

«Փաստերի ստուգումը
պաշտոնյաների համար»
դասընթացի ծրագիր

Բովանդակություն

Դասընթացի նպատակը և խնդիրները	3
Դասընթացի մեթոդաբանությունը	4
Թեմա 1. Ինչ է մեղիագրագիտությունը և ինչու է այն կարևոր	6
Թեմա 2. Լրատվամիջոցներ՝ տիպերը, կառուցվածքը	6
Թեմա 3. Արտահայտվելու և տեղեկատվության ազատություն	6
Թեմա 4. Մեղիայի տեքստ, համատեքստ, մանիպուլյացիա, փաթեթավորում	7
Թեմա 5. Տեղեկությունների ճշգրտումը և Փաստերի ստուգումը	8
Թեմա 6. Աղբյուրների ուսումնասիրությունը, որոնումը	8
Թեմա 7. Լուսանկարների ստուգում	9
Թեմա 8. Տեսանյութերի ստուգում	9
Թեմա 9. Տեղորոշում և արբանյակային լուսանկարներ	10
Թեմա 10. Կայքերի խորացված զննում	10
Թեմա 11. Հաշիվների ստուգումը սոցցանցերում	10
Թեմա 12. Էլփոստերի ստուգում	11
Թեմա 13. - Աշխատանք բաց տվյալների հետ	11
Թեմա 14. Խորացված որոնում	11
Թեմա 15. Տեղեկատվական անվտանգության սկզբունքները և իրագործման գործիքները	12
Օգտակար հղումներ	13

Ներածություն

Ինտերնետն ու սոցիալական ցանցերն այսօր դարձել են ինչպես տեղեկատվության, այնպես էլ ապատեղեկատվության տարածման առաջնային մեխանիզմ: Բերելով քաղաքացիների իրազեկվածությունը բարձրացնելու աննախադեպ հնարավորություններ՝ սոցցանցերը միաժամանակ պարարտ հող են նախապատրաստում ապատեղեկատվության ստեղծման և տարածման համար, իսկ քաղաքացիները, չունենալով մեդիագրագիտության և տեղեկատվության ճշտման անհրաժեշտ հմտություններ ու գիտելիքներ, դժվարությունների առաջ են կանգնում՝ չիմանալով ինչին հավատալ, վստահել:

Սա նշանակում է, որ ապատեղեկատվությունը՝ կեղծ կամ դիտավորյալ ուղղորդված, մանիպուլյատիվ տեղեկությունների տարածումը, որի հիմքում կոնկրետ տնտեսական կամ քաղաքական շահեր կան, տարածվում է ավելի հեշտ և արագ, քան երբևէ:

Ապատեղեկատվությունը նման է վնասաբեր վիրուսի, առավել ևս, երբ խոսքը վերաբերում է COVID-19 համավարակին առնչվող ապատեղեկատվության մասին: Դրա հետևանքով քաղաքացիները կարող են անտեսել գիտականորեն հիմնավորված փաստերը՝ վտանգելով ոչ միայն իրենց սեփական, այլև իրենց հարազատների, մտերիմների առողջությունը:

Ակնհայտ է, որ ինչպես COVID-19 վիրուսը, ապատեղեկատվությունը ևս ավելի արագ է տարածվում է, երբ դրա հետ առնչվող մարդիկ իրենց անխոհեմ վարքով պայմաններ են ստեղծում: Եվ եթե մենք փորձում ենք պատասխանատվություն ցուցաբերել վարակի տարածումը կանխելու համար, նույնքան էլ կարևոր է պատասխանատվությունը՝ ապատեղեկատվության տարածումը կանխելու հարցում: Մեկ անգամ էլ ծանրութեթև անելը, նախքան սոցիալական ցանցերում հրապարակված որևէ գրառում տարածելը կամ մեկնաբանելը, պետք է դառնա ճիշտ այնպիսի սովորույթ, ինչպիսին է COVID-19-ի տարածումը դանդաղեցնելու նպատակով ձեռքերն ախտահանելը, և կարող է նույնքան էլ արդյունավետ միջոց լինել՝ վիրտուալ համավարակը կանխելու հարցում:

Միննույն ժամանակ, կարևոր է մատնանշել, որ ապատեղեկատվության դեմ պայքարի հարցում հաջողության հասնելը անհնար է, երբ լիարժեք չի իրացվում տեղեկատվության ազատության իրավունքը: Կեղծ, մանիպուլյատիվ և ապակողմնորոշող տեղեկատվությունը դիմագրավելու համար անհրաժեշտ է քաղաքացիներին կարողություններ և գործիքներ տալ՝ լուրերին քննադատաբար մոտենալու և փաստերի ստուգում իրականացնելու համար:

Դասընթացի նպատակը և խնդիրները

«Փաստերի ստուգումը պաշտոնյաների համար» դասընթացի նպատակն է բարելավել պաշտոնյաների՝ փաստերի ստուգման գիտելիքն ու հմտությունները, դարձնել նրանց առավել դիմակայուն:

Դասընթացի հիմնական խնդիրներից է՝ պաշտոնյաներին իրազեկել փաստերի ստուգման սկզբունքների, այդ նպատակով կիրառվող լրագրողական հմտությունների, թվային հասանելիություն ունեցող հիմնական գործիքների մասին: Մեկ այլ կարևոր խնդիր է պաշտոնյաներին աջակցել, որպեսզի վերջիններս փնտրեն, ստանան եւ տարածեն վստահելի եւ ճշգրիտ տեղեկություններ:

Դասընթացը բաղկացած է 15 հիմնական բաժինից, որոնցից յուրաքանչյուրն անդրադառնում է փաստերի ստուգման առանձին հիմնահարցերի ու դրանց լուծման միջոցներին ու գործիքներին:

Դասընթացի շնորհիվ պաշտոնյաները տեղյակ կլինեն՝ ինչպես խուսափել կեղծ լուրերից, ինչպես ստուգել փաստերը նախքան դրանք տարածելը կամ մեկնաբանելը: Դասընթացին մասնակցած պաշտոնյաները կունենան հիմնարար գիտելիք և հմտություններ լրագրության հիմունքների, լրագրողական աղբյուրների, տեղեկություններ փնտրելու, տարածելու մեխանիզմների, փաստերի ստուգման անալոգային և թվային մեթոդների, գործիքների մասին և կկարողանան դրանք ինքնուրույն կիրառել փաստերի ստուգման և ճշգրտված տեղեկությունների տարածման նպատակով:

Դասընթացի մեթոդաբանությունը

Դասավանդման հիմնական մեթոդը մարդակենտրոն ուսուցման մոտեցումն է: Այն ներառում է ուսուցման, խնդիրների լուծման և որոշումների կայացմանն առնչվող բազմաթիվ առանձնահատկություններ, որոնց շնորհիվ մասնակիցները ձեռք են բերում նոր գիտելիք և հմտություններ հետևյալ փուլերի միջոցով.

- խնդրի բացահայտում,
- խնդրի հիմքում ընկած վերաբերմունքի և համոզմունքների բացահայտում,
- խնդրի հիմքում առկա փաստերի և սկզբունքների պարզաբանում,
- ապացույցների հայտնաբերում և վերլուծություն,
- խնդրի մեկնաբանում և լուծում,
- գործողություններ ձեռնարկել և վերանայել յուրաքանչյուր փուլից բխող հետևանքներն ու արդյունքները:

Այս մեթոդը հնարավորություն կտա մասնակցին բացահայտել և խորքային յուրացնել թեմաները:

Ուսուցումն իրականացվում է նաև հետևյալ մեթոդների համադրմամբ.

1. Դասախոսություններ,
2. Գործնական քննարկումներ,
3. Պրակտիկ առաջադրանքներ,
4. Խմբային քննարկումներ,
5. Բանավեճ,
6. Գործնական աշխատանքներով գիտելիքի անհապաղ կիրառում և ստուգում:

Նկատենք, որ այս դասընթացի մասնակիցներն արդեն իսկ ունեն որոշակի փորձառություն, որը կարող է կիրառվել որպես ռեսուրս նրանց ուսումնառության ընթացքում:

Դասընթացի ուսուցման ընթացքում դասավանդողը նախևառաջ մասնակիցներին ներկայացնում է տվյալ թեմայի վերաբերյալ դասախոսություն՝ փոխանցելով տեսական գիտելիք, որն անպայման զուգորդվում է գործնական օրինակներով ինչպես տեղական, այնպես էլ միջազգային պրակտիկայից:

Դասընթացում կիրառվող օժանդակ մեթոդներից է նաև դեպքերի ուսումնասիրման (case study) մեթոդը: Այն ներառում է մեկ կոնկրետ դեպքի կամ իրադարձության խորքային քննություն: Այս մեթոդի շնորհիվ մասնակիցներն ուսումնասիրում են գործնական օրինակներ՝ տեսնելու, թե ինչպես կարելի է կիրառել տեսական գիտելիքն իրական միջավայրում և կոնկրետ օրինակում: Այս մեթոդի շնորհիվ մասնակիցները կարողանում են ավելի խորը և համակողմանի հասկանալ թեման: Այսպիսով, յուրաքանչյուր թեմային առնչվող տեսական գիտելիքին հաջորդում է

թեմային առնչվող տարբեր դեպքերի (cases) և իրավիճակների քննարկումը, այդ թվում՝ խմբային աշխատանքի միջոցով: Մասնակիցներն աշխատում են փոքր խմբերով և քննարկելով առաջադրված խնդիրը՝ ներկայացնում են իրենց պատկերացումները և առաջարկում կոնկրետ լուծումներ տրված իրավիճակներին, ինչպես նաև ներկայացնում այն գործիքները, որոնք իրենք կկիրառեն տվյալ իրավիճակը լուծելու նպատակով: Օրինակ, ինչ գործիքների միջոցով կիրականացնեն աղբյուրների ստուգումը, կամ օգտատիրոջ տվյալների փնտրումը սոցցանցերում կամ լուսանկարների մետատվյալների ստուգումը: Դասավանդողի դերն է մոդերացիա անել քննարկումների ընթացքում, ինչպես նաև քննարկման ավարտին ամփոփել պատասխանները՝ ներկայացնելով տվյալ իրավիճակի համար առավել նախընտրելի լուծումներն ու գործիքները:

Գործնական աշխատանքներն իրականացվում են նաև համագործակցային ուսուցման մեթոդով, որը մասնակիցներին միավորում է համատեղ նպատակների իրականացման համար: Համագործակցային ուսուցումը կարող է լինել խմբային ուսուցումից մինչև ավելի բարդ ձևաչափեր, ինչպիսիք են տարբեր նախագծերի պլանավորումն ու իրականացումը, մասնակիցների փոխադարձ ուսուցանումը, որոնք նպաստում են նրանց միջև գաղափարների փոխանակմանն ու միմյանցից սովորելուն:

Դասընթացի սկզբում հարցաթերթիկի միջոցով կստուգվի մասնակիցների մոտ առկա նախնական գիտելիքների առկայությունը, իսկ ավարտին մասնակիցների գիտելիքը կգնահատվի վերջնական գնահատման հարցաթերթիկների միջոցով:

Թեմա 1. Ինչ է մեդիագրագիտությունը և ինչու է այն կարևոր

Այս թեմայի շրջանակում դասավանդողը ներկայացնում է, թե ինչ է մեդիագրագիտությունը առհասարակ, ինչու է այն կարևոր հատկապես հիմա՝ ինֆորմիայի ժամանակաշրջանում, խոսելու է այն մասին, թե ինչ է լրատվական հոսքը, ինչ է մեդիան, ինչպիսին պետք է լինի մեդիայի դերը հասարակությունում:

Առաջարկվում է դասը վարել հիմնականում քննարկման, հարցուպատասխանի, օրինակների ներկայացման տեսքով:

Քննարկման թեմաներ՝ ի՞նչ էք դիտում, կարդում, ինչո՞ւ է դա ձեզ համար հետաքրքիր կամ կարևոր, օրվա ընթացքում ի՞նչ նոր բան էք իմացել, որտեղի՞ց, ո՞ր դեպքերում էր այդ տեղեկատվությունը օգտակար, ո՞ր դեպքերում էր ավելորդ: Որքանո՞վ էք ձեզ զգում որպես տեղեկատվության տարածող, այլ ոչ միայն ընկալող:

Թեմա 2. Լրատվամիջոցներ՝ տիպերը, կառուցվածքը

Դասավանդողը հակիրճ ներկայացնում է մեդիայի պատմությունը՝ ժայռապատկերներից մինչև բանավոր պատմություններ, թերթեր, էլեկտրոնային հաղորդակցության միջոցներ: Այնուհետև առավել մանրամասն կենտրոնանում է հայաստանյան լրատվամիջոցների վրա, ներկայացնում առավել ազդեցիկ, մեծ լսարան ունեցող լրատվամիջոցները, խոսում է հանրային լրատվամիջոցների առանձնահատուկ դերի մասին, ներկայացնում է միջազգային լրատվամիջոցները, այդ թվում պետական՝ քարոզչական նշանակություն ունեցողները:

Հարցեր մասնակիցների համար՝ ի՞նչ թերթեր, ռադիոկայաններ, հեռուստաընկերություններ, օնլայն լրատվամիջոցներ կան Հայաստանում, դրանք ի՞նչ ուղղվածություն ունեն, ի՞նչ թերություններ և առավելություններ ունեն և այլն: Ինչպե՞ս էք ինքներդ ձեր համար զատում լրատվամիջոցները, ունե՞ք անձնական չափանիշներ:

Վարժություն / հանձնարարություն՝ մասնակիցները բաժանվում են խմբերի և կազմում լուրի, ռեպորտաժի սխեմա տարբեր տիպի լրատվամիջոցների համար, այնուհետև յուրաքանչյուր խումբ ներկայացնում է, թե կոնկրետ ինչպես են լուսաբանելու նյութը: Փորձ է արվում մշակել տարբեր տիպի լուրեր՝ քաղաքական, մշակութային, սպորտային, հասարակական, տնտեսական:

Թեմա 3. Արտահայտվելու և տեղեկատվության ազատություն

Այս թեմայի շրջանակում դասավանդողը ներկայացնում է խոսքի և տեղեկատվության ազատության հասկացությունները և անհրաժեշտությունը հասարակության համար,

մասնավորապես ապատեղեկատվության դեմ պայքարում: Ներկայացվում է այն գաղափարը, որ տեղեկություն ստանալու իրավունքի լիարժեք պաշտպանությամբ և պրոակտիվ հրապարակայնությամբ են պայմանավորված հասարակության տեղյակ լինելու իրավունքը և կառավարությանը հսկելու, հաշվետու դարձնելու հնարավորությունների իրացումը:

Քննարկման թեմաներն են.

- խոսքի և տեղեկատվության ազատության իրավական երաշխիքները,
- տեղեկություն տրամադրելու ընթացակարգերը. տեղեկություն տրամադրելու կարգը, ժամկետները և մեխանիզմները,
- ինչ պարտավորություններ ունեն պաշտոնյաները տեղեկատվության տրամադրման գործընթացում,
- խախտումների բողոքարկման հնարավորությունը,
- պրոակտիվ հրապարակայնություն,
- խոսքի և տեղեկատվության ազատության անհրաժեշտ սահմանափակումները, արգելված բովանդակություն (ատելության խոսք, բռնության կոչ, քարոզ և այլն):

Այս թեմայի շրջանակում մասնակից պաշտոնյաները կտեղեկանան տեղեկատվության ազատության օրենսդրության շրջանակում եւ միջազգային կոնվենցիաներով սահմանված տեղեկություն ստանալու հարցումներին պատշաճ ընթացք տալու մեխանիզմներին: Ինչպես օրենքով սահմանված կարգով եւ ժամկետներում տեղեկատվություն տրամադրել տարբեր դիմողներին, կտեղեկանան մերժմանը ներկայացվող պահանջներին, պաշտոնական կայքերում տեղեկատվություն հրապարակելու կանոններին եւ այլն: Պրոակտիվ հրապարակայնության ենթաթեմայի շրջանակում մասնակիցները կտեղեկանան տեղեկատվությունը սեփական նախաձեռնությամբ հրապարակելու արդյունավետ մեխանիզմներին և միջոցներին:

Թեմա 4. Մեդիայի տեքստ, համատեքստ, մանիպուլյացիա, փաթեթավորում

Այս թեմայի շրջանակում մասնակիցները պետք է պատկերացում կազմեն մեդիայով տարվող մանիպուլյացիաների, թեմայի շեշտադրումները փոխելու, պաշտոնյաների խոսքը ձևափոխելու մասին: Դասավանդողը պետք է փորձի ամենօրյա օրինակներով ցույց տալ, թե ինչպես, օրինակ, հնարավոր է նույն թեման լուսաբանել՝ տարբեր շեշտադրումներով և ստանալ լրիվ այլ ենթատեքստ: Մասնակից պաշտոնյաներին հարկավոր է ներկայացնել թե՛ տեքստային, թե՛ լուսանկարներով, թե՛ տեսանյութերով՝ այդ թվում մոնտաժի օգնությամբ և վիզուալիզացիայի կիրառմամբ մանիպուլյացիաների օրինակներ:

Քննարկվում են մանիպուլյացիաները.

- Վերնագրում
- Տեքստում

- Մեջբերվող աղբյուրներում
- Հրապարակումներին կից լուսանկարներում և տեսանյութերում

Վարժություն / հանձնարարություն՝ մասնակիցները բաժանվում են խմբերի և ընթերցում են նախապես ընտրված հրապարակում միևնույն իրադարձության մասին, բայց տարբեր քաղաքական կողմնորոշում ունեցող լրատվամիջոցների լուսաբանմամբ: Այնուհետև ամեն խումբ ներկայացնում է, թե ինչ է տեղի ունեցել՝ հիմնվելով նյութում եղած փաստերի վրա: Այնուհետև որպես խումբ վերլուծում են ստացած տեղեկատվությունը, փորձում են գտնել մեղիա մանիպուլյացիայի, տարբեր փաթեթավորման և շեշտադրումների օրինակներ ներկայացված հրապարակումներում:

Թեմա 5. Տեղեկությունների ճշգրտումը և Փաստերի ստուգումը

Դասընթացավարը ներկայացնում է երկու հիմնական տերմինների՝ տեղեկությունների՝ ճշգրտման (information verification) և փաստերի ստուգման (fact checking) առնչությունները՝ առաջինը սահմանելով որպես լրագրության հիմնարար սկզբունք, երկրորդը՝ որպես դրա առանձին կիրառություն, երբ գործ ունենք արդեն հրապարակված, հայտարարված փաստերի ու տվյալների ստուգման հետ:

Վարժություն՝ դասավանդողն աաջարկում է վերլուծել հայաստանյան և արտասահմանյան լրատվամիջոցների հրապարակած նյութեր և դրանցում մատնանշել լրագրողի թույլ տված սխալները ու փորձել նկարագրել, թե իրենք ինչ կանեին հրապարակելուց առաջ տվյալ տեղեկատվությունը ճշտելու համար, կամ նյութում ներկայացվող աղբյուրներին, ականատեսներին ուրիշ ինչ հարցեր կտային՝ ոչ հավաստի տեղեկատվություն հրապարակելուց խուսափելու համար: Մասնակիցներին կներկայացվի նաև փաստերի ստուգման և տեղեկությունների ճշգրտման տեղական ու միջազգային փորձը, այդ թվում՝ փաստերի ստուգմամբ զբաղվող հայկական ու արտասահմանյան առաջատար մեղիա կազմակերպությունները:

Թեմա 6. Աղբյուրների ուսումնասիրությունը, որոնումը

Փաստերի ստուգման առաջին քայլը հրապարակված տեղեկատվության սկզբնաղբյուրը նույնականացնելը և բավանդակությունը ստուգելն է: Դա անելու համար անհրաժեշտ է նախ հաստատել, որ գործ ունենք տեղեկության սկզբնական տարբերակի հետ և պարզելը, թե արդյոք այն ներկայացված է ամբողջությամբ, կամ գուցե ենթարկվել է մանիպուլյացիաների և կտրվել է ենթատեքստից: Անհրաժեշտ քայլերն են.

- համոզվել, թե արդյոք տեղեկությունները տարածողը վստահելի աղբյուր է,

- պարզելը, թե տվյալ աղբյուրը ի՞նչ կապ ունի թեմայի հետ և արդյոք չունի որոշակի շահագրգռվածություններ, շահեր՝ տվյալ տեղեկատվության տարածման հետ կապված,
- պարզելը, թե կան արդյոք այլ աղբյուրներ նույն տեղեկատվության վերաբերյալ:

Թեմա 7. Լուսանկարների ստուգում

Դասընթացավարը պետք է ներկայացնի լուսանկարների սկզբնաղբյուրը հայտնաբերելու հնարավորությունները որոնողական համակարգերում՝ <https://images.google.com>, <https://www.bing.com/images/>, <https://yandex.ru/images/>, ինչպես նաև <https://www.tineye.com/> մասնագիտացված որոնողական հարթակը, ցույց տա դրանցից օգտվելու եղանակները:

Թեմայի զգալի մասը պետք է նվիրված լինի լուսանկարների մետատվյալներին՝ EXIF տվյալներին, որոնք տեսանելի չեն, սակայն պարունակում են ամբողջական տեղեկություն պատկերի մասին՝ որտեղ է այն նկարվել, երբ է նկարվել, մշակվել է, թե ոչ և այլն: Լուսանկարի մետատվյալները կարդալու համար առաջարկում ենք օգտվել «Jeffrey's Image Metadata Viewer» (<http://exif.regex.info/exif.cgi>) կամ Metapicz (<http://metapicz.com>) և համանման այլ անվճար հասանելի հարթակներից:

Դասընթացավարը պետք է ներկայացնի նաև Fotoforensics.com հարթակը և դրա միջոցով լուսանկարների հետ իրականացված մանիպուլյացիաների բացահայտման հնարավորությունները:

Որպես պրակտիկ առաջադրանք պաշտոնյաներին կարելի է առաջարկել ստուգել իրենց գերատեսչությանն առնչվող տարբեր կեղծված, մշակված, ինչպես նաև չմշակված և իրական լուսանկարների իսկությունը, մետատվյալները, հայտնաբերել դրանց սկզբնաղբյուրները և այլն:

Թեմա 8. Տեսանյութերի ստուգում

Տեսանյութերի ստուգման հարցում կարևոր է նախևառաջ պատկերացում կազմել դրանցով մանիպուլյացիաներ իրականացնելու և կեղծման հիմնական երեք ուղղությունների հետ՝ ենթատեքստի բացակայություն (կամ կիրառությունը այլ ենթատեքստում), խաբուսիկ մոնտաժ, դիտավորությամբ արված տրանսֆորմացիա, ինչպես նաև համակցված իրականություն (AR):

Հաճախ տեսանյութերը օգտագործվում են բոլորովին այլ թեմայի վերաբերյալ հրապարակումներում: Օրինակ, ուկրաինական պատերազմի տեսանյութերը կարող են վերագրվել արցախյան հակամարտությանը և այլն: Նմանատիպ դեպքերում պաշտոնյաները

պետք է ծանոթ լինեն Amnesty-ի YouTube Dataviewer էջին և InVid հավելվածին, որոնք, տեսանյութից սրբինշոթեր գեներացնելով և դրանք որոնելով, հաճախ թույլ են տալիս հայտնաբերել տեսանյութերի օրիգինալները և կարող են օգտակար լինել վերը նշված բոլոր երեք դեպքերում էլ: Մասնակիցները նաև պետք է սովորեն ինքնուրույն ստեղծել սրբինշոթեր և դրանց միջոցով գտնել սկզբնաղբյուրները, քանի որ տեսանյութերը կարող են տեղադրված լինել այլ հարթակների վրա, որոնց հետ չեն աշխատում վերոհիշյալ համակարգերը (օրինակ՝ Telegram, WhatsApp):

Վերջին շրջանում տարածում է ստացել նաև կեղծ տեսանյութերի մեկ այլ կատեգորիա՝ Deepfake-երը: Թեև առայժմ այս տիպի տեսանյութերը հեռու են այն տեխնիկական կատարելությունից, որպեսզի դրանք հնարավոր չլինի անգեն աչքով տարբերել, այնուամենայնիվ, պաշտոնյաները պետք է տեղեկանան նաև այդ տեխնոլոգիաների (AR/VR) առկայության մասին և ցանկացած տեսանյութի վերաբերեն առողջ կասկածամտությամբ:

Թեմա 9. Տեղորոշում և արբանյակային լուսանկարներ

Թե՛ լուսանկարների, թե՛ տեսանյութերի, և թե՛ անգամ դեպքի վայրի տեքստային նկարագրությունների մեջ անճշտությունների, փաստերի մանիպուլյացիաների հայտնաբերման համար կան մի շարք մեթոդներ և գործիքներ, որոնց մասին անհրաժեշտ է տեղեկացված լինել:

Դասընթացավարը պետք է պաշտոնյաներին ներկայացնի «Google»-ի քարտեզների ընդլայնված գործիքը՝ «Google Earth»-ը, Here Maps-ը (<https://wego.here.com>), Bing Maps-ը (<https://www.bing.com/maps/>), «EOS» համակարգը՝ <https://eos.com/landviewer/>, «Planet»-ը՝ <https://www.planet.com/>: Հատկապես Հայաստանում (և հետխորհրդային տարածաշրջանում) լավ է աշխատում Yandex.Maps հարթակը, հետևաբար փողոցների տվյալները առավել թարմացված են: Դասընթացավարը պետք է գործնական կիրառություններով ցույց տա քարտեզների արդյունավետությունը:

Արբանյակային լուսանկարներում երևացող սովերներով օրը և ժամը որոշելու ծառայություններից էլ օգտակար կարող են լինել <http://suncalc.net/> և <https://www.suncalc.org> ծառայությունները:

Անհրաժեշտության դեպքում պետք է միջազգային փորձի ուսումնասիրման լավագույն օրինակները բերել BellingCat-ից և NY Times-ի Visual Inverstigations թիմից:

Որպես գործնական առաջադրանք մասնակիցներին տրամադրվելու են լուսանկարներ, որտեղ առկա շենքերը, շինությունները և այլ կառույցներ կօգնեն տեղորոշելու ոչ միայն լուսանկարված օբյեկտի վայրը, այլև հասկանալու, թե որտեղից է արվել լուսանկարը:

Թեմա 10. Կայքերի խորացված զննում

Այս բաժնում դասավանդողը պետք է մասնակիցներին պատկերացում տա կայքերի անվանման՝ դոմեյնային տիրույթների, հոսթինգի մասին, ինչպես նաև ներկայացնի դրանց ուսումնասիրման սկզբունքները:

Այս բաժնում պաշտոնյաները պետք է պրակտիկ վարժությունների միջոցով յուրացնեն կայքերի արտաքին զննման, html կոդի ուսումնասիրման, Whois և Geo IP Lookup ծառայությունների միջոցով ուսումնասիրության, ինչպես նաև կայքում ներդրված գովազդային, վիճակագրական վերլուծության համակարգերի դասիչներով (օրինակ՝ Google Analytics-ի կոդով) կայքերի միջև փոխկապակցվածությունների բացահայտման հմտություններ:

Որպես գործնական առաջադրանք պաշտոնյաները պետք է ստուգեն իրենց գերատեսչությունների պաշտոնական կայքերի գրանցման տվյալները՝ կիրառելով դասընթացավարի փոխանցած հմտությունները:

Թեմա 11. Հաշիվների ստուգումը սոցցանցերում

Եթե պաշտոնյանյին պետք է ճշտել ապատեղեկատվություն տարածած սոցցանցային օգտատիրոջ իրական լինելը, իհարկե, ամենաարդյունավետ ձևն է տվյալ օգտատիրոջ հետ կապի մեջ մտնել և տեսաձայնային կապ առաջարկել: Նման դեպքերը հազվադեպ են, սակայն աղբյուրն այդպես կարող է հաստատել, որ ինքն իրական է:

Առաջին քայլը պետք է լինի օգտատիրոջ լուսանկար/ների ստուգումը որոնողական համակարգերի միջոցով: Երբեմն կեղծ օգտատերերի նկարները հայտնաբերվում են այլ օգտատերերի մոտ կամ նույնիսկ ամսագրերում: Twitter-ի ու Instagram-ի դեպքում հարկավոր է ուսումնասիրել գրառումների քանակը և ակտիվությունը, այլ օգտատերերի հետ փոխկապակցվածությունը

Հաճախ կեղծ օգտատերերը կամ գերշատ, կամ էլ հակառակը՝ շատ քիչ գրառումներ են ունենում: Հարկավոր է հնարավորինս ուշադիր ուսումնասիրել բոլոր տվյալները և գտնել հնարավոր հակասությունները:

Գործնականում մասնակիցները պետք է փորձեն փնտրել պաշտոնյաների օգտահաշիվներին ակտիվ մեկնաբանողներին՝ պարզելու դրանց իրական կամ կեղծ լինելը:

Թեմա 12. Էլփոստերի ստուգում

Հաճախ հարկավոր է ճշտել, թե այս կամ այն էլեկտրոնային փոստը ինչ հետքեր ունի սոցիալական ցանցերում կամ այլ հարթակներում: Այսպես, «Email Sherlock»-ը (<https://www.emailsherlock.com/>) թույլ է տալիս տեսնել, թե որ հարթակներում է օգտագործվել տվյալ էլեկտրոնային փոստը:

Կարելի է փոստի հասցեի որոնում իրականացնել՝ օգտագործելով չակերտները: Օրինակ՝ andznavorutyun@example.com:

Գործնականում մասնակիցները կփորձեն պետական-պաշտոնական էլ. փոստերի հասցեները որոնել սոցիալական ցանցերի օգտատերեր գտնելու համար:

Թեմա 13. Աշխատանք բաց տվյալների հետ

Այս բաժնում պաշտոնյաները կծանոթանան և կսովորեն աշխատել բազմաթիվ բաց տվյալների բազաներով: Կկարողանան վերլուծել և «խոսեցնել» թվերն ու փաստերը: Մասնավորապես կծանոթանան առցանց դատական բազաներին, կսովորեն կարդալ ու հասկանալ գույքի և եկամուտների հայտարարագրերը, ընտրողների ռեզիստրը:

Դասավանդողը պետք է ներկայացնի հայաստանյան մի շարք բաց տվյալների շտեմարաններ, որոնցում կարելի է նույնականացնել մարդկանց ու նրանց հասցեները (elections.am), ստուգել նրանց անունով գրանցված ընկերությունները (e-register.am), նրանց մասնակցությամբ դատական գործերի առկայությունը (datalex.am), գույքի ու եկամուտների հայտարարագրերը, եթե ներկա կամ նախկին պաշտոնյաներ են (cpcarmenia.am): Այս թեմայի շրջանակում մասնակիցները պետք է ծանոթանան նաև ՀՀ վիճակագրական կոմիտեի armstat.am կայքին, կարողանան ճիշտ կարդալ վիճակագրությունները:

Թեմա 14. Խորացված որոնում

Այս բաժնում անհրաժեշտ է պաշտոնյաներին պրակտիկ գիտելիք տալ որոնողական համակարգերի միջոցով աղբյուրներն ուսումնասիրելու վերաբերյալ: Անհրաժեշտ է պատկերացում տալ Google, YouTube, Yandex, Bing, WolframAlpha որոնողական համակարգերի, դրանց հատուկ օպերատորների և խորացված որոնման սկզբունքների մասին:

Այս թեման նաև ենթադրում է ջնջված տեղեկատվությունը և դրա հետքերը փնտրելու կարողությունների փոխանցում, մասնավորապես՝ Google-ի արխիվացված որոնումների

Էջերից և ինտերնետային արխիվից <https://archive.org/web/> օգտվելու կարողությունները: Պաշտոնյաները կտվորեն նաև անձամբ որոշակի տվյալներ արխիվացնելու ձևերը:

Թեմա 15. Տեղեկատվական անվտանգություն

Այս բաժնում անհրաժեշտ է պաշտոնյաներին փոխանցել պրակտիկ գիտելիք տեղեկատվական անվտանգության կանոնների վերաբերյալ: Նրանք կիրառելով տեղեկատվական անվտանգության հիմնական սկզբունքների մասին ու կկարողանան դրանք կիրառել իրենց ամենօրյա աշխատանքում:

Ցանկացած տվյալ, որն ունի առևտրային, պետական, հանրային կամ անձնական արժեք, պետք է պահպանվի, հաղորդվի ու մշակվի տեղեկատվության անվտանգության սկզբունքներին համապատասխան: Այդ սկզբունքներն են.

1. Խորհրդապահությունը,
2. Ամբողջականությունը,
3. Հասանելիությունը:

Ցանկացած տեղեկատվական համակարգ մշակելիս, ինչպես նաև արդեն գոյություն ունեցող համակարգերի անվտանգության կանոնները մշակելիս այդ սկզբունքները պետք է հաշվի առնվեն և կիրառվեն համակարգի/կանոնների ցանկացած մասում կամ բաղադրիչում: Նման մոտեցումը կոչվում է «անվտանգությունը որպես նախագծման մաս» (security by design): Այս բաժինն ուսանելիս պաշտոնյաները կպատկերացնեն, որ ցանկացած տեղեկատվական համակարգ պետք է լինի անվտանգ և ապահովված լինի անվտանգության ապահովման մեխանիզմներով, ինչպես նաև ինչպես իրականացնել դրա անվտանգության պարբերական գնահատումը: Սա հատկապես վերաբերում է կրիտիկական ենթակառուցվածքներ սպասարկող պետական կառավարման համակարգերին:

Մասնակիցները նաև կծանոթանան երեք հատվածների՝ ցանցային, սարքավորումների և անձնական (օգտատիրոջ) հատվածի անվտանգության ապահովման միջոցներին:

Օրինակ անձնական անվտանգության ապահովման միջոցներից են գաղտնաբառը, անհատի իրազեկ լինելը հնարավոր վտանգների մասին, համացանցից օգտվելու հիմնական կանոնները և առհասարակ համակարգչային տեխնիկայի անվտանգության կանոնները:

Կայանային (սարքավորման) կանոնները ներառում են հակավիրուսային ծրագրերի պատշաճ տեղադրումը և շահագործումը, անվտանգության բացերի կանոնավոր փակելը (patching), պահուստային կրկնօրինակների ապահովումը:

Ցանցային անվտանգության կարող է ներառել ֆայերվոլներ, մասնավոր վիրտուալ ցանցեր օգտագործելը (VPN), ապառազմական գոտիներն (DMZ) ու անլար ցանցերից օգտվելու կանոնները (Wi-Fi policies).

Ուսուցման ընթացքում առանձին անդրադարձ կկատարվի հաղորդակցության կանոններին: Կանոնները պետք է սահմանեն անձնական տվյալներ, ինչպես նաև ցանկացած խորհրդապահական տեղեկություններ հաղորդելու պահանջները, ինչպիսիք են, օրինակ, գաղտնագրումը կամ նյութական կրիչների պահպանության ապահովման միջոցները:

Օգտակար հղումներ

1. Մեդիագրագիտություն՝ ձեռնարկ - <https://media.am/hy/lab/2020/04/16/17917/>
2. Փաստերի ստուգումը և լրագրողների տեղեկություն ստանալու իրավունքը ՁԵՌՆԱԸԿ - <http://factradar.tilda.ws/>
3. Տեղեկությունների ստուգում. բուհական դասընթացի մեթոդական ուղեցույց - <https://media.am/hy/lab/2019/02/09/11015/>
4. «Լրագրության հինգ կարևոր հարցերը», հանրային լրագրության ակումբ - <http://media.am/pjc-5-W>
5. Allan Bell, The language of News Media, Մուլտիմեդիա հավելված
6. Անվճար նյութեր ուսուցիչների համար - <http://www.medialiteracy.com/freestuff.htm>
7. Media and information literacy curriculum for teachers - <https://unesdoc.unesco.org/ark:/48223/pf0000192971>
8. Google-ի պատկերների որոնման համակարգ - <https://images.google.com>
9. Bing-ի պատկերների որոնման համակարգ - <https://www.bing.com/images/>
10. Yandex-ի պատկերների որոնման համակարգ - <https://yandex.ru/images/>
11. Պատկերների մասնագիտացված որոնման համակարգ - <https://www.tineye.com>
12. Պատկերների մետատվյալների ուսումնասիրման համակարգ - <http://exif.regex.info/exif.cgi>
13. Պատկերների մետատվյալների ուսումնասիրման համակարգ - <http://metapicz.com>
14. Google-ի քարտեզների ընդլայնված գործիք - <https://www.google.com/earth/>
15. Here Maps քարտեզագրման համակարգ - <https://wego.here.com>

16. Bing-ի քարտեզագրման համակարգ - <https://www.bing.com/maps/>
17. «EOS» քարտեզագրման համակարգը - <https://eos.com/landviewer/>
18. Կայքերի մասնագիտացված ուսումնասիրման համակարգ - <https://urlscan.io>
19. Էլեկտրոնային փոստի հասցեի ուսումնասիրման համակարգ - <https://www.emailsherlock.com>
20. Ինտերնետային արխիվ - <https://archive.org/web>