1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 7: Криптографија пријатељ или непријатељ

Доминантна дисциплина	« Филозофска радионица »
Резиме	Ученици учествују у « филозофској радионици » посвећеној актуелним утицајима криптографије. Да ли ангажовати осигуравајућу агенцију? Да ли тиме угрожавамо нашу приватност?
Појмови	« Друштвени утицаји » • Дебта о криптографији је присутна у бројним земљама. • Коришћење криптографије је проблематично за бројне владе које желе да надзиру комуникације из разлога сигурности. • Недавна масовна прислушкивања су узнемирила грађане у вези њихове приватности. • Сигурност и поверљивост комуникација су у основи функционисања наше економије.
Матријал	За одељење: • Припремљена основна литертура За сваког ученика: • Радни лист-B10

Припрема за филозофску радионицу

Наставник организује овај час у форми « филозофске радионице ».
Идеално би било да учествује и наставник-библиотекар задужен за помоћ у претрази литературе. Његова позиција би могла да помогне при изношењу и поштовању других идеја потеклих од учесника радионице. Циљ једне овакве радионице није постизање свеукупне сагласности и адаптције неког закључка него развој става код ученика у вези комплексности дилема с којим се суочавају савремена друштва и пружање помоћи при формирању неког аргументованог става.

Педагошке напомене

- Постоје различити методи вођења филозофске радионице у одељењу. Метод вођења ове радионице је инспирисан методом AGSAS-Lévine© која је предствљена делу *L'enfant philosophe, avenir de l'humanité?(Дете филозоф, будућност човечанства?,п.п.)* аутора Jacques Lévine у издању ESF Éditeur.
- Два наставника ће, као припрему овог часа, одабрати неколико чланака, пре свега из дневних листова, који ће се користити у другој етапи часа. Извора има доста, на пример у 2015, је David Cameron (*тада премијер Веике Британије, п.п)* предложио забрану шифрирања у Енглеској. Исте године је у Француској је изгласан закон по коме су све фирме које се баве снабдевањем комуникационог шифрирања обавезне да влади, на њен захтев, проследе кључеве дешифрирања.

Организација учионице мора бити прилгођена овој радионици:

- Столице постављене у круг, клупе су у углу.
- Ученици заузимају тако постављене столице.
- Наставници су ван круга и не реагују током рада радионице.

Подсећање на правила « филозофске радионице »

Наставник, независно од тога да ли су ученици већ учествовали у радионици овог типа, објашњава правила инхерентна « филозофској радионици »:

- Наставник најављује тему радионице а сваки учесник има по минут времена да формира своје мишљење по овом питању. Затим, ученици имају на располагању 10 минута за изношење свог става о овој теми, а професр у том периоду не узима реч. Излагања се региструју (без навођења имена оног ко је говорио), а затим у оквиру « филозофске радионице » шаљу сваком учеснику.
- Ученици су слободни да кажу све што им падне на памет, покушавајући да имају свој став о теми о којој се расправља. Нема добрих и лоших одговора. Јер, « филозофска радиоица » омогућује да комуницирате сами са собом, али и да пратите индивидулни и колективни ток мисли.
- Учесник узима реч само кад до њега стигне штапић који му даје могућност да говори « bâton de parole ». Тај штапић иде из руке у руку али није обавезно да кад дође до вас ви и узмете реч. Ако ученик мисли да нема шта да каже само га проследи даље свом суседу.
- Основно правило је да се поштује мишљење других. Имамо право да се не слажемо с неким, али немамо право да га исмејавамо или да се осврћемо на оно што је рекао, поготову је забрањена свака вулгарност. Морамо да саслушамо друге.

Наставник, пошто обзнани ова правила, пита ученике да ли су спремни да их поштују, и ако их неко од ученика не прихвата он и неће моћи да учествује у раду радионице.

Реализација радионице

Наставник дефинише тему: *да ли сваком дозволити употребу оруђа за криптографију?*
Док ученици размишљају укључује се регистратор тона. Наставник пита ко жели да почне да прича и даје му « штапић », затим се повлачи из простора за разговор.
Штапић може да да и насумично изабраном ученику.
Штапић иде из руке у руку. Свако излаже, ако жели, док му не истекне предвиђео време.

Наставник, после 10 минута, пита да и су сви рекли што су желели или има још неко да то учини, а затим се неко ако жели осврне на дебату која је вођена: квалитет слушања, интерес за оно што је формулисано, итд.

У наставаку: преиспитивање аргумената дебате у вези умрежених објеката

Наставник се, пошто је радионица завршена, враћа у центар круга и предлаже ученицима да саслушају оно што је регистровано.
Предлаже ученицима да прочитају неколико унапред одабраних докумената (исечци из новина, педагошка напомена са почетка часа …).
Наводимо неколико најчешће помињаних аргумената за или против који су се издвојили у дебати о криптогафији и надзору.

Аргументи за забрану (или ограничење) оруђа криптографије:

- Превенција тероризма: сигурносне агенције имају потребу да прате e- mail-ове, sms, телефонске позиве… лица сумњичених за могуће терористичке акције, и да на тај начин спрече те активности и нађу могуће налогодавце.
- Забрана криминалних мрежа: посредством интернета су организоване бројне криминалне активности попут педофилије и продаје оружија, дроге, људи,.. Надзирање комуникација овог типа омогућује елеиминисање оваквих мрежа.
- Закони неких земаља предвиђају могући компромис ауторизацијом криптографије али и обавезом агенција које се њоме баве (на пример агенција за понуду јавних и приватних кључева) да дају сва неопходна обавештења владиним сигурносним агенцијама.
- « Они који немају шта да сакрију немају ни потребу да криптују своје информације ».

Аргументи за легализацију (охрабрујући) бројних оруђа за криптографију:

- Терористичке и криминалне мреже већ користе оруђа за криптографију али и за заштиту својих комуникација. Забраном доступности ових оруђа ширем кругу корисника се сматра ограничењем људских слобода и умањењем ефикасности борбе против криминала.
- Анализа информатичког саобраћаја омогућује да се добију бројна обавештења захваљући метаподацима (сазнање ко с ким комуницира, кад, колико времена, итд.) а да при томе нема потребе да се сазна и садржај порука.
- Криптографија је једини начин којим је могуће гарантовати поштовање наше приватности у епохи у којој се сви наши лични подаци преносе информатичким серверима. Европска конвенција о праву човека препознаје и поштовање права приватности комуникација.
- Развој трговине, и успешно економско функционисање је могуће ако се очува поверљивост личних и предузетничких комуникација. Јер без криптографије би свима могле да буду пиратиране банарске картице, узурпира идентите као и да се добију обавештења (или новац) уместо неког другог.
- Бројне професије(новинари, адвокати, лекари, комерцијалисти, …) морају да чувају професионалне тајне па тиме и да криптују своје податке на начин да се избегне вулгаризација поверљивих информација на интернету или у штампи.

Закључак

Независно од става сваког појединца, на крају овог часа, по питању слободе шифрирања или њене забране (или пак неког средњег решења које би се састојало у ограничењу у неком оквиру), ученици и наставници дискутују о начину који би им омогућио да заштите своје личне податке.

Дискусија може да се води уз помоћ неког документа попут овог који је развила *Национална комисија за инфораматику и слободе - CNIL* (посебно прилагођено за адолесценте) а дат је Радном листу-B10.
