**Հեղինակ ուսուցիչ՝ Վարդանուշ Հովհաննիսյան**

| **Առարկա** | **Համակարգչային գիտություն և թվային գրագիտություն** |
| --- | --- |
| **Դասարան և կիսամյակ** | **VII դասարան, I կիսամյակ** |
| **Թեմայի գլուխ և թեմա** | ***Էլեկտրոնային ապահովություն*** |
| **Օգտագործվող նյութեր՝** | *1.* [*http://www.checkshorturl.com/*](http://www.checkshorturl.com/) *- կարճ URL հասցեները ստուգող կայք*  *2.* [*https://tsantsar.media.am/worlds/social-media-security*](https://tsantsar.media.am/worlds/social-media-security) *առցանց խաղ՝ «****Սոցիալական մեդիա****» (հեղինակ՝ Մեդիա նախաձեռնությունների կենտրոն)*  *3.* [*https://tsantsar.media.am/worlds/accounts-security*](https://tsantsar.media.am/worlds/accounts-security) *առցանց խաղ՝ «****Հաշիվներ****» (հեղինակ՝ Մեդիա նախաձեռնությունների կենտրոն)* *4.* [*https://youtu.be/hdf8JFzEYyA*](https://youtu.be/hdf8JFzEYyA) *Ինչպես ակտիվացնել Երկփուլային վավերացումը (Two-factor authentication)* ***Ֆեյսբուքում*** *(հեղինակ՝ Անձնական տվյալների պաշտպանության գործակալություն / Armenian PDPA)**5.* [*https://youtu.be/988Db38NNew*](https://youtu.be/988Db38NNew) *Ինչպես ակտիվացնել Երկփուլային վավերացումը (Two-factor authentication)* ***Instagram****-ում (հեղինակ՝ Անձնական տվյալների պաշտպանության գործակալություն / Armenian PDPA)* 6. [*https://passwordsgenerator.net/*](https://passwordsgenerator.net/) *գաղտնաբառեր գեներացնող կայք* |
| **Ամբողջական պատկեր և դասի նպատակ** | ***Նպատակ***  ***Իմանալ տվյալների արտահոսքերի բացասական ազդեցությունը, գաղտնաբառերի պաշտպանության հիմնական սկզբունքները։***  ***Ծանոթանալ սոցիալական ցանցերում, օնլայն խաղերում և մեսենջերներում հիմնական տարածված վտանգներին։*** |
| **Վերջնարդյունքները** | ***Այս դասին սովորողները կկարողանան***  *Բացատրել թե ինչու է էլեկտրոնային ապահովությունն անհրաժեշտ և ինչի համար է պետք տվյալները գաղտնի պահել։*  *Գնահատել ռիսկերը էլեկտրոնային ապահովության բացակայության դեպքում*։  *Գնահատել ինտերնետի օգտագործման սեփական փորձը և կիրառել քայլեր հնարավոր վտանգները նվազագույնին հասցնելու համար։*  *Գնահատել էլեկտրոնային փոստի օգտագործման սեփական փորձը և կիրառել քայլեր հնարավոր վտանգները նվազագույնին հասցնելու համար։*  *Գնահատել սոցիալական մեդիայի/ցանցերի կայքերի, հաղորդագրությունների անմիջական փոխանակման գործիքների (instant messaging), ինտերնետում առկա զրուցասենյակների (internet chatrooms) օգտագործման սեփական փորձը և կիրառել քայլեր հնարավոր վտանգները նվազագույնին հասցնելու համար։*  *Նկարագրել թե ինչ միջոցառումներ է պետք կիրառել ինտերնետում առկա խաղերով անվտանգ խաղալու համար։* |
| **Դասի ընթացք/ ընտրված մեթոդ/ներ** | ***Ներածություն*** *Դասի սկզբում բերել որևէ օրինակ, որի միջոցով սովորողները կհասկանան, որ անձնական տվյալների հանրայնացումը և ոչ պատշաճ պաշտպանությունն իր մեջ մեծ վտանգներ է պարունակում։ Որպես օրինակ կարելի է դիտարկել սիրելի հեքիաթներից որևէ մեկը։ Դրա համար հարցն ուղղել սովորողներին․*  *1. Վստահ եմ, որ շատ եք սիրում հեքիաթներ, կարո՞ղ եք բերել հայտնի հեքիաթների հերոսների օրինակներ, որոնք անձնական տվյալները անծանոթներին տրամադրելով՝ մեծ անախորժությունների մեջ են հայտնվել՝ իրենց հետ վնասելով նաև հարազատներին։ (Կարմիր գլխարկ, Սևուկ ուլիկ․․․․)։ Հիշում ենք, որ դեռ մանկուց ծնողները միշտ զգուշացրել են զգույշ լինել, անձնական ինֆորմացիա չտրամադրել և որևէ տեղ չգնալ անծանոթների հետ։ Այժմ դիտարկենք էլեկտրոնային անվտանգությունը։*  *Ընտրված մեթոդներ՝* ***Մտագրոհ, Մտավոր փորձ***  *Ներկայացնել դասի հիմնական բաժիններն ու դրանց տևողությունը*   1. *Սկիզբ (5 րոպե)* 2. *Հիմնական մաս (13+8+12 րոպե)* 3. *Ամփոփում (7 րոպե)* |
| **Տերմիններ** | *Հաշիվների երկփուլային վավերացում, ֆիշինգային հարձակումներ, տվյալների արտահոսք, անձնական բնույթի տեղեկություն, New Incognito Window*, *ավատար* |
| **Տնային աշխատանք** | *1. Սովորողներին բաժանել երկու խմբի, մի խմբին հանձնարարել սոցիալական մեդիայի միջոցով տվյալներ հավաքագրել մյուս խմբի սովորողներից, իսկ մյուս խմբին՝ հնարավորինս պաշտպանել անձնական տվյալները արտահոսքից։*  *2.* [*https://tsantsar.media.am/worlds/social-media-security*](https://tsantsar.media.am/worlds/social-media-security) *«****Սոցիալական մեդիա****» առցանց խաղի միջոցով ստուգել և ամրապնդել ձեռք բերած գիտելիքները, դուրս գրել այն հարցերի մեկնաբանությունները, որոնց պատասխանելիս սխալվել են։* |

| Գործողությունները | Ուղղորդող, գաղափարներ | Առցանց | Տևող: |
| --- | --- | --- | --- |
| Սովորողներին տալիս եմ հարցեր, որոնց պատասխանելով սովորողները կհանգեն այն գաղափարներին, որոնց անդրադառնալու ենք դասի ընթացքում։ | Այստեղ գրում եմ թեմայի վերաբերյալ այն գաղափարը, որի շուրջ այնուհետև կառուցելու եմ դասը։ Մի քանի գաղափարի դեպքում կարող եմ դրանք դասավորել որոշակի աստիճանակարգով -   * ընդհանուրից մասնավոր, * առավել պարզից բարդ, * առավել ոգևորողից՝ սակավ հետաքրքիր   Գ1/ Տվյալների արտահոսքեր, գաղտնաբառերի պաշտպանության հիմնական սկզբունքները։  Գ2/ Սոցիալական ցանցերում օնլայն խաղերում և մեսենջերներում հիմնական տարածված վտանգներից պաշտպանություն։  Այստեղ հստակ գրում եմ հարցը յուրաքանչյուր գաղափարի համար՝ մտածելով, թե ինչու այս հարցը կարող է հետաքրքրություն առաջացնել յուրաքանչյուր աշակերտի մոտ: Ինչու՞ է կարևոր աշակերտին այս թեմայի շուրջ մտածել։  Գ1 Հ1/ Ի՞նչ էլեկտրոնային ծառայություններից եք օգտվու՞մ։ Ո՞ր սոցիալական ցանցերում ունեք հաշիվներ։  Գ1 Հ2/ Ի՞նչ է գաղտնաբառը։ Ի՞նչ կանոնների է պետք հետևել գաղտնաբառեր կազմելիս։  Գ1 Հ3/ Արդյո՞ք բոլոր հաշիվների համար օգտագործում եք նույն գաղտնաբառը։  Գ2 Հ1/ Ինչ գիտեք երկփուլային վավերացման մասին։ | Օգնականը բացում է [Գլխավոր դոկը](https://docs.google.com/document/d/1E8M_7gloFXHaNNz64pALMVbrF_U6xCvyInKpskqFtJU/copy) և ցուցադրում է գրված հարցերը։ | 1 ր |
| Խնդրում եմ յուրաքանչյուրին բարձրաձայն արտահայտել իր կարծիքը, որոնք առանց մեկնաբանությունների ու քննադատությունների գրառում եմ գրատախտակին։  **Մեծաթիվ երեխաների դեպքում** կարող եմ խնդրել **զույգերով կամ եռյակներով միավորել**` ավելի մեծ խմբերում քննարկելու և հնչեցնելու ընդհանուր պատասխան։  Նույնանման կարծիքները, ըստ անհրաժեշտության, խմբավորում եմ։ | Ինչ մտքեր եմ ակնկալում.  Մ1 Էլ փոստ, Instagram, Facebook, Snapchat, TikTok․․․ , տարբեր զրուցարաններ․․․, խաղեր․․․  Մ2  Այլ անձանցից գաղտնի պահվող բառ կամ սիմվոլների հերթականություն, որն օգտագործվում է ինքնությունը կամ իրավասությունը հաստատելու համար Գաղտնաբառը պետք է կազմված լինի մեծատառերի և փոքրատառերի, ինչպես նաև թվերի և սիմվոլների համադրությունից։  Չպետք է պարունակի հեշտ գուշակվող տեղեկատվություն․ օրինակ՝ ծննդյան թիվը, հեռախոսահամարը, երեխաների, քույր-եղբայրների անունները և այլն։  Մ4  Տարբեր հաշիվների գաղտնաբառերը երբեք չպետք է կրկնվեն։ Եթե մարդը բոլոր հաշիվների համար կիրառում է նույն գաղտնաբառը, ապա նման բացահայտումը վտանգում է նրա բոլոր գրանցումները։  Մ5  Այսօր ամենախորացված պաշտպանության միջոցը երկփուլային մուտքի ընթացակարգն է (Two-factor authentication), որը ենթադրում է գաղտնաբառի մուտքագրումից բացի երկրորդ քայլով անընդհատ փոփոխվող կոդի մուտքագրում, որն օգտվողին տրամադրվում է կամ հատուկ բջջային հավելվածի, կամ սարքի, կամ կարճ հաղորդագրությունների միջոցով։  Ակնկակվող մտքերը չհնչելու դեպքում կարող եմ շարունակել մտագրոհը կամ տալ հետևյալ ուղղորդիչ հարցերը.  ՈՒՀ1  Ո՞ր դեպքում է ավելի հեշտ գուշակել դիմացինի էլեկտրոնային հաշիվների գաղտնաբառերը։  ՈՒՀ2  Արդյո՞ք ձեր անունը կամ ծննդյան տարեթիվը օգտագործել եք որպես գաղտնաբառ։ | Գրառվում են հնչող պատասխանները համապատասխան սյունյակում։ Ուսուցչի հրահանգով օգնականը մգեցնում է ակնկալվող պատասխանները։ | 9 ր |
| Ամփոփում եմ առաջին գաղափարը։  Նույնանման կարծիքները խմբավորում եմ, կատարում եմ հավելումներ և շտկումներ։  Ցուցադրում եմ երկփուլային վավերացման տեսանյութերից մեկը՝  [*https://youtu.be/988Db38NNew*](https://youtu.be/988Db38NNew) *Ինչպես ակտիվացնել Երկփուլային վավերացումը (Two-factor authentication)* ***Instagram****-ում* | Ամբողջ խոսակցությունը հանգում է հետևյալ գաղափար(ներ)ին.  Գաղտնաբառերը հաշիվների պաշտպանության հիմնական բանալին են։ Օգտագործողի համար ամենահեշտ գաղտնաբառը, որը սովորաբար հեշտ է հիշվում, վնասողի համար ավելի դյուրին կռահելի կլինի։  Գաղտնաբառերը մեր անձնական անվտանգության հարցում ամենակարևոր գործոններից են: Գաղտնաբառի վերաբերյալ գոյություն ունեն մի քանի հստակ սկզբունքներ, և եթե մենք դրանց պարբերաբար հետևենք, մեր հաշիվները քիչ թե շատ պաշտպանված կլինեն:  Կարելի է օգտվել գաղտնաբառեր գեներացնող կայքերից, օրինակ՝ [*https://passwordsgenerator.net/*](https://passwordsgenerator.net/)  Երկփուլային մուտքի վավերացումը (Two-factor authentication) նշանակում է, որ եթե ուրիշն անգամ ունի ձեր գաղտնաբառը, նա չի կարող մտնել ձեր հաշիվը՝ առանց հատուկ կոդի, որն էլ անընդհատ փոխվում է։ | Օգնականը ցուցադրում է գլխավոր գաղափարները և եթե ժամանակը բավարար է օգնականը ցուցադրում է հետևյալ կայքը՝ <https://passwordsgenerator.net/>։  Բացված պատուհանում կարող ենք որոշել ծածկագրի կառուցվածքը՝   1. Ծածկագրի երկարությունը(Password Length) 2. Ներառել սիմվոլներ(Include Symbols) 3. Ներառել թվեր(Include Numbers) 4. Ներառել փոքրատառեր(Include Lowercase Characters) 5. Ներառել մեծատառեր(Include Uppercase Characters) 6. Բացառել նմանատիպ տառերը և թվերը շփոթություն չառաջացնելու համար(Exclude Similar Characters) 7. Բացառել տարօրինակ նշանները(Exclude Ambiguous Characters) 8. !Ստեղծել տվյալ սարքի վրա!(Generate On Your Device) 9. Հիշել կարգավորումները հետագայում նորից օգտագործելու համար(Save My Preference) 10. Ստեղծել ծածկագիրը(Generate Password)։ | 2 ր |
| Սովորողներն բաժանում եմ խմբերի։ Մեծ լսարանի դեպքում 4, իսկ մինչև 15 հոգանոց լսարանի դեպքում 3 խմբի։  Սովորողներին կոչ եմ անում իրենց պատկերացնել որևէ իրավիճակում, որից հետո այդ իրավիճակի վերաբերյալ հարցեր են տրվում:  Խմբերին տալիս եմ հարցեր և 6 րոպե այդ հարցերի շուրջ մտածելու և տարբերակներ առանձնացելու (նոթագրման եղանակով) համար։ | Այստեղ նկարագրում եմ այդ իրավիճակը՝ տալով այն լավ պատկերավոր ներկայացնող օրինակներ  Օ1 Չնայած պահել եք գաղտնաբառեր կազմելու վերը նշված կանոնները, սակայն պատկերացրեք, որ փորձում եք մուտք գործել ձեր էլեկտրոնային հաշիվ (էլ․ փոստ, սոցիալական ցանց), բայց չի ստացվում, ինչից էլ եզրակացնում եք, որ այն ենթարկվել է հարձակման, որ ձեր գաղտնաբառը կոտրել են։  Հ1 Ինչպիսի՞ գործողությունների դեպքում է հնարավոր հայտնվել նման իրավիճակում։  Հ2 Ինչպե՞ս խուսափել նման իրավիճակում հայտնվելուց։ | Օգնականը բաժանում է դասարանը 4 կամ 3 խմբի և ուղարկում է [առաջադրանքի ֆայլը](https://docs.google.com/document/d/1HM_ZuDkyG0Cn7O7qnkcLyUJL0e697wSlhJkEDOQhaag/edit?usp=sharing)։ | 4ր |
| Խնդրում եմ սովորողներին գրել իրենց գործողությունների, զգացողությունների, որոշումների մասին։ | Տալիս եմ ուղղորդող հարցեր, որ սովորողները առավել հստակ պատկերացնեն իրենց այդ իրավիճակում և պատասխանեն հարցերին։  ՈւՀ1 Սիրու՞մ եք լրացնել առցանց թեստեր։  ՈւՀ2 Բացու՞մ եք բոլոր եկած նամակների հղումները։  ՈւՀ3 Պահպանու՞մ եք գաղտնաբառը, որ ամեն մուտք գործելուց նորից չհավաքեք։ |  |  |
| Ընդգծում եմ այն գաղափարները, բառերը, որոնք կնպաստեն թեմայի ընկալմանն ու դրա նկատմամբ հետաքրքրության բարձրացմանը։  Հաշվի կորուստ կարող է լինել նաև ոչ անձնական համակարգչից մուտք գործելու դեպքում՝ բրաուզերի մեջ էլեկտրոնային հասցեն և գաղտնաբառը պահպանելով կամ հաշվից դուրս գալ մոռանալով։ Նման վտանգներից խուսափելու համար ոչ անձնական համակարգչից կամ շարժական սարքից պետք է բրաուզերով մուտք գործել հատուկ ռեժիմով, որը չի պահպանում տվյալները պատուհանը փակելուց հետո։ Google Chrome-ի դեպքում դա միանում է որպես New Incognito Window (կամ ստեղնաշարով Ctrl+Shift+N) | Այստեղ նշում եմ աշակերտներից ակնկալվող գաղափարներից մի քանիսը։  Հ1ԱԳ1  Չնայած բարդ գրված գաղտնաբառի, առցանց տիրույթում որոշ անփույթ գործողությունների պատճառով հնարավոր է կորցնել գաղտնաբառը՝   * Բացել ենք կասկածելի հղումները։ * Այլ համակարգիչներից կամ սարքերից օգտվելիս, պահպանել ենք գաղտնաբառերը։ * Պատասխանել ենք այն նամակներին և մուտք ենք գործել այնպիսի էջեր որոնք պահանջում են լրացնել իրական մուտքանունը և [գաղտնաբառը](https://hy.wikipedia.org/wiki/%D4%B3%D5%A1%D5%B2%D5%BF%D5%B6%D5%A1%D5%A2%D5%A1%D5%BC)։ * Խաղացել ենք առցանց թեստեր՝ անձնական հաշվով մուտք գործելով։   Հ2 ԱԳ1 Չի կարելի անզգուշորեն բացել այն կասկածելի հղումները, որոնք նստացել ենք նույնիսկ մեր վստահելի ընկերներից, քանի որ հնարավոր է, որ ընկերոջ հաշիվն արդեն գտնվում է հաքերների վերահսկողության տակ, և տվյալ նամակն ինքը չի կազմել, այլ ուղարկվել է մեզ չարագործների կողմից։  Հ2 ԱԳ2 Չգայթակղվել առցանց թեստերից, դրանք վտանգավոր են և կարող են գողանալ մեր տվյալները։  Հ2 ԱԳ3 Բրաուզերում գաղտնաբառերը պատահաբար չպահպանելու համար մուտք գործել հատուկ ռեժիմով, որը չի պահպանում տվյալները պատուհանը փակելուց հետո։ Google Chrome-ի դեպքում դա միանում է որպես New Incognito Window (կամ ստեղնաշարով Ctrl+Shift+N)  Հ2 ԱԳ4 Պարտադիր ակտիվացնել երկփուլային վավերացումը։ | Գրառվում են հնչող պատասխանները համապատասխան սյունյակում։ Ուսուցչի հրահանգով օգնականը մգեցնում է ակնկալվող պատասխանները։ | 6 ր |
| Նույնանման կարծիքները խմբավորում եմ, կատարում եմ հավելումներ և շտկումներ։ | Ամբողջ խոսակցությունը հանգում է հետևյալ գաղափար(ներ)ին.  **Ֆիշինգը** կիբեռհանցագործության տեսակ է, որի նպատակն է ստանալ որևէ [սոցիալական կայքի](https://hy.wikipedia.org/wiki/%D5%8D%D5%B8%D6%81%D5%AB%D5%A1%D5%AC%D5%A1%D5%AF%D5%A1%D5%B6_%D5%AF%D5%A1%D5%B5%D6%84) օգտատիրոջ գաղտնի տվյալները, ծածկագիրը և ծածկանունը։ Ֆիշինգի զոհ դառնալուց խուսափելու համար հետևել վերոնշյալ գաղափարներին։ | Օգնականը ցուցադրում է գլխավոր գաղափարը։ | 2 ր |
| Այժմ քննարկում ենք մեկ այլ իրավիճակ, որից հետո այդ իրավիճակի վերաբերյալ հարցեր են տրվում: | Այստեղ նկարագրում եմ այդ իրավիճակը՝ տալով այն լավ պատկերավոր ներկայացնող օրինակներ  Օ1 Հանկարծ հայտնաբերում եք, որ սոցիալական ցանցում ունեք ձեր նմանակը, նույն անվամբ և նույն նկարներով։    Հ1 Ինչպիսի՞ գործողությունների դեպքում է հնարավոր հայտնվել նման իրավիճակում։  Հ2 Ինչպե՞ս խուսափել նման իրավիճակում հայտնվելուց։  Տալիս եմ ուղղորդող հարցեր, որ սովորողները առավել հստակ պատկերացնեն իրենց այդ իրավիճակում և պատասխանեն հարցերին։  ՈՒՀ2 Գրառումների, տվյալների հասանելիության ինչպիսի՞ կարգավորումներ են դրված ձեր սոց․ հաշիվներում։    ՈՒՀ2 Հաճա՞խ եք խաղում առցանց խաղեր, որի ժամանակ չեք օգտագործում ավատարներ։ | Օգնականը ուղարկում է [առաջադրանքի ֆայլը](https://docs.google.com/document/d/1JREULUvw6YpmhWBa_S3vxRY-XgeqKuXvotk-wLKRsKc/copy)։ | 4ր |
| Խնդրում եմ սովորողներին արտահայտվել իրենց գործողությունների, զգացողությունների, որոշումների մասին։  Գրատախտակին գրում եմ այն գաղափարները, բառերը, որոնք կնպաստեն թեմայի ընկալմանն ու դրա նկատմամբ հետաքրքրության բարձրացմանը։ | Այստեղ նշում եմ աշակերտներից ակնկալվող գաղափարներից մի քանիսը։  Հ1 ԱԳ1 Սոցիալական ցանցերում բոլոր նկարները և անձնական տվյալները դրված են հրապարակային ռեժիմով։  Հ1 ԱԳ1 Գրանցվել ենք առցանց խաղերի, որտեղ օգտագործել ենք իրական նկարներ։  Հ2 ԱԳ1  Զգույշ վերաբերվել անձնական տեղեկություններին: Լուսանկարները հրապարակելիս անպայման նշել «Միայն ընկերների համար» կարգավորումը։  Հ2 ԱԳ3  Հրապարակային չդնել, բնակության հասցեն, էլ փոստի հասցեն, տարիքը։  ԱԳ4  Համակարգչային խաղեր խաղալիս ընտրել անվտանգ խաղանուն, օրինակ՝ SecretNinja99․․․, օգտագործել ավատար համացանցային տեսախցիկի փոխարեն: Տեսախցիկը շատ լավ բան է, բայց կարիք չկա, որպեսզի անծանոթներն իմանան, թե ինչ արտաքին ունենք: | Գրառվում են հնչող պատասխանները համապատասխան սյունյակում։ Ուսուցչի հրահանգով օգնականը մգեցնում է ակնկալվող պատասխանները։ | 6 ր |
| Նույնանման կարծիքները խմբավորում եմ, կատարում եմ հավելումներ և շտկումներ։ | Ամբողջ խոսակցությունը հանգում է հետևյալ գաղափար(ներ)ին.  Սոցիալական ցանցում պետք չէ հրապարակել այնպիսի բաներ, որը չէիք ցանկանա հեռարձակվեր հանրության համար և արտացանցային աշխարհում:    Խնդիրն այն է, որ համացանցում անձնական բնույթի տեղեկատվություն տեղադրելուն պես` մարդն այլևս ի վիճակի չէ վերահսկել, թե ով կտեսնի դա կամ ինչպես այն կօգտագործվի:  Նկարները հեշտությամբ կարող են կրկնօրինակվել և սեղմակի մեկ հպումով տարածվել հազարավոր մարդկանց շրջանում: Ունենալով թվային բնույթ` նրանք կարող են  փոփոխվել կամ աղավաղվել: Նկարները կարող են նաև օգտագործվել որոնման նոր ծրագրերի կողմից` մարդկանց նույնականացնելու նպատակով (եթե անգամ նկարի կողքին չկա անունը):  Համացանցային խաղերը զվարճալի են և ինտերակտիվ: Կարող եք խաղալ ընկերների և աշխարհի տարբեր ծայրերում գտնվող անձանց հետ: Համոզվեք, որ համացանցային խաղեր խաղալիս պաշտպանված եք դուք և ձեր անձնական բնույթի տեղեկությունները: | Օգնականը ցուցադրում է գլխավոր գաղափարները։ | 4 ր |
| Ամփոփում եմ դասը՝ հանձնարարելով պատասխանել «Հաշիվներ» առցանց խաղի հարցերին։  Կախված իրավիճակից (տեխնիկական հագեցվածություն, ինտերնետի առկայություն) կարող եմ հանձնարարել թեստին պատասխանել անհատապես կամ կարող եմ միացնել պրոյեկտրով և պատահականության սկզբունքով ընտրել հարցը և այն սովորողին, որը կպատասխանի հարցին՝ պատասխանը քննարկելով բոլոր սովորողների հետ։ | [*https://tsantsar.media.am/worlds/accounts-security*](https://tsantsar.media.am/worlds/accounts-security) *առցանց խաղ՝ «****Հաշիվներ****»* | Կախված առկա պայմաններից օգնականը ուղարկում է [խաղի հղումը](https://tsantsar.media.am/worlds/accounts-security), կամ միացնում է այն էկրանի վրա։ | 7ր |