատվել է որպես ոչ բավարար, սակայն ոչ ծայրահեղ: Անհրաժեշտ է շտկել մեկից վեց ամսվա ընթացքում:

3. Հեռահար աշխատանքները թույլատրված են բացառության կարգով, սակայն.

    - Բացառությամբ Ջերմուկի համայնքի չեն օգտագործվում ՎՄՑ-ը (VPN):
    - Աշխատակիցների նույնականացումը բավարար է:
    - Ցանցի մշտադիտարկման գործիքներն օգտագործվում են, սակայն ավտոմատիզացված չեն և ոչ անընդհատ:

Իրավիճակը գնահատվել է որպես ոչ բավարար բոլոր համայնքներում, բացառությամբ Ջերմուկի: Պահանջում է հնարավորինս արագ լուծում՝ ՎՄՑ-ի պարտադիր օգտագործում:

4. Անվտանգության մասնագետների հաստիքները կամ արտաքին խորհրդատուներ վարձակալելու հնարավորությունները նախատեսված չեն: Իրավիճակը գնահատվել է որպես ոչ բավարար, սակայն ոչ ծայրահեղ: Անհրաժեշտ է գտնել լուծում առկա ռեսուրսների շրջանակներում: Ժամանակավոր լուծում կարող է լինել արտաքին մասնագետների ներգրավվումը՝ ծայրահեղ նշանակություն ունեցող անվտանգության բացերը շտկելու նպատակով:

5. Համակարգերում պահպանվող անձնական տվյալների գաղտնագրումը բացակայում է: Տվյալների բազաները պաշտպանված են գաղտնաբառային համակարգերով: Իրավիճակը գնահատվել է որպես ոչ բավարար, ծայրահեղ, սակայն արագ լուծում ամենայն հավանականությամբ գտնել հնարավոր չէ: Անհրաժեշտ է շտկել համակարգը վերանախագծման կամ կատարելագործման փուլում: Կարող է պահանջել մինչև մեկ տարի աշխատանք՝ արտաքին մասնագետների այդ թվում սպասարկող կազմակերպության (ՏՀՋԿԿ) մասնակցությամբ:

6. Ցանցային պաշտպանության միջոցները առկա են մասամբ՝ օգտագործվում է ցանցը մեկուսացման սարք/համակարգ (firewall), սակայն ներթափանցման բացահայտման (intrusion detection) և ներթափանցման կանխարգելման (intrusion prevention) համակարգերը չեն օգտագործվում: Այնուամենայնիվ, հաշվի առնելով համաչափության սկզբունքը իրավիճակը գնահատվել է որպես բավարար: Դա, սակայն, չի նշանակում, որ վերոհիշյալ համակարգերի կիրառումը անհրաժեշտ չէ և կարող է անտեսվել: Վերջնական որոշումը պետք է կայացվի հաշվի առնելով վտանգների հավանականությունը և հետևանքները:

7. Անձնական տվյալներ մուտք գործելու գրանցումները (access logs) պահպանվում են և պարբերաբար կարող են վերլուծվել (access log audit): Բոլոր ՏԻՄ-երում իրավիճակը գնահատվել է որպես բավարար:

8. Վնասակար ծրագրերից պաշտպանության համակարգերը և հակավնասակար ծրագրերը (anti-virus and anti-malware tools and systems) չեն կիրառվում: Սիսիանում կիրառվել են անվճար ծրագրեր, որոնք սովորաբար արդյունավետ չեն: Իրավիճակը գնահատվել է որպես ոչ բավարար և ծայրահեղ: Պահանջում է անհապաղ շտկում՝ մեկից երեք ամսվա ընթացքում:

9. Անձնական տվյալներ պարունակող համակարգը տեղադրված է պաշտպանված տարածքում: Իրավիճակը կարող է համարվել բավարար, սակայն որոշ բարելավումն անհրաժեշտ է: Մասնավորապես, անհրաժեշտ է լուծել շարժական կրիչների պաշտպանվածության (գաղտնագրման ու օգտագործման կանոնների) հարցը, ինչպես նաև վթարային իրավիճակներին արձագանքելու կանոնների խնդիրները:

10. Համացանցային կայքում հրապարակվող տվյալները անմիջականորեն կապված չեն անձնական տվյալների բազաների հետ: Իրավիճակը կարելի է համարել բավարար, սակայն համակարգի կառուցվածքի համար էական նշանակություն այն տվյալ պահին չունի: Միևնույն ժամանակ արագ անհրաժեշտ է լուծել կայքերի

անվտանգության սերտիֆիկատների և անվտանգ արձանագրությունների (TSL/SSL, HTTPS) կիրառման հարցը:

11. Գաղտնաբառերի օգտագործման կանոնները բացակայում են: Սիսիանի համայքապետարանում կիրառվող մոտեցումները ընդհանուր առմամբ համապատասխանում են ոլորտում ընդունված չափանիշներին, սակայն ևս կանոնակարգված չեն: Իրավիճակը գնահատվել է որպես ոչ բավարար, ծայրահեղ և պահանջում է արագ շտկում (մեկից երեք ամիս):

12. Մուտքի իրավասությունները կառավարման (access privileges management) իրականացվում են ըստ խմբերի, հաշվի առնելով աշխատակիցների պարտականությունները ըստ ծառայողական անձնագրերի: Սակայն, գործընթացը կանոնակարգված չէ: Իրավիճակը համարվել է բավարար, սակայն պահանջում է հստակ կանոնակարգում:

13. Անվտանգ բազմակի նույնականացման միջոցներ (multi factor authentication) մուտքը համակարգ չի կիրառվում ոչ համակարգի հեռահար կառավարման, ոչ էլ հեռահար աշխատանքներ կազմակերպելու դեպքում: Անհրաժեշտ է կիրառել առնվազն հեռահար աշխատանքների համար՝ մանավանդ կարգավորման/տնօրինման իրավասություններ (administrator privilages) ունեցող աշխատակիցների համար: Իրավիճակը գնահատվել է որպես ոչ բավարար, սակայն ոչ ծայրահեղ: Լուծումները պետք է նախատեսել համակարգը լրամշակելու կամ վերանախագծելու դեպքում:

14. Ծրագրային ապահովությունը և անվտանգության թերությունները չեն թարմացվում: Իրավիճակը գնահատվել է որպես ոչ բավարար և ծայրահեղ: Խնդիրը պահանջում է շտապ լուծում՝ թե կանոնակարգման, թե տեխնիկական իրագործման պարագայում: Անհրաժեշտ է շուտափույթ պլանավորել և աստիճանաբար իրագործել շահագործումից հնացած և անվտանգության ապահովում չստացող (technical support and serucity patching) սարքավորումների և համակարգերի դուրս գրման գործընթացը:

15. Անձնական տվյալների և առհասարակ համակարգչային տեխնիկայի համակարգերի մատակարարների վստահության և կարողության ստուգում ՏԻՄ-երում չի անցկացվում: Սակայն, հաշվի առնելով, որ մատակարարների խնդիրը պետք է լուծվի պետական և համայնքային գնումները կարգավորող օրենսդրության շրջանակներում, այս չափանիշը գնահատման ընթացքում համարվել է անվերաբերելի: Սակայն, անվտանգության քաղաքականությունը և կանոնները մշակելիս անհրաժեշտ է նախատեսել մատակարարների ստուգման գործընթաց՝ հանրային-մասնավոր համագործության ծրագրերի շրջանակներում:

16. Անձնական տվյալների մշակման համակարգերի անվտանգության թեստավորման կանոններ չկան: Պահանջը համարվել է անբավարար, սակայն քանի որ ծրագրային ապահովության որակի խնդիրը՝ այդ թվում նախնական ստուգման և սերտիֆիկացման՝ պետք է լուծվի պետական և համայնքային գնումները կարգավորող օրենսդրության շրջանակներում, գնահատման այս չափանիշը համարվել է անվերաբերելի և գնահատման վրա չի ազդել:

17. Մատակարարի ու սպասարկող կազմակերպության չվերահսկվող մուտքը կամ միջամտությունը համակարգի աշխատանքին ըստ գործող պրակտիկայի բացակայում է: Իրավիճակը գնահատվել է որպես բավարար, սակայն սպասարկող կազմակերպության և ՏԻՄ-ի SS մասնագետների համագործակցությունը մուտք գործելուց անհրաժեշտ է կանոնագարգել կանոններով կամ արձանագրությամբ:

18. Վճարներին և կիբեր հարձակումներին արձագանքելու ընթացակարգերը բացակայում են: Իրավիճակը գնահատվել է որպես ոչ բավարար ու ծայրահեղ: Սակայն իրավիճակը շտկելու շտապ լուծումներ գտնելը քիչ հավանական է: Լավագույն դեպքում խնդիրը կարող է լուծում ստանալ երեքից վեց ամսվա ընթացքում և հնարավոր կլինի համակարգչային անվտանգության արտաքին մասնագետների մասնակցությամբ:

Առաջարկություններ ուղղված ԱՏՊ ոլորտում ՏԻՄ կարողությունների և հմտությունների զարգացմանը

1. ՏԻՄ կարողություններն ու հմտությունները գնահատվել են ոչ բավարար: ՏԻՄ աշխատակիցներից որեւէ մեկը չի անցել ԱՏՊ ոլորտում համապատասխան վերապատրաստում: Առաջարկում ենք ՏԻՄ աշխատակիցներին սեղմ ժամկետում ներգրավել ՀՀ Արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալության կողմից իրականացվող վերապատրաստումներում: Միեւնույն ժամանակ, հաշվի առնելով գործակալության ծանրաբեռնվածությունը, կարծում ենք, այս փուլում կարող է նպատակահարմար լինել նաև ՏԻՄ-երի կողմից ուսուցումների կազմակերպում համայնքապետարանի բյուջեի միջոցներով կամ միջազգային դոնոր կազմակերպությունների աջակցությամբ՝ ներգրավելով անկախ փորձագետների անձնական տվյալների պաշտպանության թեմայով անձնակազմի համապարփակ ուսուցում իրականացնելու նպատակով:

2. Ուսուցումները համակարգված եւ հասցեական իրականացնելու նպատակով անհրաժեշտ է մշակել Անձնական տվյալների պաշտպանությունը ՏԻՄ համակարգում թեմայով ուսումնական ծրագրի մոդուլ, որը նախատեսված կլինի համայնքային ծառայողների համար պարբերական ուսուցումներ կազմակերպելու եւ այս ոլորտում նրանց կարողությունները զարգացնելու համար:

3. Առաջարկում ենք նաև մշակել անձնական տվյալների մշակման հանգամանալից եւ գործնական ուղեցույց (ձեռնարկ) համայնքային աշխատակիցների համար՝ ինչպես իրականացնել քաղաքացիների եւ անձնակազմի անձնական տվյալների մշակման գործընթացը: Որպես լավագույն փորձ կարող ենք առաջարկել Մեծ Բրիտանիայի տեղեկատվության և անձնական տվյալների հանձնակատարի գրասենյակի պատրաստած ուղեցույցը:[6]

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=1#link20

4. Անձնական տվյալների մշակման գործընթացի բարելավումը մշտական դարձնելու նպատակով առաջարկում ենք իրականացնել ՏԻՄ-երի կողմից անձնական տվյալների մշակման գործընթացների պարբերական գնահատում (Data Protection Compliance and Impact Assessment), ռիսկերի վերհանում եւ կառավարում: Այս գնահատումը միջոց է համակարգված և համակողմանիորեն վերլուծելու տվյալների մշակման գործընթացը և օգնել բացահայտել, կառավարել և նվազագույնի հասցնել տվյալների պաշտպանության հետ կապված ռիսկերը:

5. ՏԻՄ գործիքակազմը հզորացնելու նպատակով առաջարկում ենք նաեւ մշակել եւ գործարկել ՏԻՄ-երի ինքնագնահատման հարցաթերթ (self assessment checklist), որի միջոցով ՏԻՄ-երը կարող են որոշակի պարբերականությամբ գնահատել իրենց ներքին կարողություններն ու գործընթացները՝ ապահովելով շարունակական բարելավում:

   Այս ինքնագնահատման գործիքակազմի կիրառման շնորհիվ կբարձրանա ՏԻՄ-երի հեղինակությունը, քաղաքացիների եւ աշխատակիցների վստահությունը, և անձնական տվյալների ճշգրիտ, համաչափ և անվտանգ լինելու շնորհիվ կխնայվեն և՛ ժամանակը, և՛ տեխնիկական միջոցները:

Այլ հարցեր

Տեսահսկման գործընթացի կանոնակարգում

Քանի որ ուսումնասիրված 4 ՏԻՄ-երից երեքում (բացի Ջերմուկից) իրականացվում է տեսահսկման գործընթաց, ուստի անհրաժեշտություն կա գործընթացն անհապաղ համապատասխանեցնել ԱՏՊ գործակալության մշակած կանոններին [7]: Մինչ այդ, անհրաժեշտ է ընդունել տեսահսկման ներքին ընթացակարգ՝ խորհրդակցելով ՀՀ ԱՆ ԱՏՊ գործակալության հետ:

Տվյալների սուբյեկտների իրազեկում

Լրացուցիչ խնդիրների ցանկում անհրաժեշտ է նշել նաեւ քաղաքացիների՝ անձնական տվյալների ոլորտում իրազեկվածության ցածր մակարդակի հարցը: ՏԻՄ-երը կարող են կարեւոր գործառույթ իրականացնել համայնքի բնակիչներին՝ տվյալների սուբյեկտներին իրենց անձնական տվյալների պաշտպանության նվազագույն կանոններին ծանոթացնելու և իրազեկելու նպատակով՝ կազմակերպելով իրազեկման արշավներ՝ ակտիվ համագործակցելով ՀՀ ԱՆ ԱՏՊ գործակալության հետ:

7. Հավելվածներ

1. Գնահատման մեթոդաբանություն
2. Գնահատման հարցաթերթ
3. Տվյալների հոսքի դիագրամ/աղյուսակ

[7] http://www.foi.am/u_files/file/Manual_Video.pdf