ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ
ԿՐԹՈՒԹՅԱՆ, ԳԻՏՈՒԹՅԱՆ,
ՄՇԱԿՈՒՅԹԻ ԵՎ ՍՊՈՐՏԻ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

ՀՀ ԿԳՄՍՆ «ԵՐԵՎԱՆԻ ԼԵՈՆԻ
ԱՆՎԱՆ
Հ. 65 ԱՎԱԳ ԴՊՐՈՑ» ՊՈԱԿ

ՀԵՐԹԱԿԱՆ ԱՏԵՍՏԱՎՈՐՄԱՆ ԵՆԹԱԿԱ ՈՒՍՈՒՑԻՉՆԵՐԻ ՎԵՐԱՊԱՏՐԱՍՏՄԱՆ ԴԱՍԸՆԹԱՑԻ

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ

Առարկա՝ Ինֆորմատիկա

Մասնակից՝ Նաիրա Մարտիրոսյան

Թեմա՝ Կիբեռանվտանգությունը դպրոցական կրթության մեջ

Ղեկավար՝ Գայանե Կոստանդյան

ԵՐԵՎԱՆ 2023

Բովանդակություն

Ներածություն

Կիբեռանվտանգությունը աճող մտահոգություն է կրթական հաստատությունների համար: Թեև շատերը կարող են մտածել, որ կիբեռանվտանգության սպառնալիքները միայն առցանց համալսարանների ու հաստատությունների համար են: Ճշմարտությունն այն է, որ բոլորը թիրախ են: Լինի դա դպրոց, պետական համալսարան, կամ առցանց ուսումնական հարթակ, կիբերսպառնալիքները կարող են լուրջ վնաս հասցնել:

Կիբեռանվտանգությունը վերջին տասնյամյակի ընթացքում շատ լուրջ առաջընթաց է ապրել: Տեղեկատվությունը պահելու և փոխանակելու ավելի անվտանգ եղանակներով մենք գնում ենք ճիշտ ուղղությամբ: Այնուամենայնիվ, բավական չէ պարզապես ուսուցիչներին, սովորողներին, ուսանողներին կրթել կիբեռանվտանգության սպառնալիքների վերաբերյալ տեղեկատվությամբ: Պետք է լինեն գործող գործընթացներ և ռազմավարություններ, որպեսզի բոլորն առցանց ապահով մնան:

Փաստ է, որ կորցնելով անձնական տվյալները, ֆինանսներ, նոր սկսում ենք ուսումնասիրել և ձեռք բերել կիբեռգրագիտություն: Կիբեռգրագիտության հասնելու համար պետք է ուսումնասիրել հետևյալ հարցերը՝

1.Ին՞չ է կիբեռանվտանգությունը կրթության մեջ:

2.Ինչու՞ է կիբեռանվտանգությունը կարևոր կրթության մեջ:

3.Ի՞նչ է անվտանգության իրազերկումը կրթության մեջ:

4. Ինչու՞ անվտանգության իրազեկվածությունը բավարար չէ կրթական հաստատությունները կիբեռսպառնալիքներից պաշտպանելու համար:

5.Որո՞նք են կրթության ոլորտում կիբեռանվտանգության լավագույն փորձը:

6. Ինչպե՞ս կարող են կրթական հաստատությունները պատրաստվել կիբեռհարձակմանը:

7. Ո՞րն է տեխնոլոգիայի դերը կիբեռանվտանգության և կրթության մեջ:

Ի՞նչ է կիբեռանվտանգությունը:

Կիբեռանվտանգությունն թվային միջավայրերում զգայուն տվյալները պահպանելու միջոց է: Կրթական հաստատությունները կունենան շատ տարբեր ոլորտներ, որոնք պետք է ապահովեն գաղտնիությունը, երբ խոսքը վերաբերում է այնպիսի տեղեկատվությանը, ինչպիսին է.

- ուսանողների և մանկավարժների անձնական կոնտակտային տվյալներ,
- ֆինանսական տեղեկատվություն և առցանց հաշիվներ, որոնք կարող են օգտագործվել հաստատության կողմից
- ներքին գործառնական տվյալներ/գործընթացներ, որոնք խիստ գաղտնի են և մասնավոր այդ հաստատության համար
- ուսումնական նյութերի կառավարման համար օգտագործվող այլ տվյալներ (հատկապես առաջադրանքների, քննությունների և գնահատման առումով):

Ի հավելումն հաստատություններին հատուկ ոլորտների՝ անձնական տվյալները նույնպես կարող են վտանգված լինել: Եթե որևէ անձնական հաշիվ առցանց օգտագործվում է ուսանողների/ուսուցիչների կողմից, դրանցից կարող են օգտվել նաև չարամիտ ներխուժողները:

Ի՞ՆՉ Է ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ԻՐԱԶԵԿՈՒՄԸ:

Այնուամենայնիվ, երբեմն-երբեմն անվտանգության իրազեկման ուսուցումը միայն առաջին քայլն է կրթության ոլորտում կիբեռանվտանգությունը խթանելու համար: Արդյունավետ անվտանգության համար հաստատությունը պետք է ունենա միջադեպերի պլաններ և ապահովի, որ կազմակերպության յուրաքանչյուր անդամ լրջորեն վերաբերվում է կիբեռանվտանգությանը:

Հիմնական քայլերը, որոնք կարող են անվտանգության իրազեկումը հասցնել հաջորդ մակարդակի.

- Ռիսկերի գնահատում և դրանք բոլոր կողմերին հաղորդելը,
- Տրամադրել ուսուցում յուրաքանչյուր անձի, որպեսզի նրանք հասկանան, թե որն է իրենց հիմնական դերը անվտանգության ապահովման գործում,
- Հաստատությունների ներսում անհրաժեշտ ռեսուրսների ստացում (և ռեսուրսների փոխանակում) (հակավիրուսային ծրագրեր, VPN մուտք և այլն),
- Անվտանգության միջոցառումների վերանայում/թարմացում,
- Միջադեպերի արձագանքման պլանների ստեղծում:

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՍՊԱՌՆԱԼԻՔՆԵՐԸ ԿՐԹՈՒԹՅԱՆ ՄԵՋ

Ուսումնական հաստատություններում կիբերանվտանգության սպառնալիքներն են՝

Հակերություն. Համակարգչային համակարգ/ցանց չարտոնված մուտք, որը հանգեցնում է զգայուն տեղեկատվության գողության կամ համակարգերին վնասելու: Օրինակ, հաքերները կարող են մտնել համալսարանի տվյալների բազա և գողանալ անձնակազմի անձնական տվյալները, որպեսզի մուտք գործեն իրենց անձնական ֆինանսական հաշիվները՝ միջոցներ գողանալու համար:

Ֆիշինգ. Հարձակվողներն օգտագործում են էլ.փոստ, կեղծ վեբ կայքեր կամ նույնիսկ տեքստեր՝ մարդկանց խաբելու համար, որպեսզի բացահայտեն այնպիսի զգայուն տեղեկություններ, ինչպիսիք են գաղտնաբառերը կամ վարկային քարտերի համարները: Կեղծ վճարային հղումները կամ հաշիվ-ապրանքագրերը բիզնեսների և ուսումնական հաստատությունների վրա օգտագործվող ամենատարածված ֆիշինգ հարձակումներից են:

Տվյալների խախտումներ. Գաղտնի տեղեկատվության գողություն, օգտագործում կամ բացահայտում (օրինակ՝ անձնական/ֆինանսական տվյալներ):

Չարամիտ. Վնասակար ծրագրակազմ, որը վնաս է հասցնում հաստատության ցանցին կամ համակարգին: Դրանք ներառում են տրոյաններ, վիրուսներ և փրկագիններ, որոնք վնասում են սարքերը՝ դրանք դարձնելով անօգտագործելի:

MitM-ի հարձակումները. Սրանք «մարդը միջինում» հարձակումներ են, որտեղ հաղորդակցությունները գաղտնալսվում են, և երկու կողմերի միջև ուղարկվող տեղեկատվությունը փոփոխվում է հարձակվողի կողմից:

ԿԻԲԵՌԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԸ ԿՐԹԱԿԱՆ ՀԱՍՏԱՏՈՒԹՅՈՒՆՆԵՐՈՒՄ

Երբ հաստատությունները տեղյակ են կիբեռանվտանգության միջոցառումների իրականացման հնարավոր մարտահրավերների մասին, նրանք կարող են ավելի արդյունավետ պլանավորել, թե ինչպես շրջանցել այդ խոչընդոտները:

Ֆինանսավորման սահմանափակումներ. Ոչ բոլոր հաստատություններն ունեն ռեսուրսների հասանելիություն, որպեսզի կարողանան կիրառել անվտանգության գործիքներ: Սահմանափակ բյուջեն կարող է հանգեցնել ավելի քիչ անվտանգ սերվերների, պորտալների և սարքերի: Այս դեպքում դրսից ֆինանսավորում փնտրելը կարող է լինել այնպիսի տարբերակ, որը պետք է ուսումնասիրեն հաստատությունները:

Տեխնիկական հմտություններ: Ուժեղ կիբեռանվտանգություն ապահովելու համար անհրաժեշտ է փորձաքննության բարձր մակարդակ: Ինքնուրույն որոշ հաստատությունների համար դժվար կլինի հստակ իմանալ, թե ինչպես պետք է ապահովեն իրենց համակարգերը, հետևաբար մասնագետ վարձելը ճանապարհին է:

Մարդկանց կառավարում. Ոչ ոք չի կարող պատասխանատվություն կրել ուրիշի համար: Հիմնական որոշում կայացնողները կարող են կառավարել օգտատերերի վարքագիծը (օրինակ՝ կանոններ ստեղծելու համար, որպեսզի ուսանողներին չկարողանան մուտք գործել սոցիալական մեդիա սարքերով), սակայն այս վարքագծի մշտադիտարկումը դժվար է: Մարդկանց պետք է խրախուսել պաշտպանել իրենց և հավատարիմ մնալ քաղաքականությանը:

Կիբեռվտանգներ. Օրվա վերջում սպառնալիքներն ավելի հաճախակի են դառնում, իսկ հարձակվողները՝ ավելի խելացի: Ահա թե ինչու պոտենցիալ սպառնալիքների մասին տեղյակ մնալը, քանի որ տեխնոլոգիական լանդշաֆտի փոփոխություններն այդքան կարևոր են: Իմանալը, թե ինչ նոր սպառնալիքներ են մտնում առցանց ոլորտ, կօգնի որոշում կայացնողներին ավելի լավ նախապատրաստել իրենց միջավայրը և կանխել որևէ լուրջ վնասի առաջացումը:

ԻՆՉՊԵՍ ԳՈՐԾԻ ԴՆԵԼ ԿԻԲԵՐԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԱՍԻՆ ԻՐԱԶԵԿՈՒԹՅՈՒՆԸ

Հետևյալը հակիրճ ուղեցույց է, որը կօգնի ապահովել ամուր կիբեռանվտանգություն ցանկացած ուսումնական հաստատության համար, որը դուրս է գալիս միայն կիբեռանվտանգության իրազեկման ուսուցում տրամադրելուց:

- **Ռիսկի գնահատումը**

Կիբեռանվտանգության ռիսկերի գնահատման բազմաթիվ եղանակներ կան: Այս ոլորտում մասնագիտացած խորհրդատուի ներգրավումը չափազանց արժեքավոր կլինի: Այն հաստատությունների համար, որոնք չունեն այս բյուջեն, ռիսկերի գնահատումը պետք է ներառի բոլոր ոլորտների ուսումնասիրությունը, որոնք կարող են խոցելի լինել շահագործման համար:

- **Ռազմավարություն և ուսուցում**

Հաստատությունները պետք է ուրվագծեն անվտանգության պլանը՝ հիմնվելով գնահատման ընթացքում բացահայտված հնարավոր ռիսկերի վրա: Նրանց համար, ովքեր ունեն կիբեռանվտանգության խորհրդատու ներգրավելու բյուջե՝ ռազմավարություն ստեղծելու համար, դա իդեալական կլիներ: Եթե երրորդ կողմը կատարեր ռիսկի գնահատումը, նրանք կարող էին նաև պլան ստեղծել հաստատության համար: Նրանց համար, ովքեր չունեն մուտք դեպի խորհրդատուներ, ռազմավարությունը նախանշում է.

- Հիմնական որոշումներ կայացնողների դերերն ու պարտականությունները
- Պարտականություններ մեծ համայնքի համար (ուսանողներ և անձնակազմ)
- Ինչպես է իրականացվելու պլանի յուրաքանչյուր փուլ, երբ և ում կողմից
- Թիմի յուրաքանչյուր հիմնական անդամի կոնտակտային տվյալները
- Ռեսուրսներ, որոնք կօգտագործվեն (ստորև նշված գործիքները):

Կարող եք նաև զննել համացանցը՝ կիբեռանվտանգության ծրագրերի և ռազմավարությունների մի քանի անվճար ձևանմուշների համար՝ ավելի լավ պատկերացում կազմելու համար, թե ինչպես ստեղծել դրանք:

Վերապատրաստման ասպեկտը, ըստ էության, վերաբերում է այն տեղեկատվության և ռեսուրսներին, որոնց յուրաքանչյուր անդամ պետք է հասանելի լինի ծրագրի իրականացման համար: Ո՞վ է վերապատրաստելու անձնակազմին, և ինչպե՞ս է նրանք պետք վերապատրաստվեն: Իսկ ի՞նչ կասեք ուսանողների մասին: Ինչի՞ց են պետք նրանց կրթություն ստանալու համար: Օնլայն ձեռնարկները, անհատական դասընթացները և ամբողջական հաստատության հանդիպումներն ու սեմինարները վերապատրաստման տարբերակներ են:

- **Տրամադրել ռեսուրսներ**

Որոշումներ կայացնողները պետք է անդրադառնան իրենց ռիսկերի գնահատմանը և ռազմավարությանը, որպեսզի ընտրեն, թե որ ռեսուրսները պետք է օգտագործվեն և համօգտագործվեն: Որոշ ռեսուրսներ և գործիքներ կպահանջեն միայն մեկանգամյա ներբեռնում և վճարում, մինչդեռ մյուսները կարող են հիմնված լինել բաժանորդագրության վրա, իսկ որոշները կարող են լինել անվճար:

Պետք է նաև հաշվի առնել այն փաստը, որ անձնակազմին սովորաբար անհրաժեշտ են տարբեր անվտանգության գործիքներ, որոնք կարող են օգտագործել ուսանողները: Այս ամենը պետք է մանրամասնված լինի պլանում:

Ահա անվտանգության միջոցառումներից ընդամենը մի քանիսը, որոնցում ցանկացած ուսումնական հաստատություն պետք է ներդնի, եթե դեռ չի արել.

- Հակավիրուսային ծրագրեր
- Գաղտնաբառերի կառավարիչներ և կոդավորման գործիքներ
- Մուտք գործելու համար վավերացուցիչներ
- VPN կազմակերպության սարքերի համար, ներառյալ VPN բջջային հեռախոսների համար

Ավելի երիտասարդ ուսանողների համար, ովքեր ցանկանում են ավելին իմանալ կիբերանվտանգության մասին և նույնիսկ հետաքրքրություն ցուցաբերել ապագայում այս ոլորտում զարգացնելու հարցում, Կիբեր որոնումներ ինտերակտիվ առցանց հավելված է, որն ուղղված է կիբերանվտանգության կրթությանը:

- Թարմացրեք անվտանգության պլանները

Վերջապես, անվտանգության ռազմավարությունը միշտ պետք է հարմարեցվի ընթացիկ սպառնալիքներին և կիբեռանվտանգության ցանկացած նորամուծություններին: Եթե նոր տեխնոլոգիան կարող է փոխարինել ուրիշներին, թարմացրեք միջոցները և վերակրթեք այն մարդկանց, ովքեր պետք է օգտագործեն այս տեխնոլոգիան: Ծրագիրը երբեք չպետք է լճանա և պետք է պարբերաբար վերագնահատվի և ճշգրտվի: Ի վերջո, երբ խոսքը վերաբերում է կիբեր աշխարհին, ամեն ինչ արագ է փոխվում:

Ձեր կիբեռանվտանգության ռազմավարության ստեղծման և թարմացման մի մասն է որակյալ միջադեպերի արձագանքման պլան ունենալը՝ մանրամասն ընթացակարգ, երբ հարձակումները տեղի են ունենում: Այստեղ պետք է նշվի, թե ում հետ պետք է կապ հաստատել, ինչպես և ինչ միջոցներ պետք է ձեռնարկել տվյալների ապահովման և սպառնալիքի վերացման համար:

- **Կիբեռանվտանգությունը կարևոր է**

Կրթական հաստատությունները պաշտպանված չեն կիբեր սպառնալիքներից: Անհրաժեշտ է ոչ միայն իմանալ, թե որոնք են վտանգները, այլ նաև ինչպես մեղմել դրանք և կառավարել դրանք, երբ դրանք տեղի ունենան: Իրազեկությունը մեզ միայն հեռու է տանում, այնուհետև գալիս է գործողությունը:

Տեխնոլոգիական գործիքների, ռեսուրսների, ուսուցման, ռազմավարության և, ի վերջո, թիմային աշխատանքի մեջ ներդրումներ կատարելը կարող է հաստատություններին դարձնել անթափանց և ավելի վստահ, որ իրենց զգայուն տեղեկատվությունը ապահով է:

Կիբեռբուլինգը թվային հաղորդակցության գործիքների (բջջային հեռախոս, պլանշետ, համակարգիչ, համացանց և այլն) օգտագործումն է անձին կամ մի խումբ անձնանց նվաստացնելու, վիրավորելու, հետապնդելու, ոտնձգելու, էմոցիոնալ և հոգեբանական ճնշման ենթարկելու, սպառնալու կամ ահաբեկելու համար՝ պատճառելով տառապանք, բարկություն վախ և/կամ վնաս: Կիբերբուլինգը կարող է ներառել անձի մասին կեղծ տեղեկատվության տարածումը կամ նրանց կամքին հակառակ նրանց անձական տվյալների հանրայնացումը:

Դեռահասը կարող է կիբեռբուլինգի զոհ լինել, եթե նրա վարքագծում նկատելի են անսպասելի, տարօրինակ փոփոխություններ.

- Հանկարծ դադարում է հեռախոսից, համակարգչից, սոցիալական կայքերից օգտվել կամ անհանգստություն է դրսևորում օգտվելու ընթացքում:
- Բարկանում է, վհատված է, նկատելի են դեպրեսիայի նշաններ կամ ինքնամփոփ է դառնում մեսինջերից, չատից կամ սոցիալական կայքից օգտվելուց հետո:
- Կորցում է դասի կամ դուրս գնալու նկատմամբ հետաքրքրությունը:
- Հրաժարվում է խոսել, մանավանդ՝ առցանց գործունեությունից:

Դեռահասը կարող է կիբերբուլինգ լինել, եթե նա՝

- Հանկարծ անջատում է համակարգչի մոնիտորը կամ թաքցնում հեռախոսը/պլանշետը:
- Օգտագործում է համակարգիչը/ հեռախոսը/ պլանշետը գիշերվա ընթացքում:
- Բորբոքվում է, երբ չի կարողանում օգտվել համակարգչից/ հեռախոսից/ պլանշետից ինչ որ պատճառով:
- Հրաժարվում է քննարկել առցանց գործունեությունը:
- Ստեղծում և օգտագործում է սոցիալական կայքերի մի քանի հաշիվներ կամ օգտագործում է այլ անձի ինքնությունը:

Պետությունը պետք է արդյունավետ ռազմավարություն մշակի կիբեռբուլինգի դեմ եւ ստեղծի կամ սահմանի ինտերնետային տեխնոլոգիաների անվտանգ օգտագործման համար պատասխանատու մարմին: Ոչ պակաս կարեւոր է ծնողների ու դպրոցի դերը կիբեռբուլինգի դեմ պայքարում:

Ծնողների դերը. Հաճախ ծնողները կարծում են, որ երեխային համացանցից օգտվել արգելելը և խիստ հսկողությունը կարող են լուծում և կանխարգելող միջոց լինել:

Իրականում հնարավոր և արդարացված չէ ժամանակակից դեռահասներին համացանցից հեռու պահել կամ վերահսկել 24 ժամ: Այս խնդրի լավագույն լուծումը ծնող-երեխա հարաբերություններում բաց հաղորդակցության և վստահության մթնոլորտի ստեղծումն

է: Ծնողն ավելի լավ կհասկանա երեխայի խնդիրները, եթե երեխան անկեղծ պատմի իր առցանց հաղորդակցությունների մասին:

Ծնողներն, իրենց հերթին, պետք է անեն առավելագույնը երեխայի հետ հաղորդակցվելու, նրան լսելու և անվերապահ սեր և աջակցություն ցուցաբերելու համար ժամանակ գտնելու համար: Դեռահասը պետք է միշտ հիշի, որ ծնողը կօգնի և չի վատթարացնի իրավիճակը: Եթե երեխայի ֆիզիկական անվտանգությունը տեսանելիորեն վտանգված է, երեխայի համաձայնությամբ ծնողը ահազանգում է ոստինակություն անվտանգության համապատասխան միջոցառումներ պահանջելու համար:

ԱՌՑԱՆՑ ԽԱՂԵՐԸ և ԿԻԲԵՐԲՈՒԼԻՆԳԻ ՎՏԱՆԳՆԵՐԸ

Ժամանակակից դեռահասների 72%-ը խաղում է առցանց խաղեր: Տեսախաղերի մեծ մասը հնարավորություն են տալիս խաղալ ընկերների և անծանոթների հետ՝ միաժամանակ առցանց զրուցելով: Առցանց խաղերն ունեն առավելություններ, ինչպես նաև թերություններ: Առցանց խաղերի դրական կողմը զվարճանքն է, նոր ընկերներ ձեռքբերելը, սոցիալիզացիան, ռազմավարական մտածողության և խնդիրների լուծման հմտությունների զարգացումը: Բացասական կողմերն են կախվածությունը, ժամանակի զգացողության կորուստը, հավանականությունը, որ տեսախաղը կարող է դառնալ կիբերբուլինգի աղբյուր/ դաշտ և այլն: Տեսախաղի օգտատերը կարող է լինել անանուն, գրանցվել դեռահասի այլընտրանքային «երևակայական հերոսի» տեսքով ներկայացող ալտեր էգոյի անձով: Սա մասամբ զվարճալի է, բայց նաև հնարավորություն է ընձեռում դեռահասներին անանուն ծաղրել, վիրավորել կամ սպառնալ այլ դեռահաս օգտատերերի: Ցանկացած բան կարող է խթան հանդիսանալ վիրավորանքի համար, օրինակ՝ եթե խաղացողին չի հաջողվում ինչ որ բան անել կամ պարտվում է: Հաճախ մեկ դեռահասի վիրավորելը վերածվում է զանգվածային կիբերբուլինգի, ինչը կարող է ավարտվել խաղացողին խաղից հանելով կամ կիբերբուլինգը կարող է շարունակվել սոցիալական կայքում կամ հաղորդակցության այլ միջոցներում: Խաղացողների և կիբեռբուլիների անանուն լինելը բարդացնում է վիրավորողի ինքնությունը պարզելը: Դա է պատճառը, որ առցանց խաղերը սրիկաների և մանկապիղծերի համար

հարթակ են հանդիսանում նոր զոհեր փնտրելու կամ նրանց հետ հաղորդակցվելու համար: Տեսախաղի ժամանակ կիբեռհանցագործը կարող է հղում տարածել, որի վրա սեղմելու դեպքում վերջինս հնարավորություն կստանա ներխուժել խաղացողի համակարգիչ և

տնօրինել տվյալները: Երբ ծնողը/ դպրոցը բացահայտում է դեռահասի կիբերբուլինգային վարքագիծը, առաջին հերթին պետք է հիշի, որ դեռահասը սոցիոպատ կամ դաժան մարդ չէ: Ավելի շուտ որոշ երեխաներ չունեն կարեկցանքի զգացում եւ սխալներ են անում: Նախ ծնողը, դպրոցը կամ ընկերը պետք է հիշեցնեն կիբերբուլիին, որ հավասարապես հնարավոր է անձին ցավ պատճառել եւ վնասել առցանց եղանակով, որքան իրական կյանքում, եւ որ հետեւանքների համար պատասխանատվությունը նույնն է, ինչ իրական կյանքում:

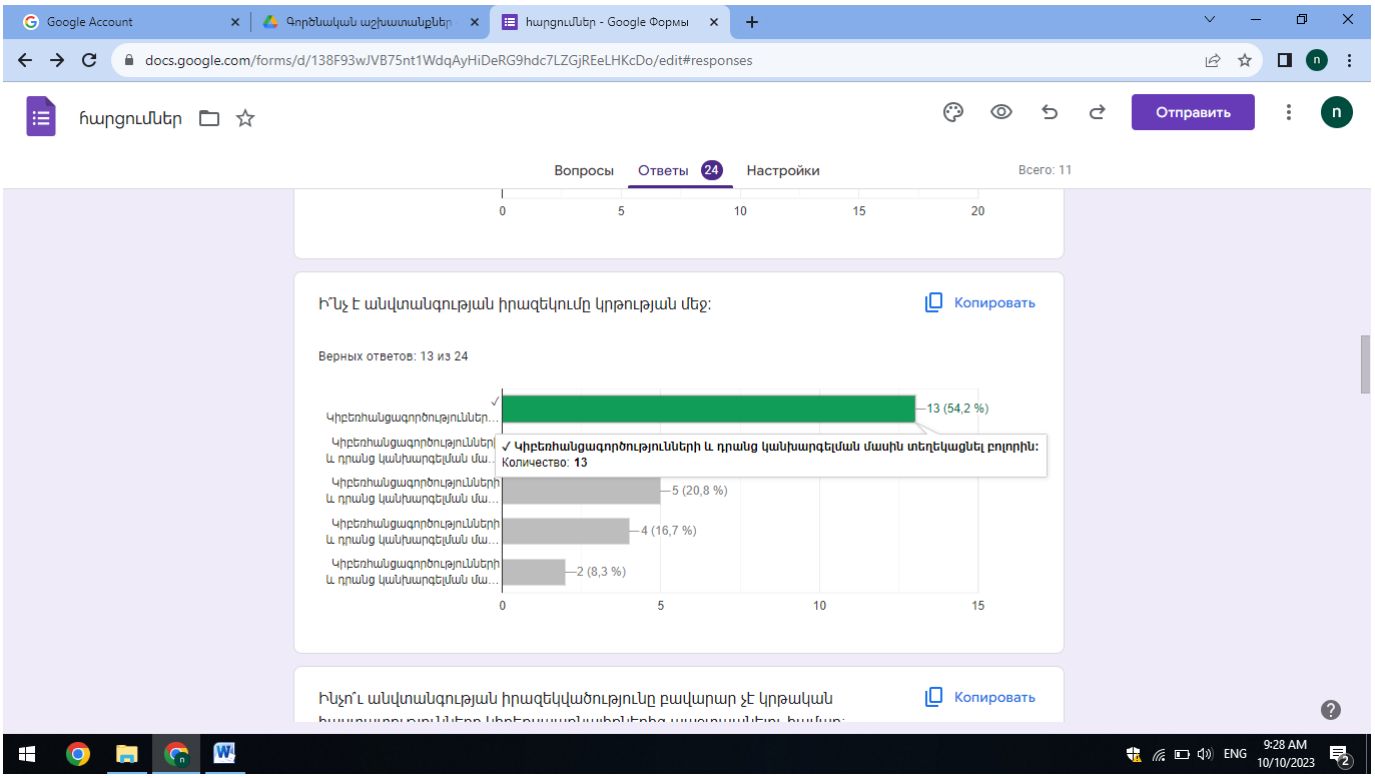
Դպրոցի դերը. Բուլինգի, այդ թվում կիբերբուլինգի ցանկացած ձեւի դեմ պայքարի եւ ռազմավարության մշակումը եւ իրականացումը պետք է լինի դպրոցի պատասխանատվության ներքո: Դպրոցը պետք է ունենա ընդգծված անհանդուրժողականության քաղաքականություն ընդդեմ բուլինգի, եւ ավագ դպրոցի դեռահասները պետք է ակտիվորեն ներգրավվեն այդ քաղաքականության մշակման եւ իրականացման գործում: Երբ դպրոցն ունենա խիստ հակաբուլինգային քաղաքականություն, յուրաքանչյուր աշակերտ կիմանա, որ բացի բարոյական պատասխանատվությունից, կիբերբուլինգը կհանգեցնի նրանց նկատմամբ կարգապահական պատժամիջոցների կիրառման:

Համացանցի անվտանգ օգտագործում սովորեցնելը հակաբուլինգային գործունեության մի մաս է: Կարևոր է նաև, որ աշակերտները ներգրավվեն իրազեկման գործողություններում, օրինակ՝ նկարելով հակաբուլինգային պաստառներ, ստեղծելով և տարածելով հաղորդակցության հիմնական ուղերձներ:

ՀԱՐՑԱԹԵՐԹԻԿԱՅԻՆ ՀԱՐՑԵՐԻ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

Ուսումնասիրության վերաբերյալ կազմել ենք հարցաթերթիկ <<Կիբեռանվտանգությունը դպրոցական կրթության մեջ>> թեմայով: Հարցաթերթիկային հարցման նպատակն է պարզել կիբեռանվտանգության դերն ու ազդեցությունը կրթության մեջ: Հարցմանը մասնակցել է Երևանի տարբեր դպրոցների ուսուցիչներ և աշակերտներ: Հղումը ստորև.

https://docs.google.com/forms/d/138F93wJVB75nt1WdqAyHiDeRG9hdc7LZGjREeLHKcDo/edit



Google Account | Գործնական աշխատանքներ | հարցումներ - Google Формы

docs.google.com/forms/d/138F93wJVB75nt1WdqAyHiDeRG9hdc7LZGjREeLHKcDo/edit#responses

հարցումներ

Отправить

Вопросы | Ответы 24 | Настройки | Всего: 11

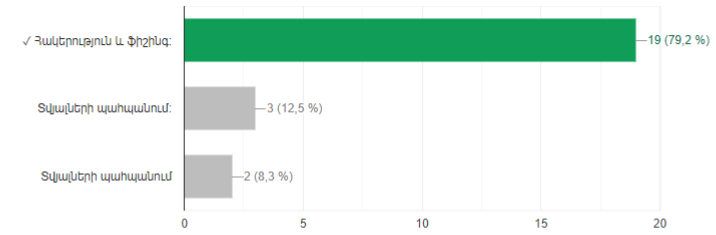
Ճիշտ ոգտվելու կարողունակություն

Կիբեռանվտանգության ապոբեռաբաո հոաձեևում:

Копировать

Նշել կիբեռանվտանգության սպառնալիքները կրթության մեջ:

Верных ответов: 19 из 24



ENG 9:33 AM 10/10/2023

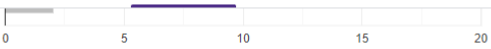
Google Account | Գործնական աշխատանքներ | հարցումներ - Google Формы

docs.google.com/forms/d/138F93wJVB75nt1WdqAyHiDeRG9hdc7LZGjREeLHKcDo/edit#responses

հարցումներ

Отправить

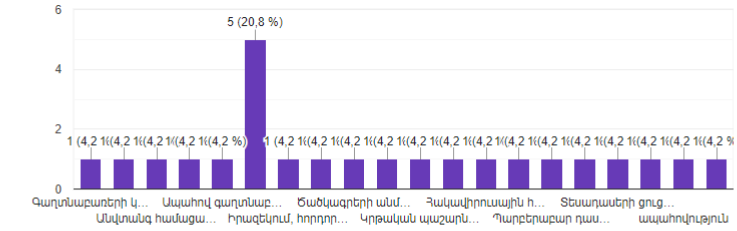
Вопросы | Ответы 24 | Настройки | Всего: 11



Копировать

Նշել անվտանգության միջոցառումներից մի քանիսը, որոնք ներդրված են ուսումնական հաստատության մեջ:

24 ответа



ԻՆչ է կիբեռբուլինգը:

Копировать

ENG 9:38 AM 10/10/2023

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

Անհնար է պատկերացնել 21-րդ դարն առանց տեղեկատվական տեխնոլոգիաների կիրառման, ուստի մեծանում է կիբեռհանցագործությունների թիվը: Կիբեռանվտանգության մասին իրազեկումը կարևոր է նաև ուսումնական հաստատություններում, քանի որ մեծ է կիբեռհանցագործությունների թիվը կրթության ոլորտում: Մեր ուսումնասիրությունները ցույց տվեցին, որ կիբեռանվտանգության մասին գիտելիքների պակասը մեծ է: Անհրաժեշտ է ձեռնարկել այնպիսի միջոցներ, որոնք կբարձրացնեն կիբեռանվտանգության մասին գրագիտության մակարդակը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. https://www.youtube.com/watch?v=Itb0UgqFwLM

2. https://www.youtube.com/watch?v=BzyRe9sCJdw

3. Եվրոպայի խորհրդի Համացանցային գրագիտության ձեռնարկը http://safe.am/ilh/ilh.html

4. Համացանցի Կառավարում գիրքը 5րդ հրատարակություն http://safe.am/book/IG_Book_Armenian_5th_Edition.pdf

5.https://docs.google.com/forms/d/138F93wJVB75nt1WdqAyHiDeRG9hdc7LZGjREeLHKcDo/edit