

Թեմա 2 - Թվային գործիքներ և համագործակցություն

3. Կապ

Այս գլխում կձևաթանաք հետևյալ թեմաներին.

- Էլեկտրոնային մեյլ օգտագործելիս կապի սահմանափակումներ.
- Էլեկտրոնային մեյլի խմբեր.
- Ամպային պահեստ.
- Սպամ.
- Համացանց.
- Ինտրանետներ.
- World wide web (www).
- Բլոգներ, վիկիներ և սոցիալական կայքեր.
- Համացանցում ինֆորմացիայի որոնում:

Այս գլուխն ընդգրկում է համացանցից օգտվելու որոշ ասպեկտներ: Մենք կքննարկենք Էլեկտրոնային նամակներ ուղարկելու կանոնները և կարգավորումները, ինչպես նաև համացանցի որոշ առանձնահատկություններ: Մասնավորապես, մենք կսահմանենք և կբացատրենք մի շարք համացանցային տերմիններ և ինչպես փնտրել ինֆորմացիա համացանցում: Գլուխը նաև ընդգրկում է համացանցի, world wide web-ի և ինտրանետների տարբերությունը:

10.1 Կապն այլ ICT օգտատերերի հետ Էլեկտրոնային մեյլի միջոցով

10.1.1 Սահմանափակումներ

Էլեկտրոնային նամակները ներկայումս մարդկանց միջև շփման ամենատարածված ձևերից են: Սակայն կան մի շարք կանոններ, որոնց պետք է հետևել՝ անվտանգությունն ապահովելու և անթույլատրելի գրառումները կանխելու համար: Գլխի առաջին մասն ընդգրկում է հետևյալ սահմանափակումները:

Օրենքներ

Ճատ երկրներ ունեն կանոններ, որոնք պաշտպանում են մարդկանց Էլեկտրոնային մեյլերի շահագործումից: Հետևյալ ցուցակը կանոնների ուղեցույց է: Ճատ երկրներ պահանջում են ընկերություններից և անհատներից հետևել այդ կանոններին Էլեկտրոնային նամակներ ուղարկելիս:

- **Ճատ երկրներ պահանջում են նամակ ուղարկողներից ձեռք բերել «մասնակցության» իրավունք մինչև էլեկտրոնային նամակներ ուղարկելը:**
- **Կարևոր է, որ էլ.նամակները չուղարկեն կեղծ կամ ապակողմնորոշող թեմաներով:**
- **Ընկերությունը կամ անհատը պետք է ունենա պարզ ձև ստացողների՝ նամակը ստանալուց հրաժարվելու համար:**
- **Վավեր փոստային հասցեն պետք է ուղեկցի ընկերություններից և կազմակերպություններից էլ.նամակները:**
- **Ընկերությունները պետք է բաժանորդներին տրամադրեն բաժանորդագրությունից հրաժարվելու պարզ ճանապարհ:**
- **Ճատ երկրներ թույլ չեն տալիս ընկերություններին և կազմակերպություններին պահել էլ.հասցեները (էլ. հասցեների ձեռքբերման գործընթացն է):**
- **Ընկերությունները և կազմակերպությունները պետք է իրենց գաղտնիության քաղաքականությունը շատ պարզ ներկայացնեն իրենց բաժանորդներին, վերջիններս էլ պետք է քաջատեղյակ լինեն այդ քաղաքականությանը:**

Ընդունելի խոսելաձև

Խոսելաձևը, որը մարդիկ օգտագործում են էլ.նամակներում, պետք է պրակտիկայի օրենսգրքի սահմաններում լինի: Հետևյալ ցուցակը ցույց է տալիս այն անթույլատրելի բովանդակությունը, որը կարող է հայտնվել էլ. նամակներում, տեքստային նամակներում և օնլայն ֆորումներում.

- անպարկեշտ նկարներ,
- վիրավորական, սրբապիղծ, բորբոքող, հարկադրական, զրպարտչական կամ հայիոյանք պարունակող խոսք,
- ռասիստական, շահագործող և անկիրթ նամակներ,
- անօրինական նյութերի օգտագործում նամակներում:

Այս ցուցակը չի ընդգրկում ամեն ինչ, սակայն մոտավոր ներկայացնում է, թե ինչն է անթույլատրելի համացանցում նամակ կամ ապրանք ուղարկելիս: Ճատ երկրներ սահմանում են խիստ տուգանքներ տրված սահմաններից անցնելու

համար, և եթե որոշ նամակներ կամ նկարներ համապատասխան չեն, ստացողները կարող են դրանք պարզապես ջնջել:

Պարտադիր է, որ յուրաքանչյուր ոք [Էլ.նամակ գրելիս](#) կամ հաղորդագրությունների տախտակի վրա որևէ բան տեղադրելիս տեղյակ լինի հետևյալ սահմանափակումներից:

Ջեդիսակային իրավունքը

Կարևոր է հասկանալ, որ [Էլ.նամակները](#) նույնպես ենթարկվում են հեղինակային իրավունքի օրենքներին: Չնայած նամակ փոխանցելը բավականին հեշտ գործընթաց է, այն ոչ միշտ է օրինական: Սա նաև վերաբերում է նամակին կցված ցանկացած նյութին:

Ինչ վերաբերում է վեբ կայքերին, հեղինակային իրավունքը որոշվում է դրանց բովանդակությամբ:

Տպելը, պատճենելը և նամակներ փոխանցելը հիմնականում հեղինակային իրավունքի խախտում չի համարվում, եթե իհարկե նամակատերը հատուկ չի նշել, որ նամակը կոնֆիդենցիալ է և հեղինակային իրավունք ունի: Նամակ ստացողի համար կարևոր է ստուգել դա մինչև նամակը մեկ ուրիշին փոխանցելը: Ծատ կազմակերպություններ և ընկերություններ պարզ ներկայացնում են իրենց [Էլ.նամակ ուղարկելու օրենքները](#) և պարունակվող նյութերը: Սա հատկապես վերաբերում է այն ուղարկողներին, որոնց անվան մեջ մտնում է կազմակերպության անունը, օրինակ՝

A.N.User@company_name.com: Կազմակերպություններից և ընկերություններից ստացված [Էլ.նամակները](#) և կցված ֆայլերը սովորաբար պարունակում են հեղինակային իրավունքի մասին հայտարարություն, օրինակ.

Տվյալ [Էլ.նամակի](#) կամ կցված ֆայլի տարածումը կամ պատճենումը խստորեն արգելվում է, եթե դուք նախատեսված ստացողը կամ ուղարկելու համար պատասխանատուն չեք: Եթե շփոթմունքի հետևանքով եք ստացել այս [Էլ.նամակը](#), տեղյակ պահեք մեզ և ջնջեք բնօրինակն ու ցանկացած կցված ֆայլ:

Հաղորդագրության համար ընդունված է նաև հայտարարել, որ նամակում գրված հայացքներն ու կարծիքները չեն ներկայացնում կազմակերպության հայացքներն ու կարծիքը, և բովանդակությունը կարող է ենթակա լինել բացահայտման «Տեղեկատվության ազատության մասին» օրենքի համաձայն: Կազմակերպությունները մտահոգված են հեղինակային իրավունքի խախտման ամեն մի հավանական ռիսկով:

Անվտանգություն և գաղտնաբառի պաշտպանություն

Ճատ կարևոր է հաշվի առնել Էլ.նամակների անվտանգությունը: Ճատ անվտանգության ասպեկտների արդեն անդրադարձել ենք, սակայն որոշ գործոններ հաշվի առնելու հարցերը կրկնվում են սպառիչ լինելու համար:

Որոշ մեթոդներ Էլ.նամակների անվտանգությունը բարձրացնելու համար.

- օգտագործել ուժեղ գաղտնաբառեր մուտք գործելիս (օրինակ՝ ձեր սիրած ընտանի շան անունը թույլ գաղտնաբառ է, ուժեղ գաղտնաբառերը պարունակում են տառերի, թվերի և այլ նշանների համակցություն. Sy12@#TT90kj=0 կհամարվիր ուժեղ գաղտնաբառ),
- հաճախակի փոփոխել գաղտնաբառերը,
- օգտագործել սպամի ֆիլտրներ կասկածելի Էլ.նամակներից ազատվելու կամ ուղարկողին արգելափակելու համար,
- մշտապես օգտագործել հակավիրուսային կամ հակասպամ ծրագիր համակարգչում այն անձանոթ կամ վտանգավոր աղբյուրներից Էլ.նամակներ ստանալուց պաշտպանելու համար:

Էլ. նամակները կարող են լինել խոցելի թե՛ պասիվ, թե՛ ակտիվ հարձակումների համար: Պասիվ հարձակումներն իրենցից ներկայացնում են առանց ձեր համաձայնության ուրիշներին Էլ.նամակներ ուղարկելը: Ակտիվ հարձակումները ձեր հաղորդագրությունների փոփոխությունն են կամ նույնիսկ ծառայության մերժումը (այսինքն՝ հազարավոր նամակներ ուղարկել, որոնք գերձանրաբեռնում են համակարգիչը և դարձնում համացանցից օգտվելը գրեթե անհնար): Ակտիվ հարձակումներից են նաև վիրուսները և ֆիշինգ հարձակումները:

Նետիկետ

Նետիկետը ինտերնետ Էտիկետի կրճատ տարբերակն է, ըստ որի՝ պետք է հարգել այլ օգտատերերի հայացքները և ցույց տալ ընդհանուր քաղաքավարություն օնլայն քննարկման խմբերում հայացքներ տեղադրելիս կամ Էլ.նամակներ ուղարկելիս: Միշտ կարևոր է հաշվի առնել՝ ինչ եք գրում, քանզի կարդացողը չի կարող տեսնել ձեր դեմքի արտահայտությունը կամ ժեստերը: Մի բան, որը պետք է լիներ հումորային, կարող է վիրավորել ոմանց, եթե նրանք սխալ հասկանան հաղորդագրությունը և սխալ եզրակացություններ անեն: Միշտ հիշեք այս մասին հաղորդագրություններ ուղարկելիս կամ Էլ.նամակներ գրելիս:

Կան մի շարք կանոններ, որոնք կառավարում են նետիկետը. այդպիսի աղբյուր է Վիրջինիա Շեայի «The Core Rules of Netiquette»-ը (տպագրված 1994-ին): Տվյալ ցուցակը կարդացողին մոտավոր ներկայացնում է նետիկետի կանոնները:

1. Մի եղեք բռնի. մի՛ սպառնացեք մարդկանց կամ մի թույլ տվեք անձնական բռնություն:
2. Մի ուղարկեք սպամ.մի՛ ուղարկեք ինչ-որ մեկին նույն ինֆորմացիան մի քանի անգամ:
3. Եղեք պարզ և հակիրճ ձեր հաղորդագրություններում. մի՛ շատախոսեք:
4. Հիշեք, որ գրառումները հանրային են և շատ դեպքերում բոլորը կարող են դրանք կարդալ:
5. Միշտ ստուգեք ձեր ուղղագրությունն ու քերականությունը. թողեք լավ տպավորություն:
6. Հարգեք մարդկանց գաղտնիությունը և մի քննարկեք կամ հրապարեք ինֆորմացիա, որը կարող է մեկին խայտառակել:
7. Ներեք մարդկանց սխալները. պարտադիր չէ սխալներին պատասխանելը:
8. Մի օգտագործեք ՄԵԾԱՏԱՌԵՐ մեկնաբանություններն ընդգծելու համար. սա դիտվում է որպես «բղավոց» Էլ.նամակներում, տեքստային հաղորդագրություններում և օնլայն ֆորումներում:
9. Գրագողությամբ մի զբաղվեք. միշտ հիշեք մեջբերումների մասին ցանկացած նամակ գրելիս:
10. Մի օգտագործեք շատ Էմոջիներ, դրանք կարող են զայրացնել ձեզ կարդացողներին:

10.1.2 Սպամ

Համացանցով ուղարկված անցանկալի Էլ.նամակները կոչվում են սպամ: Այն հաճախ ուղարկվում է մի քանի հասցեատիրոջ և կարող է լինել պարզապես զայրացնող կամ նույնիսկ վտանգավոր: Սպամը կարող է պարունակել վիրուսներ կամ ֆիշինգի միջոցով խաբեության մաս լինել (տե՛ս նախորդ գլուխները): Բառի ծագումը բաց է քննարկման համար. մեկնաբանությունները բազմաթիվ են՝ սկսած հին պատերազմական ուտելիքից, որը կոչվում էր սպամ, մինչև BBC-ի «Մոնթի Փայթոն» երգիծական հեռուստասերիալում անընդհատ կրկնվող բառը («սպամ, սպամ, սպամ, սպամ...»):

Սպամը կարող է ազդել բազմաթիվ օնլայն գործողությունների վրա (օրինակ՝ Youtube-ի), որտեղ տեղադրվում են լինքեր (կոչվում են «սպամբոտ»), որոնք հասցեատերերին տանում են դեպի այլ կայք:

Չնայած ոմանք սպամը համարում են գովազդի էժան եղանակ, մարդկանց մեծ մասին դա մեծ անհանգստություն է պատճառում: Հիմնական թերություններն են՝

- վատնում է մարդկանց ճամանակը,
- հիմնականում զայրացնում է մարդկանց,

- օգտագործում է արժեքավոր թողունակություն համացանցում, դանդաղեցնում է այն,
- կարող է ունենալ կցված վիրուսներ, լինել ֆիշինգ խաբեության մաս կամ խցանել օգտատերերի փոստային արկղերը:

Սպամը խնդիր է ոչ միայն համակարգից օգտվողների համար. այն նաև կարող է ազդել բջջային հեռախոսների վրա: Այս դեպքում այն տեքստային հաղորդագրություն է, որն ուղարկվում է մի քանի բջջային: Դրանք երբեմն կոչվում են «սպամ» (սպամ SMS). դրանք պարզապես զայրացնում են մարդկանց, մանավանդ որ շատ երկրներում կամ մի շարք բջջային օպերատորներ օգտատիրոջից գումար են գանձվում տվյալ նամակները ստանալու համար:

10.1.3. Էլ.փոստերի խմբեր

Էլ. փոստերի խմբերն օգտագործվում են մի շարք պատճառներով՝

- օգտատիրոջ համար ավելի հեշտ է մի քանի էլ. նամակ ուղարկելը, եթե բոլոր հասցեները խմբավորված են մի անվան տակ. օգտատերը միայն պետք է օգտագործի մեկ անուն «to» մասում,
- ընկերությունները և կազմակերպությունները կարող են խմբավորել մարդկանց մարկետինգի համար, օրինակ՝ ըստ տարիքի, էթնիկ պատկանելիության, հոբբիների, սիրած երաժշտության և այլն. սա նշանակում է, որ յուրաքանչյուր էլ.նամակ կարող է թիրախավորել կոնկրետ խմբի,
- «սպամերները» կարող են էլ.փոստերի խմբեր ստեղծել՝ գնելով մարդկանց հասցեներ որոշ կազմակերպություններից կամ էլ օգտագործելով համակարգչային կամ էլեկտրոնային կազմակերպությունների հասցեագրքեր գրոհող ծրագրեր.սա նշանակում է, որ նրանք կարող են ուղարկել հազարավոր մարդկանց նամակներ՝ ընդամենը սեղմելով «enter» կոճակը,
- ընկերություններն օգտագործում են էլ.փոստի խմբերը հանդիպումներ կազմակերպելու համար (օրինակ՝ տեսազանգեր), որպեսզի ապահովեն բոլոր հրավիրվածների մասնակցությունը. ինչ-որ մեկին մոռանալը ավելի հեշտ է, եթե էլ. հասցեները գրվում են անհատական, այս միջոցով կարող եք վստահ լինել, որ բոլոր ճիշտ մարդիկ ստացել են նամակները:

10.2 Համացանցի արդյունավետ օգտագործում

10.2.1 Համացանցը

Յամացանցը ցանցերի համաշխարհային հավաքածու է, որը թույլ է տալիս օգտատերերին՝

- ուղարկել և ստանալ էլ. նամակներ,
- շփվել առցանց (օգտագործելով տեքստային, ձայնային կամ տեսահաղորդագրություններ),
- կատարել ֆայլերի փոխանակումներ համակարգիչների միջև,
- թերթել համաշխարհային ցանցը:

2015 թվականի տվյալներով՝ շուրջ մեկ միլիարդ մարդ աշխարհում օգտվում էր համացանցից: Յամացանցը չունի կոնկրետ սեփականատեր և չի պատկանում որևէ կազմակերպության: Այն ավելի շատ հայեցակարգ է, քան որևէ շոշափելի բան և ապավինում է ֆիզիկական ենթակառուցվածքներին, որոնք միացնում են ցանցերն իրար:

World wide web-ը (web-ը կամ www) համացանցի միայն մի մասն է, որը հասանելի է օգտատերերին բրաուզերի միջոցով: Այն կազմված է վեբ էջերի հսկայական հավաքածուից և հիմնվել է հիպերտեքստային փոխանցման արձանագրության վրա (http)՝ սկսած 1989 թվականից: World wide web-ը համացանցով ինֆորմացիայի հասանելիության միջոց է, «www» և «համացանց» տերմինները նույնը չեն և չպետք է դրանք շփոթել:

10.1.3 Էլեկտրոնային հասցեների խմբերը

Սրանք օգտագործվում են մի քանի նպատակներով.

- Օգտատերը շատ հեշտությամբ է կարողանում մեծ թվով նամակներ ուղարկել, եթե էլեկտրոնային հասցեները խմբավորված են և մեկ բառով գրված են «to»- ի դիմաց:
- Կազմակերպությունները և խոշոր ընկերությունները խմբավորում են էլեկտրոնային հասցեները մարկետինգային նպատակներով, այսինքն՝ դա կարող է լինել, օրինակ, ըստ տարիքի, էթնիկ պատկանելության, նախասիրությունների, սիրած երաժշտության և այլն: Սա նշանակում է որ յուրաքանչյուր նամակ կհասնի միայն կոնկրետ խմբի մարդկանց:
- Սպամերները խմբավորում են մարդկանց՝ գնելով էլեկտրոնային հասցեների ցուցակներ ընկերություններից, և ընդամենը մի կոճակի սեղմումով կարող են սպամ նամակներ ուղարկել հազարավոր մարդկանց:
- Կազմակերպությունները հաճախ անց են կացնում առցանց հավաքներ ինչ-որ գործի հետ կապված հարցեր քննարկելու համար: Սակայն

բարդությունն այն է, որ մարդկանց առանձին-առանձին հրավիրելը շատ դժվար է, որովհետև շատ հեշտ է մոռանալ, թե ում ես հրավիրել, ում՝ ոչ: Իսկ ստեղծելով էլեկտրոնային հասցեների խումբ՝ կարող ենք կատարել այս աշխատանքը շատ հեշտ, քանի որ ստիպված չենք լինի հիշել բոլոր մարդկանց էլեկտրոնային հասցեները:

10.2 Համացանցի էֆեկտիվ օգտագործումը

10.2.1 Համացանցը

Համացանցը՝ ինչպես անունն է ասում, համաշխարհային մակարդակով ցանցերի հավաքածու է, որը թույլ է տալիս.

- ուղարկել և ստանալ էլեկտրոնային նամակներ,
- հաղորդակցվել առցանց (տեքստերով, ձայնային և տեսահաղորդագրություններով),
- փոխանցել \$այլեր մեկ համակարգչից մյուսին՝ օգտագործելով \$այլի փոխանցման նախնական համաձայնությունը,
- առցանց տարածել աշխարհով մեկ:

Հայտնի է որ 2015 թվականին արդեն 3 միլիարդ մարդ օգտվում էր համացանցից: Ինտերնետը ինչ-որ մեկ անձի կամ կազմակերպության չի պատկանում, այն ավելի շատ հասկացություն է, քան ինչ-որ շոշափելի առարկա: Այն հենվում է ֆիզիկական ենթակառուցվածքների վրա : Համաշխարհային www (World Wide Web) ցանցը կազմում է համացանցի միայն մի մասը, որը մեզ հասանելի է դառնում բրաուզերների օգնությամբ: Այն կազմված է առեղծված քանակությամբ կայքէջերից և հիմնված է հիպերտեքստի փոխանցման արձանագրության (Hypertext Transfer Protocol – http) վրա 1989 թվականից: Համաշխարհային ցանցը ինֆորմացիա ստանալու միջոց է այն միջավայրում, որը կոչվում է համացանց: Այս երկու տերմինները՝ համաշխարհային ցանցը և համացանցը, նույն իմաստը չեն կրում և դրանք չպետք է շփոթել:

10.2.2 Ինտրանետ

Շատ կազմակերպություններ, ինտերնետից օգտվելուց բացի, օգտագործում են նաև ինտրանետը: Ի տարբերություն ինտերնետի, այն հասանելի չէ հանրությանը, այլ հասանելի է միայն կազմակերպությանը: Դրանք պաշտպանված են firewall-ով և միայն հասանելի են՝

- կազմակերպության աշխատողներին՝ ներսի մարդկանց,
- կազմակերպությունից դուրս, բայց որոշակի մակարդակով հասանելիություն ունեցող մարդկանց:

Կան մի քանի պատճառներ ինտրանետը համացանցից գերադասելու համար.

- ինտրանետը ավելի ապահով է վիրուսներից և հաքերային հարձակումներից,
- ավելի հեշտ է կանխել արտաքին հղումները՝ ուղղված որոշ կայքէջերի,
- կազմակերպությունը կարող է համոզվել, որ առկա ինֆորմացիան, հատուկ է իրենց կարիքներին,:
- հեշտությամբ կարելի է ուղարկել հաղորդագրություն՝ իմանալով որ այն հասանելի է միայն կազմակերպության ներսում,
- ինտրանետի թողունակությունը ավելի բարձր է, քան համացանցինը, կապի առումով չկան սահմանափակումներ, այսինքն՝ մեկ վայրկյանում փոխանցված բիթերի քանակը ավելի շատ է ինտրանետի դեպքում,
- Նաև էքստրանետներ ստեղծելու հնարավորություն կա ինտրանետը որոշ չափով կազմակերպությունից դուրս հասանելի դարձնելու համար, սա պետք է գալիս, օրինակ, համագործակցող ընկերություններին :

Որո՞նք են ինտերնետի և ինտրանետի տարբերությունները

- Համացանցը՝ ինտերնետը (**Internet- International network**) և ինտրանետը (**Intranet- Internal Network**), ինչպես տեսանք, ունեն ծագումնաբանության և նշանակության տարբերություն:
- Ինտրանետն օգտագործվում է ինֆորմացիան միայն մեկ կոնկրետ կազմակերպության ներսում տարածելու համար, իսկ ինտերնետը տարածում է ինֆորմացիան աշխարհով մեկ:
- Ինտրանետում որոշ կայքէջեր մուտք գործելը արգելելը շատ ավելի հեշտ է, քան ինտերնետում:
- Ինտրանետին հասանելի լինելը պայմանավորված է գաղտնաբառ իմանալով և ID ունենալով կամ թույլտվություն ունեցող համակարգչից օգտվելով, սակայն ինտերնետը հասանելի է աշխարհի յուրաքանչյուր անկյունում, եթե օգտվողը ունի ISP հաշիվ:
- Ինտրանետը որոշակիորեն պաշտպանված է վիրուսներից և հաքերային հարձակումներից firewall-ի օգնությամբ, սակայն ինտերնետը՝ ոչ, քանի որ հասանելի է բոլորին:
- Ինտերնետը հասանելի է ամբողջ հասարակությանը, իսկ ինտրանետը ավելի փակ շրջանի մարդկանց օգտագործման համար է: