Բաց դաս

Առարկան՝ ինֆորմատիկա

Թեման՝ Ապահով համացանց

Նպատակը՝ համացանցից ապահով օգտվելու հմտությունների ձեռքբերում, համացանցի անսահմանափակ հնարավորությունները արդյունավետ կիրառելու կարողությունների զարգացում, կատարած աշխատանքների համար պատասխանատվության խորացում:

Խնդիրները՝

1) կրթական- աշակերտներին սովորեցնել տրամաբանել, կարողանալ վերլուծել և համակարգել ստացած գիտելիքները, ծանոթացնել համացանցում աշխատելու անվտանգության կանոններին:

2) Զարգացնող-զարգացնել ստեղծագործական մտածելակերպը, բանավոր խոսքը:

3) Դաստիարակչական - համացանցում աշխատելիս պահպանել էթիկայի կանոնները:

Մեթոդը՝ կիրառել ինտերակտիվ մեթոդներից 'խմբային հետազոտություն' մեթոդը, կազմակերպել քննարկում, գնահատում:

Դասի փուլերը՝

I խթանման փուլ- կազմակերպչական մաս- դասի թեմայի, նպատակների և խնդիրների հայտնում, «մաթեմատիկական թելադրություն» ինտերնետ թեմայից:

II Իմաստի ընկալման փուլ- կատարված աշխատանքի ներկայացում,

III Կշռադատման փուլ- 1) անդրադարձ, 2)գնահատում, 3)տնային հանձնարարության :

Դասի ընթացքը՝

կազմակերպչական մաս / աշակերտների հաճախումը/ , դասի թեմայի, նպատակների և խնդիրների հայտնում: *(2րոպե)*

Անցկացնել «մաթեմատիկական թելադրություն» ինտերնետ թեմայից: Այն կստուգի աշակերտների գիտելիքները: Առավելագույն միավորը՝ 5:

1. Համակարգչային գլոբալ ցանց, որը միավորում է լոկալ, տարածաշրջանային և կորպորատիվ բազմաթիվ ցանցեր:

ա/google chrom, բ/ ինտերնետ, գ/yandex,

2. Համակարգիչը ցանցին միացնող սարք.

ա/մոդեմ, բ/ մկնիկ, գ/սկաներ,

3. Ինֆորմացիա փոխանակելու կապուղու օրինակ է.

ա/ցանցային արձանագրությունը, բ/հեռախոսային ցանցը, գ/ համացանցը,

4. Կրթությանը վերաբերող դոմեն է.

ա/org, բ/com գ/edu,

5. Հիպերտեքստերի էջերի դիտման ծրագիր է.

ա/բրաուզերը, բ/ սերվերը, գ/ համակարգիչը:

Ստուգել պատասխանները, կատարել ուսուցանող գնահատում (*Յրոպէ*)

Կատարված աշխատանքի ներկայացում: Դասարանը նախօրոք բաժանվել է 4 խմբի, յուրաքնչյուրում՝ 5 աշակերտ: Նրանք ներկայացնում են իրենց պատրաստած սահիկաշարերը հետևյալ թեմաներով՝

1/ Համացանց- հնարավորությունները, վտանգները

1. Համացանցը համակարգչային ցանցերի միավորում է, համաշխարհային գլոբալ համակարգ, որը ինֆորմացիայի փոխանակումը ապահովում է տեղեկատվական տեխնոլոգիաների օգնությամբ:
2. Համացանցում հանդիպող վտանգները՝
   վիրուսակիր վտանգավոր ծրագրեր,
   տեղեկատվության գողություն,
   հակերների հարձակում,
   աշխատակիցների կամայականություն,
   ֆինանսական մեքենայություններ,
   սպամ,
   տեխնիկական և ծրագրային խափանումներ:

2/ Համակրգչային վիրուսներ, վտանգավոր ծրագրեր, կայքեր.

1. Համակարգչային վիրուսները տարբեր համակարգչային ծրագրեր են կամ վնասակար կոդեր, որոնք հիմնականում օժտված են ինքնաբազմացմամբ:
2. Ներկա պահին գոյություն չունի վիրուսների դասակարգման միասնական համակարգ: Ընդունված է դրանք առանձնացնել հետևյալ խմբերում՝

Ըստ վնասված օբյեկտների՝

Ֆայլային վիրուսներ-Այս վիրուսները պարազիտներ են, որոնք իրենց պատճենները տարածելիս փոխում են գործարկված ֆայլի բովանդակությունը, ընդ որում հիմնականում վիրուսակիր ֆայլը ամբողջովին կամ մասնակի կորցնում է իր աշխատունակությունը:

Բեռնավորվող վիրուսներ-Դրանք տեղակայվում են համակրգչի կոշտ կամ ճկուն սկավառակի վրա և գործարկվում են օպերացիոն համակարգի բեռնավորման ժամանակ:

Սկրիպտային վիրուսներ-պահանջում են որևէ սկրիպտային լեզու(Javascript, VBScript), որ կարողանան ինքնուրույն մուտք գործել տեղեկատվական սկրիպտներ:

Մակրովիրուսներ- մակրոլեզուներով գրված վիրուսներ են, որոնք ընդգրկված են այնպիսի փաթեթներում, ինչպիսին է Microsoft office-ը:

Ըստ վնասված օպերացիոն համակարգի և պլատֆորմի՝

–DOS, -Microsoft Windows, -Unix, - Linux

Տեխնոլոգիաներ, որոնք վիրուսակիր են

Պոլիմորֆ վիրուսներ- վիրուսներ են, որոնք ֆայլերի կամ դիսկի համակարգային տիրույթներ վարակելիս տեղադրում են իրենց անհատական կոդը:

Ստելս-վիրուսներ

1. Դրանք, մասնակի կամ ամբողջովին թաքցնելով իրենց ներկայությունը համակարգում, օպերացիոն համակարգի բեռնավորման ժամանակ գրոհում են նրա վրա:
2. Այն լեզվի հիման վրա, որով գրված է վիրուսը, դրանցից են՝
   Asembler, բարձր կարգի ծրագրավորման լեզուներ, սկրիպտային լեզուներ և այլն:

Լրացուցիչ վտանգավոր ֆունկցիոնալությամբ օժտված՝

Բեկդորներ ծրագիր է, որը տեղադրվում է այն համակարգչի վրա, որի սկզբնական տվյալները ցանցին միացնելիս վերցվել են այն նպատակով, որ նորից միանան նրան:

Կեյլոգերներ մոդուլներ են, որոնք նախատեսված են ստեղնաշարի ստեղնը սեղմելիս վիրուսը միացնելու համար:

Շպիոններ Spyware ծրագրային ապահովում է, որը համակարգչի կոնֆիգուրացիայի մասին տեղեկություն է հավաքում առանց օգտագործողի համաձայնության:

Բոտնետեր Համակարգչային ցանց է, որը բաղկացած է մի քանի «խոստերից» , որոնք բոտերի կողմից թողարկված ինքնավար ծրագրային ապահովմամբ անհատական համակարգիչներ են՝ միացված ինտերնետ ցանցին: Ընդհանրապես օգտագործում են անլեգալ և չթույլատրվող գործունեություն ծավալում, սպամ են ուղարկում, գաղտնաբառեր են գողանում:

3/ Ինչպես պայքարել այդ վտանգների դեմ

1. **Տեղադրել պաշտպանության կոմպլեքս համակարգ**
   Հակավիրուսի տեղադրումը անցյալ է, հարկավոր է տեղադրել պաշտպանության կոմպլեքս համակարգ , որն իր մեջ ներառում է հակավիրուս, ֆայրվոլ, հակասպամ, ֆիլտրեր և ևս մի քանի մոդուլներ պաշտպանության համար: Յուրաքանչյուր օր նոր վիրուսներ են հայտնվում , դրա համար հարկավոր է անընդհատ թարմացնել հակավիրուսը կամ դնել ավտոմատ թարմացման ռեժիմում:

2. **Զգու՛յշ եղեք էլեկտրոնային փոստի հետ**
   Կարևոր ինֆորմացիան պետք չէ ուղարկել էլեկտրոնային փոստով, տեղադրել արգելք էլ. փոստը բացելու վրա, քանի որ շատ վիրուսներ գտնվում են ներդրված ֆայլերի մեջ:

3. **Windows օպերացիոն համակարգը թարմացնել**
   Նոր տարբերակները նոր հնարավորություններ են տալիս վիրուսների հարձակումներից պաշտպանվելու համար:

4. Հանդիպում են կայքեր, որոնք փակում են ձեր էջը և բացելու համար պահանջում են SMS հաղորդագրություններ ուղարկել, դա ձեզանից կխլի որոշակի գումար և դեռ վիրուս էլ կուղարկի:

5. **Օգտվե՛ք լիցենզավորված ծրագրերից:** Որքն հայտնի է ծրագիրը, այնքան հավանական է, որ այն վիրուսակիր է:

6. **Օգտագործե՛ք «բրանդմաուէր»**-դրանք թույլ չեն տալիս , որ համակարգիչ մուտք գործեն «որդեր», վիրուսներ, վտանգավոր ծրագրեր:

7. **Օգտագործե՛ք բարդ գաղտնաբառեր:** Ծածկագրերի 80%-ը պարզ են: Լավ կլինի՝ դրանք պարունակեն 7-12 սիմվոլ: 5 սիմվոլից բաղկացած ծածկագիրը կարելի է բացել 2-4 ժամում, իսկ 7 սիմվոլից բաղկացած ծածկագիրը հնարավոր է բացել 2-4 տարում: Լավ կլինի օգտագործել տարբեր ռեգիստորների տառեր, թվեր, նշաններ:

8. **Կատարո՛ւեք լրացուցիչ պատճեններ**: Պատճենները պահեք արտաքին կրիչների վրա:

Դադար, աչքերի վարժանք (*2րոպե*)

4/ Հայաստանի Հանրապետությունում ի՞նչ օրենքներով ենք մենք պաշտպանվում

Ինտերնետ համացանցի զարգացումն իր հետ բերեց կիբերհանցավորության դրսևորումների որակապես նոր փուլ: Տարբեր ինտերնետային չարագործներ սկսեցին ստեղծել և տարածել վիրուսների տարատեսակներ՝ «որդեր-Worm», որոնք վարակում և գաղտնի հասանելիություն էին ապահովում «կոտրված» համակարգչին: Նմանանատիպ համակարգիչները կարող են միացվել միասնական ցանցի մեջ և դառնալ «բոտնետներ», ինչը հնարավորություն է տալիս չարագործներին կազմակերպել կիբերհարձակումներ / DDoS/ տիպի կազմակերպությունների կամ հետաքրքրող համակարգչային ցանցերի վրա, արժեքավոր տեղեկատվություն ստանալու նպատակով:

ՀՀ քրեական օրենսգրքի 24-րդ գլուխը պատիժ է սահմանում այն բոլոր տեսակի հանցագործությունների համար, որոնցով կարող է վտանգվել տեղեկատվական համակարգերի անվտանգությունը: Մասնավորապես, տվյալ գլխում նկարագրված հանցագործության տեսակները, որոնց համար սահմանված է պատժաչափեր, հետևյալն են՝ Հոդված 251. Համակարգչային տեղեկատվության համակարգ առանց թույլտվության մուտք գործելը (ներթափանցելը),

Հոդված 252. Համակարգչային տեղեկատվությունը փոփոխելը,

Հոդված 253. Համակարգչային սաբոտաժը,

Հոդված 254. Համակարգչային տեղեկատվությանն ապօրինի տիրանալը,

Հոդված 255. Համակարգչային տեղեկատվություն ապօրինի մուտք գործելու (ներթափանցելու) համար հատուկ միջոցներ պատրաստելը կամ իրացնելը,

Հոդված 256. Վնասաբեր ծրագրեր մշակելը, օգտագործելը և տարածելը,

Հոդված 257. Համակարգչային համակարգը կամ ցանցը շահագործելու կանոնները խախտելը:

Այս հոդվածներում նկարագրված հանցակազմերը առավելագույնս ներառել են իրենց մեջ համակարգչային տեղեկատվության դեմ կատարվող հանցագործությունների տեսակները, սակայն չի կարելի մոռանալ տեխնիկական առաջընթացի սրընթաց տեմպերի մասին, այդ իսկ պատճառով օրենսդիրի և իրավակիրառի կապը անչափ կարևոր է տվյալ տեսակի հանցագործությունների արդյունավետ բացահայտման համար: Այս ամենին զուգընթաց՝ կարևորվում են միջազգային համագործակցությունը, քանի որ կիբերհանցագործությունների վերջին տարիների զարգացման միտումների ուսումնասիրությունները ցույց են տալիս, որ տարեցտարի ավելանում են անդրսահմանային բնույթ կրող հանցատեսակները: Այսպես՝ համակարգչային հարձակում կազմակերպող չարագործը կարող է գտնվել որևէ եվրոպական երկրում, օգտագործել որևէ ասիական երկրում վարակված համակարգիչների խումբ և գրոհ կազմակերպել լատինաամերիկյան որևէ պետությունում գտնվող իրեն հետաքրքրող համակարգչային համակարգի վրա, որի արդյունքում հնարավոր կլինի հափշտակել գումարներ չորրորդ երկրում գտնվող բանկից: Նմանատիպ հանցատեսակները վերջին տարիներին լայն տարածում են ստացել ամբողջ աշխարհում: Վերը նշվածին հարկ է ավելացնել նաև ՀՀ

քրեական օրենսգրքի հետևյալ հոդվածները, որոնք առավել հաճախակի կատարվում են համակարգչային տեղեկատվական համակարգերի օգնությամբ:

Հոդված 181. Հափշտակությունը, որը կատարվել է համակարգչային տեխնիկայի օգտագործմամբ,

Հոդված 144. Անձնական կամ ընտանեկան կյանքի մասին տեղեկություններ ապօրինի հավաքելը, պահելը, օգտագործելը կամ տարածելը ,

Հոդված 137. Սպանության, առողջությանը ծանր վնաս պատճառելու կամ գույք ոչնչացնելու սպառնալիքը,

Հոդված 140. Սեքսուալ բնույթի գործողությունների հարկադրելը, ինչպես նաև այլ հոդվածներ:

Կիբերհանցագործությունը սահմաններ չի ճանաչում, այն պետք է պաշտպանվի միջազգային օրենքներով:

5/ Անվտանգության ի՞նչ կանոններ պահպանել համացանցից օգտվելիս:

I կանոն Ցանկալի չէ անձնական ինֆորմացիան տեղադրել համացանցում:

II կանոն Չպատասխանել էլեկտրոնային փոստով եկող անծանոթ նամակներին:

III կանոն Եթե դուք հրապարակում եք Ձեր նամակները կամ տեսաֆիլմը, հիշե՛ք, որ այն կարող է օգտագործել յուրաքանչյուր ոք իր նպատակների համար:

IV կանոն Անծանոթների հետ ընկերություն մի՛ հաստատեք տարբեր սոցիալական կայքերում:

V կանոն Օգտագործե՛ք գաղտնաբառեր, որոնք կպարունակեն և' թվեր, և' տառեր, և' սիմվոլներ:

VI կանոն Համակարգչի հետ աշխատանքը կանոնակարգե՛ք:

VII կանոն Օգտագործե՛ք լիցենզիոն ծրագրեր, հակավիրուսային ծրագրեր, որոնք էլ ժամանակին թարմացրեք:

VIII կանոն Մի՛ պահպաներ Ձեր գաղտնաբառը այն համակարգիչների վրա,որոնցից շատ մարդիկ են օգտվում: Գաղտնի ինֆորմացիան մի՛ պահպանեք ուսումնական կենտրոններում, աշխատավայրի համակարգիչներում:

IX կանոն Միայնակ մի' հանդիպեք այն մարդկանց հետ, ում հետ ծանոթացել եք ինտերնետով:

X կանոն Մի՛ բացեք անծանոթներից ստացված ֆայլերը:

XI կանոն Հաղորդակցվելիս պահպանե՛ք ցանցից օգտվելու էթիկայի կանոնները:

XII կանոն Վեբ-տեսախցիկը օգտագործելիս հետևեք, որ օտար մարդիկ չտեսնեն, կամ չլսեն այն, քանի որ կարող են ձայնագրել և օգտագործել տարբեր նպատակներով:

(*20րոպե*)

Ցուցադրում են պատրաստած պաստառները համապատասխան թեմաներով: (*5րոպե*)

Անդրադարձ՝

Յուրաքանչյուր խումբ ներկայացնում է նախապես պատրաստած երեք հարց իրենց պատրաստած թեմայի շուրջ՝ մյուս խմբերին գնահատելու համար:

Կարդում են հարցերը, լսում պատասխանները: (*3րոպե*)

Կատարում են ինքնագնահատում՝ օգտագործելով գունավոր քարտեր, որոնք դրված են սեղաններին: Թեման լավ յուրացնելու դեպքում բարձրացնել կարմիր քարտեր, միջինի դեպքում՝ դեղին, վատ յուրացնելու դեպքում՝ կանաչ: (*2րոպե*)

Ուսուցիչը կատարում է աշակերտների գնահատում՝ ըստ չափորոշչային պահանջների Ա, Բ, Գ մակարդակները ներկայացնող գնահատման ռուբրիկի:

Գնահատման ռուբրիկ		
Ա մակարդակի պահանջներ	Բ մակարդակի պահանջներ	Գ մակարդակի պահանջներ
Կարողանալ թվարկել ցանցերի կառուցման համար անհրաժեշտ սարքավորումները: Կարողանալ օգտվել ինտերնետում որոնման տարբեր համակարգերից: Կարողանալ ինքնուրույն օգտվել էլեկտրոնային փոստից:	Ճանաչել ինտերնետային որոնման տարածված համակարգերը, կարողանալ օգտվել դրանցից: Կարողանալ ստեղծել էլեկտրոնային փոստի հասցեներ տարբեր կայքերում: Իմանալ ինտերնետի ընձեռած հիմնական հնարավորությունների մասին: Իմանալ հակավիրուսային ծրագրերի մասին:	Իմանալ ինտերնետային տարբեր զննիչ ծրագրեր, կարողանալ օգտվել դրանցից: Իմանալ և կիրառել ցանցային էթիկայի կանոնները:
		Աշակերտները ավելացնում են՝ իմանալ վտանգավոր ծրագրերի, «շպիոնների», մոդուլների, կայքերի մասին, դրանցից պաշտպանվելու հնարների մասին: Իմանալ օրենքներ համակարգչային հանցագործությունների վերաբերյալ:
4-5 միավոր	6-7 միավոր	8-10 միավոր

Գնահատվում են աշակերտները ուսուցչի կողմից, (*2րոպե*)

Այսպիսով՝ մենք իմացանք, որ համացանցը հաճելի է և օգտակար սովորելու, հանգստանալու, ընկերների հետ շփվելու համար, բայց ինչպես և իրական կյանքը, այն կարող է լինել վտանգավոր:

Այսօրվա դասի ընթացքում մենք իմացանք, թե ինչ վտանգներ են մեզ սպառնում համացանցում, ինչպես փորձենք պաշտպանվել դրանցից, պետականորեն ինչպես ենք պաշտպանված, ինչ կանոններ պահպանել ինտերնետից օգտվելիս հնարավոր վտանգներից պաշտպանվելու համար: (*1րոպե*)

Տնային հանձնարարություն՝ գրել շարադրություն «Տեղեկատվական տեխնոլոգիաները իմ կյանքում» թեմայով: (*1րոպե*)

6/ Դիտել տեսանյութ «Ապահով համացանց» թեմայի շուրջ: (*4րոպե*)

Մի՛ դարձրեք կուռք տեխնիկական միջոցները,
Մի՛ պահեք դրանք շատ մոտ ձեր մարմնին,
Մի՛ հավատացեք նրանց անմեղությանը,
Մի՛ քիչ էլ հոգացեք ձեր առողջության համար:

Վաղարշապատի Մ. Գորկու անվան հմ.5 ավագ դպրոց

Ուսուցիչ՝ Ա. Գրիգորյան