Hedayah
countering violent extremism

Project funded by the
EUROPEAN UNION

Passage4prevent:

Употреба на образованието во спречување на онлајн радикализација кај младите

Спречување на онлајн радикализација: Кон образовна политика за онлајн безбедност

Марија Ристеска, Методи Хаџи-Јанев и Самет Шабани

CRPM Center for Research and Policy Making
... policy impact since 2004

Cyber Security, Corporate Security and Crisis Management Initiative

Скопје, 2021

Hedayah
countering violent extremism

Project funded by the EUROPEAN UNION

Оваа публикација беше изготвена во рамките на проектот „Премин кон превенција: употреба на образованието во спречување на онлајн радикализација кај младите“

Passage4prevent:
Употреба на образованието во спречување на онлајн радикализација кај младите

За издавачот: Центар за истражување и креирање политики – ЦИКП Скопје

Автори: Марија Ристеска
Методи Хаџи-Јанев
Самет Шабани

Дизајн: Омни Груп

Оваа публикација беше изготвена со финансиска поддршка од Европската Унија. Содржината е единствена одговорност на Центарот за истражување и креирање политики и на ниту еден начин не ги одразува ставовите на ЕУ или на Хедаја

Скопје, 2021

Содржина

Извршно резиме

Дигитализацијата на образованието е процес којшто е во тек со децении, а кризата предизвикана од вирусот ковид-19 само го забрза темпото, ставајќи ја онлајн безбедноста во образованието како приоритетна реформска тема за секоја земја. Северна Македонија се соочува со онлајн радикализација како ризик надополнет и со отсуство на рамка за јавни политики којашто се занимава со прашања поврзани со онлајн безбедноста во училиштата. Ова го прави главното прашање од интерес во овој труд, спречување на онлајн радикализацијата преку образовни политики за онлајн безбедност, апсолутна неопходност за креаторите на образовните политики.

Трудот има цел да даде придонес кон дебатата за воведување образовна политика за онлајн безбедност. За таа цел, прво се претставува проблемот – онлајн радикализацијата и факторите што придонесуваат кон проблемот, поврзувајќи го со докази за тоа колку се раширени овие фактори кај средношколците од Скопје, Тетово, Гостивар, Велес, Куманово и Штип. Второ, трудот ги анализира политиките за сајбер безбедност, едукација и превенција од рамката на политика за насилен екстремизам и како овие рамки реагираат на ситуацијата, ублажувајќи ја ранливоста на средношколците при изложеност на фактори кои придонесуваат за феноменот на онлајн радикализација. Потоа, документот за јавни политики го презентира решението што се предлага да биде на повеќе нивоа, опфаќајќи: законодавна реакција, реакција преку јавни политики на ниво на училиште и градење капацитети, како и зголемување на свесноста на учениците, наставниците и родителите. Конечно, документот за јавни политики препорачува неколку алатки што можат да се прилагодат на потребите на образовните институции и заедниците за да обезбедат соодветни политики за онлајн безбедност што ќе спречат онлајн радикализација.

Вовед

Интернетот, особено социјалните медиуми, се користи како канал не само за промовирање и ангажирање, туку и како командна структура за радикализација што може да доведе до насилен екстремизам. Честопати оваа промоција го велича насилството, привлекувајќи и влијаејќи врз многу луѓе, вклучително и деца, и во екстремни случаи ги радикализира. Исто така, се јавува уште еден тренд кој го промовира страдањето, а што ја активира емпатијата и персонификацијата со каузата (особено кај жените), кој на крајот може да доведе до прифаќање на радикално однесување за постигнување одредени цели.

Донесувањето стратегија за онлајн безбедност во образованието треба да биде приоритет за секоја земја, имајќи предвид дека младите го поминуваат поголемиот дел од своето време во училиштата. Оттаму земјите што имале искуство со феноменот на странските борци, дури треба да им дадат и приоритет на напорите за поставување на стандарди за онлајн безбедност, градење капацитети и континуирано подигнување на свеста.

Овој документ за јавни политики има цел да даде придонес кон развојот на образовна политика за онлајн безбедност. Документот е развиен со примена на повеќе методи: (i) истражување од биро, (ii) интервјуа лице в лице со клучни засегнати страни кои за целите на трудот остануваат анонимни и (iii) примарни наоди од податоците од студијата за основна проценка на состојбата на Центарот за истражување и креирање политики - ЦИКП за употребата на образованието во спречување на онлајн радикализација кај младите[1].

Документот за јавни политики ја следи методологијата на решавање на проблеми. Прво, се претставува проблемот - онлајн радикализација и нејзиниот обем во Северна Македонија - потоа се дава анализа на јавните политики за тоа како се справува со овој проблем. Како заклучок, трудот нуди препораки за тоа како образовната политика и училишната политика можат да се подобрат за да се реши проблемот.

[1] Истражувањето беше спроведено од февруари до март 2020 во општините Куманово, Штип, Велес, Тетово, Гостивар и Град Скопје, на репрезентативен примерок од 756 средношколци.

Зошто фокус на онлајн безбедност?

Околу 250.000 ученици од март 2020 следат онлајн настава, што придонесува кон растечкиот тренд на користење интернет од страна на младите во РС Македонија (оттука натаму Македонија), што според Државниот завод за статистика изнесува 99,5% од младите на возраст помеѓу 15 и 24 години во 2019[2]. Адолесценцијата е време кое се карактеризира со идеализам, со тенденција кон сè или ништо размислување. Понатаму, тие минуваат околу 6 часа на ден на интернет, најмногу на социјалните мрежи и гледање видеа[3].

Средношколците се многу зависни од своите соученици за чувството на благосостојба, имајќи потреба да се чувствуваат како дел од група, но и да бидат доживувани како уникатни, а нивната валута се лајкови и рејтинзи. Основната студија на ЦИКП **„Премин кон превенција: употреба на образованието за спречување на онлајн радикализација меѓу младите“** дава дополнителни наоди за средношколците во Гостивар, Куманово, Скопје, Штип, Тетово и Велес, забележувајќи дека 99% од учениците имаат пристап до интернет во нивните домови, од кои 85% рекле дека имаат пристап во секое време, но и дека во 74,4% од домовите нема правила за користење на интернетот. Скоро половина од учениците би прифатиле родителска контрола (44,1%), додека повеќе од половината (55,9%) од учениците мислат дека родителски надзор или контрола е неопходна.

Училиштата, од друга страна, немаат политики за безбедно користење на интернетот и не вклучуваат во наставната програмата образование и подигање на свесноста за приватноста и прашањата за сајбер безбедност. Ова резултира со тоа 26,4% од средношколците понекогаш да ги споделуваат нивните кориснички имиња и лозинки со нивните пријатели и 33,8% да користат опцијата за автоматско зачувување на нивните профили на интернет-пребарувачите. Понатаму, 10% од испитаните средношколци рекле дека не се

[2] Државен завод за статистика достапна на: http://makstat.stat.gov.mk/PXWeb/pxweb/en/MakStat/MakStat__InfOpstestvo__DomakinstvaPoedinci/325_InfOpst_Mk_050_Int3mLica_mk.px/table/tableViewLayout2/?rxid=01468531-a0c4-42ac-8159-fb98946968f2

[3] Студија за младите во Северна Македонија 2018/2019, Фридрих Еберт Фондација, стр.16 достапна на: http://library.fes.de/pdf-files/id-moe/15266.pdf

чувствуваат безбедно онлајн, а 8,5% имале и непријатно лично искуство на интернет.

Имајќи предвид дека земјата го искуси процесот на радикализација на млади, коешто беше особено видливо за време на конфликтот во Сирија преку феноменот на „странски терористички борци“ (повеќе од 140 борци), главно од Скопје (Чаир, Гази Баба), Куманово, Липково, Тетово и тековниот процес за нивно враќање во земјата (83 лица беа вратени и судени според член 322а од Кривичниот законик којшто беше воведен во 2014, како и други 23 лица коишто не беа судени бидејќи нивното враќање се случи пред измените во Законот и криминализацијата на делата за мобилизирање и служење во странски војски.) Останатите странски борци и нивните семејства се очекува да бидат вратени наскоро, за што Владата усвои Национален акциски план за рехабилитација, ресоцијализација и реинтеграција на странските борци и нивните семејства. Дополнително, меѓуетничките односи меѓу заедниците продолжуваат да бидат тензични особено во деловите од државата каде што екстремистичките групи сè уште се присутни и активни, а коишто се спремни да користат насилство за постигнување на целите. Некои од овие процеси се случуваат онлајн, заради што напорите на Муншот (Moonshot) за спречување на насилен екстремизам (CHE) да одговорат на зголемениот тренд на онлајн радикализација дефинираат сеопфатна онлајн и офлајн кампања за спречување на пораките на меѓународните терористи и насилно екстремистичките организации во земјата, а во исто време делуваат кон спречување на ризиците од екстремни пораки преку активности кои ги таргетираат двигателите коишто придонесуваат кон овие ризици, особено помеѓу младите[4]. Меѓутоа, потребни се посеопфатна стратегија и политики за мониторирање, контрола, превенција и промоција на практики за онлајн безбедност.

[4] Борба против регрутацијата од страна на насилно-екстремистичките организации во Грузија, Азербејџан и Македонија достапно на: е: https://www.phint.org/program/242

Како функционира онлајн радикализацијата?

Зголеменото време поминато на интернет значи дека на децата постојано им се претставуваат морални и етички избори како произведувачи и консументи на содржина (Дај, 2016) и веќе се активни носители на одлуки во процесот. Во Македонија, иако странските борци се во затвор бидејќи се криминализираа нивните активности, постојат докази дека тие сè уште се активни на интернет и дека нивните фејсбук-страници се многу популарни помеѓу младите. Поради тоа средношколците се соочени со најголеми ризици, а им недостигаат вештини, стратегија за справување и отпорност за справување. Ако тие не се обучени, нивната ранливост (онлајн ранливоста генерално се објаснува преку слични фактори како оние кои придонесуваат за офлајн ранливост и ризик) нема да се промени.

Општо прифатен аргумент е дека современите технологии, како што се интернетот и онлајн апликациите за комуникација, се нож со две острици. Овие технологии нудат многу предности, но исто така и воведуваат многу ризици. Државните и недржавните чинители ја злоупотребуваат оваа технологија за да ги остварат нивните цели замаглувајќи ја линијата помеѓу предностите и ризиците кои навлегуваат во границите на индивидуалната безбедност и сигурност (емоционална/психолошка, економска) - преку употреба на сајбер просторот од страна на терористички организации на една страна и државните безбедносни агенции од друга страна. Поради тоа алатките

и медиумите коишто ја обезбедуваат удобноста и благосостојбата на нашето општество стануваат канал на закани.

Напорите за градење на дигитална отпорност имаат цел да ја зајакнат способноста на децата точно да ги идентификуваат и да ги интерпретираат влијанието и последиците од различни ризици од радикализација и да развијат и технички и емоционални вештини за да се справат со екстремистичката пропаганда и регрутацијата. Затоа потребно е да се гради знаење и свесност кај средношколците за онлајн ризиците без притоа да се фокусираме на специфичен и непосреден ризик. Вандомник, д'Хенес и Смахел (2014) заклучуваат дека кога децата се чувствуваат поспособни за справување со ризик, тие веројатно помалку ќе се плашат или ќе бидат загрижени за ризикот. Преку помагање на децата да станат посамоуверени и вешти корисници на интернетот, вклучително и способноста да се соочат и да се справат со онлајн ризиците, тие ќе бидат отворени за уште повеќе можности без да има потреба да бидат ограничени од рестриктивни стратегии за медијација.

Радикализацијата може да произлезе од:

- Политички цели (на пример: промена на формата на владеење, како укинување на демократскиот систем со избори како што имаме сега и воведување диктатура)
- Социјални цели (на пример: кога фанови на спортски клуб настојуваат да направат промена или да постигнат цел – да убедат фанови од други клубови да навиваат за нивниот клуб)
- Религиозни цели (на пример: кога членови на една религија сакаат да наметнат промена којашто ќе ја направи нивната религија доминантна и ексклузивна).

Процесот на онлајн индоктринација често се јавува преку конверзација (чатови), убедување, влијание, наклонетост или предавања организирани во затворени и изолирани групи, форуми, посебни соби. Собрани преку онлајн весници, блогови, услуги и чат-соби, учесниците влегуваат во форумите каде што екстремистичката идеологија се самозајакнува (Шан и Филипс, 2011, с.24) .

Процесот на онлајн насилна радикализација преку сајбер просторот во нашата држава, како и секаде, варира. Имајќи предвид дека овој процес е скроен според личноста (целта, таргетот), може да следи специфични правила и динамика. Онлајн насилната радикализација на интернет и

социјалните медиуми се јавува преку регрутација и индоктринација[5]. Во текот на процесот на регрутација оние коишто радикализираат, пробуваат да привлечат и во крајна линија да изолираат поединец (или група) за поединецот да може да се приврзе, употребувајќи политички и/или социоекономски непогоди како отскочна штица за мобилизација кон промена преку употреба на насилни средства.

Насилната онлајн радикализација обично почнува преку селекција којашто може да биде таргетирана и организирана или, пак, може да биде спонтана, т.е. самоселекција кога некој е селектиран преку неговото/нејзиното однесување[6], употребувајќи современи технологии и прилагодено општествено однесување (т.е. со леснотија да употребуваш современи комуникациски технологии и апликации како конвенционалните комуникации во физичкиот свет)[7]. За оваа цел (селекција), некои од добро организираните малициозни групи и индивидуалци имаат изработени методологија за профилирање. Со скенирање на онлајн активностите, собирајќи и обработувајќи податоци (анализирајќи го однесувањето на целта/таргетот), овие групи или индивидуалци почнуваат процес на селекција. Постојат повеќе начини преку кои малициозни групи и индивидуалци можат да собираат лични податоци за младите на интернет:

- Лични податоци на која било платформа (Фејсбук, Твитер, Инстаграм, Јутјуб) за комуникации и видеоцели. Тие можат да проучуваат лични навики, навики за купување, желби, хобија и инфлуенсери, места и страници од интерес на таргетираната личност и да ги идентификуваат неговите/нејзините ранливи места. Пристапот за собирање на оваа количина податоци може да биде или преку искористување на слабата заштита на профилите на луѓето или преку праќање на случајни покани за пријателства на Фејсбук. Други методи за идентификација на поединци ранливи

[5] UNESCO Background note Social media and youth radicalization in digital age, достапно онлајн: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/background_social_media_radicalization.pdf

[6] Методи Хаџи Јанев, Митко Богдановски (2020) „Кон безбедна и сигурна младина онлајн: Прифаќање на концептот на медиумска и информациска писменост'' , Конрад Аденауер Фондација

[7] Види на пример: Postmes Tom & Brunsting Suzanne, (2002), "Collective action in the age of internet: Mass-communication and online mobilization", Social Science Computer Review, 20, 290-301, available at: https://journals.sagepub.com/doi/10.1177/089443930202000306

на екстремистички идеи може да вклучуваат одредени хаштагови на објавите на социјалните медиуми итн.

- Собирање информации преку веб-страници и форуми за чат. Многу често луѓето со малициозни намери имаат добро организирани веб-страници коишто се атрактивни и наполнети со содржина наменети за одредени индивидуалци и групи коишто многу веројатно ќе ја прегледаат содржината[8]. Информациите на овие страници може да бидат точни, делумно точни или целосно неточни[9]. Веб-страниците или форумите за чат може, а и не мора да се поврзани со содржината што е крајната цел. Овие страници често содржат содржина којашто е подготвена однапред да ја тестира потенцијалната жртва[10]. Собирачите знаат како да ги измерат поединечните реакции на одредена содржина и да направат стратегија за придување на идентификуваната жртва врз основа на ова.
- Собирање информации преку гледање видеосодржина. Како и со другите техники за следење на однесувањето, онлајн регрутерите можат да ја искористат историјата на прелистување на некоја личност за да соберат податоци. Повеќето платформи имаат соодветни алгоритми - програми што избираат што гледате на нив. На некои платформи, објавените видеа имаат список на индивидуални прегледи, со пристап до профилите на гледачите. Може многу лесно да се забележат ако гледаат видеа што имаат содржина наменета да ги намамат новите претплатници кон одреден идеолошки светоглед кој повикува на насилство. Иако се добронамерни, некои карактеристики на социјалните апликации ги користат терористичките организации, како што се упатствата на YouTube за тоа како да дизајнирате видео засновано врз профилот/навиките на посакуваните гледачи или следбеници. За

[8] Weimann Gabriel, (2015) "Terrorism in Cyberspace: The Next Generation", New York, NY: Columbia University Press/Washington, DC: Woodrow Wilson Center Press, ISBN: 978-0-231704496.

[9] Неколку независни истражувања го потврдуваат ова, види на пример: Brachman Jarret and Levine Alex, (April 13, 2011), "The World of Holy Warcraft", Foreign Policy, достапно на: http://foreignpolicy.com/2011/04/13/the-world-ofholy-warcraft/; или: Behr Ines Von, Reding Anaïs, Edwards Charlie & Gribbon Luke, (2013); или: Sageman Martin, (2008), "Leaderless Jihad", University of Pennsylvania Press

[10] Busher Joel (2015), "What part do social networks play in radicalisation?", Radicalization Research, available at: http://www.radicalisationresearch.org/debate/busher-social-networks/

регрутерите е многу лесно да го злоупотребат овој метод за свои цели[11].

- Игри. Игрите се уште еден начин на кој онлајн менторите кои се радикални и бараат нови следбеници можат да пристапат до лични информации. Современите видеоигри и апликации за играње овозможуваат комуникација во специјално дизајнирана соба за разговор од еден играч до друг и како такви создаваат совршена можност за предаторите. На пример: криење зад карактер на игра за генерирање дискусија во форма на говор на омраза, што пак може лесно да се искористи како форма на агресија против групи/поединци од физичкиот свет[12]. Според некои статистички податоци, младите во нашата земја претпочитаат да играат на интернет, а 38% користат интернет за играње и преземање игри, што е далеку над европскиот просек од 34%[13]

Основната студија за проценка на состојбата на ЦИКП „Премин кон превенција: употреба на образованието за спречување на онлајн радикализација кај младите " открива дека над половина од испитаните средношколци многу често имаат пристап до содржини со тролање, малтретирање и навреди (52,7%), проследени со насилна содржина што е хумористично портретирана (47,7%) или содржина што покажува физички напад, палење и тепање (39,9%) и говор на омраза што директно ги охрабрува луѓето да се однесуваат насилно или да извршат дело насилство (39,2%). Интересно, над 20% од анкетираните студенти потврдија дека овој вид насилна интернет-содржина ја споделуваат најмалку половина од нивните пријатели. Ова сугерира на широка распространетост на насилна содржина на интернет и високо ниво на изложеност на младите на насилство. Сепак, дали постои ризик од користење на оваа содржина за радикализирање и прифаќање на насилни екстремистички идеи, треба дополнително да се истражи.

[11] Види повеќе на YouTube Creator Academy, достапно на: https://creatoracademy.youtube.com/page/lesson/discoverability-analytics

[12] Selepak, Andrew, (2010), "Skinhead Super Mario Brothers: An Examination of Racist and Violent Games on White Supremacist Web Sites" Journal of Criminal Justice & Popular Culture, 17(1), 1-47, достапно на: https://www.semanticscholar.org/paper/Skinhead-Super-Mario-Brothers%3A-An-Examination-of-on-Selepak/581e60a66b63bd58853d9cffb9304fb81f25314e

[13] Игор Петровски, (Јуни 29, 2018), „Младите и интернетот", Капитал

Откако предаторите ќе пронајдат цел што користи каква било комуникација на социјалните медиуми (Фејсбук, Твитер, Инстаграм, Снепчет, Јутјуб, итн.) на интернет, тие преминуваат во следната фаза од регрутирањето: пристап и изолација. Првичната комуникација обично е во насока на поддржување на огорченоста на жртвата за да се придобие нејзината доверба[14]. Ова значи дека „лицето“ и „групата“ можат да воспостават посебни онлајн врски поради наводно слични интереси, навики, искуства, ставови, мислења и однесувања.

Голем дел од овие наводни сличности се претходно поставени и прилагодени врз основа на процесот на профилирање. Почесто, во овој период добро организирани претставници на малициозни групи се претставуваат како членови кои споделуваат слични ставови со жртвата и на тој начин потајно инвестираат во градење доверба во „просторијата“ (соба за разговор). Крајната цел во оваа фаза е да се создаде врска. За таа цел, тие создаваат затворени простории за разговор. Оттука започнува изолацијата.

За да напредува и да создаде понатамошна изолација, жртвата може да добие ексклузивна понуда. На пример: може да ѝ бидат понудени одредени привилегии, т.е. да станете член на „специјалните/одбраните“.[15] Друг метод за изолација на таргетот може да биде влез со препорака во избрани или специјални групи каде што се појавуваат сите „жешки теми“. Разговорите се подготвени претходно и обично може да вклучуваат теми како што се: немири, промена на системот и говор на омраза против оние кои се различни.

Општо земено, затворените групи имаат правила засновани врз принципот „само за членови“. Целта во оваа фаза е да се создаде чувство на припадност и жртвата да се чувствува рамноправна со другите. Стекнатата доверба може да вклучува и компензација. Од лице (жртва на насилна онлајн радикализација) може да биде побарана услуга (да стори нешто) за која ќе биде наградено. Откако ќе

[14] Weimann Gabriel, (2015)
[15] Weimann, Gabriel, (2010), “Terror on Facebook, Twitter, and Youtube”, Brown Journal of World Affairs, 16(2), 45-54, достапно на: http://bjwa.brown.edu/16-2/terror-on-facebook-twitter-and-youtube/

се добие довербата, започнува процесот на градење заеднички идентитет (индоктринација).[16]

За време на фазата на индоктринација, одредени формулации и фрази доминираат во изолираните простории за разговор за да поттикнат општ став за конкретни прашања. Нема правило за тоа колку време поминува од процесот на селекција до индоктринација. Може да биде долг процес, но може да се случи и многу брзо. Овој процес се прави преку манипулација - верување дека нешто што треба да се промени, мора да се направи дури и ако тоа повлекува употреба на насилство. Манипулацијата има цел да произведе изобличување и злоупотреба на

Основната студија за проценка на состојбата на ЦИКП „Премин кон превенција: употреба на образование за спречување на онлајн радикализација меѓу младите“ открива дека 44% од испитаниците добиваат насилна содржина преку лични пораки (сандаче) или во простории за разговор (chat rooms). Понатаму, 37% од средношколците, испитаниците во истражувањето на ЦИКП изјавиле дека овие видови насилна содржина се споделуваат и преку креирани групи за споделување. Ова сугерира дека инфраструктурата и моделот на однесување што се користат при онлајн радикализација (изолација и индоктринација) се практикуваат и се нормализираат кај голем број средношколци, што претставува ризик за можна онлајн радикализација.

[16] Овој процес некои го нарекуваат „спојување на идентитетот“ , види: Swann William Jr. & Buhrmester D, Michael (2015), “Identity Fusion”, Psychological Science, Vol. 24(1) 52–57, достапно на: https://labs.la.utexas.edu/swann/files/2016/03/52-57.pdf

убедувањата, политичките идеологии и етничките и културните разлики (привлекување едноставни глобални ставови што го делат светот на „нас наспроти нив“), со што ги поттикнуваат жртвите да бараат одговори[17]. Фразите како „нас“, „ние“, „заедно“ и „наши“ се користат за зајакнување на припадност, компензација за несреќи и трагедии и охрабрување на прилагодено однесување преку нанесена лојалност и потрага по „возбуда и авантура“ и „моќ и контрола“ - заменување на реалното со виртуелниот свет[18]. Врз основа на профилирање во изолираната група за време на процесот на индоктринација, целите можат да се изразат, да се чувствуваат емотивно пријатно и заштитени. Овие групи создаваат круг на доверба и кога жртвата се чувствува безбедно, тогаш индивидуата е подготвена да биде всадена во однесувањето што претходно беше сфатено како погрешно, забрането или чудно[19]. Прибегнувањето кон насилство честопати станува морално оправдување наспроти сите ситуации што ја стават жртвата на спротивниот пол од поларизираниот спектар во општеството.

Врз основа на испитување на 150 написи, од кои само 18 беа емпириски изведени студии, РАНД ја идентификуваше куќата за производство на медиуми на Ал-Каеда, Ас-Сахаб Фондација за објавување на исламски медиуми и нивните веб-страници како таков извор. Саморадикализацијата може да се случи и кога случајна жртва чита литература, форуми и блогови од сомнителни извори или емитува видеа, аудиозаписи или песни со содржина што имаат цел насилно радикализирање.

Практиката покажува дека целиот процес опишан погоре може да се случи и преку „само-радикализација“.[20] Како што споменавме, претходно подготвените манипулативни веб-страници може да се

[17] Ibid

[18] Во истражувањето од 2017 на Атлантската иницијатива, таканаречениот човечки допир секогаш се идентификува на почетокот на радикализацијата, во In the изданието на Аризановиќ, В (др) (2017) “Between Salvation and Terror: Radicalisation and the Foreign Fighter Phenomenon in the Western Balkans. The Atlantic Initiative, p. 17, available at: http://www.atlantskainicijativa.org/bos/images/BETWEEN_SALVATION_AND_TERROR/BetweenSal vationAndTerror.pdf

[19] Во прирачникот на УНЕСКО овие фактори се издвоени како фактори на повлекување. Види повеќе во УНЕСКО (2017)

[20] Повеќе за ова може да се најде во: Sageman Martin (2008), “Leaderless Jihad: Terror Networks in the Twenty-First Century”, Philadelphia: University of Pennsylvania Press

најдат на интернет кои користат пишани текстови, видеа и музика за да ги нарушат фактите и да влијаат кон насилна радикализација или насилно саморадикализирање.

Од прегледот на литературата, може да се идентификуваат следниве пет улоги што ги има интернетот во промовирање на радикализацијата: (i) интернетот создава повеќе можности за радикализација[21]; (ii) интернетот делува како „ехо-комора“[22]; (iii) интернетот го забрзува процесот на радикализација[23]; (iv) интернетот овозможува радикализација без физички контакт[24]; (v) интернетот ги зголемува можностите за саморадикализација.[25] Помладата генерација е особено ранлива на радикализација преку интернет бидејќи тие ги прифаќаат мрежните медиуми многу поприродно како дел од нивните животи и социјални односи отколку постарите генерации[26]. Ова значи дека важноста на комуникацијата лице в лице се намалува и контактите преку интернет се соочуваат со голема доверба, правејќи ги интервенциите на политиката кон зголемена безбедност на интернет да бидат приоритет на секоја влада.

---

[21] Pantucci 2011; Briggs and Strugnell 2009; Homeland Security Institute 2009; Weimann 2006; Precht 2008 кои дојдоа до сознание дека има корелација помеѓу џихадистичките веб-страници и пропагандата на интернет и радикализацијата во емпириска студија на 242-ца џихадисти од 2001 до 2006.

[22] Интернетот се опишува како „ехо-комора“(Ramakrishna, 2010; Saddiq, 2010; Stevens and Neumann, 2009) или „активност за ментално зајакнување“(Silber and Bhatt, 2007) што дава наводна анонимност (Weimann, 2006) и степен на заштита и безбедност од детекција (Gray and Head, 2009), а обезбедува и прифаќање: информацијата не е цензурирана и не следи хиерархија (Bartlett, 2011)

[23] Schmidle (2009) посочува особено на улогата на собите за разговор во ефектот на забрзување бидејќи екстремистите можат да разменат мислења со слични индивидуи 24/7, без разлика на границите.

[24] „Поединците ја имаат удобноста на пристапување на радикални содржини од нивниот приватен простор наместо да мораат да поминат низ непријатностите на посета на 20 собирања со радикална религиозна содржина. (Yeap and Park, 2010, p. 2)

[25] Според RAND (2013) „Радикализација во дигитална ера“, она што го одликува саморадикализирањето од онлајн радикализирањето е тоа дека се случува во изолација и упатува на процес каде што немало контакт со други терористи или екстремисти, било во живо или виртуелно“

[26] KAS (2013) “*Online-Radicalisation: Myth or Reality?*”, КАС (2016) „Онлајн радикализација: мит или реалност?“ достапно на: https://www.kas.de/c/document_library/get_file?uuid=baca4877-ac6c-4df4-ae77-28b4ba2aafac&groupId=252038

Спречување на онлајн радикализација преку јавни политики

Предизвик за владите и сите засегнати страни е да го разберат опсегот на фактори во кои социјалните медиуми можат да играат улога во радикализацијата така што реакцијата да не биде погрешно поставена или да се заснова на непоткрепени претпоставки[27]. Врз основа на ова, можно е да се идентификуваат соодветни чекори за спротивставување на активноста на онлајн радикализацијата и да се обезбедат соодветни правни, институционални, административни и образовни рамки за да се спречи заканата, во целосна усогласеност со Меѓународниот закон за човекови права. Чекорите треба да осигурат дека слободата на изразување и приватноста се ослободени од произволно, незаконско или непропорционално мешање и се во можност да ги зачуваат карактеристиките на интернетот како отворен, инклузивен и да придонесува за одржлив развој и просперитет на современото општество[28].

И покрај континуираната ранлива состојба, напорите во поглед на спречување на насилен екстремизам (СНЕ) во земјата се ограничени, а на онлајн радикализацијата на младите уште повеќе. Аналитика[29] ги проучуваше двигателите на екстремизмот кои опфаќаат слични фактори како оние што го движат глобалниот екстремизам. Исламската верска заедница во Македонија започна обука за борба против насилниот екстремизам (БНЕ) за имами за да ја охрабри заедницата да најде алтернатива за прифаќање на насилство. Фондацијата Бергхоф започна со иницијатива за заедничко истражување и дијалог, истражувајќи зошто некои заедници се особено погодени, додека другите заедници можат да покажат поголема отпорност на радикализација. Центарот за истражување и

[27] Dan Shefet (2016) Policy options and regulatory mechanisms for managing radicalization on the Internet, UNESCO
[28] UN (2015) Plan of Action to Prevent Violent Extremism, достапно на: https://undocs.org/A/70/674
[29] Analytica, 2016 "Assessment of Macedonia's Efforts in Countering Violent Extremism"
Аналитика, 2016 „Проценка на напорите на Македонија за спречување на насилен екстремизам“

креирање политики спроведе истражување за перцепцијата на училишниот кадар за радикализација и насилен екстремизам и изгради капацитети преку развој на прирачник и алатки (списоци за проверки и протоколи) и работилници за обука за рано откривање на радикализацијата. Жени без граници го поттикнаа мајчинскиот училиштен проект кој има цел да ја подигне свеста за борба против радикализмот и да ги зајакне вештините и можностите на македонските мајки да се справат со феноменот на радикализација во нивниот однос со децата. ОБСЕ обучи наставници да станат обучувачи за прашања поврзани со радикализацијата и насилниот екстремизам. ИОМ работеше на ниво на заедница обезбедувајќи обука за размислување за млади за младите. ЦИКП разви наставна програма за обука на средношколци за да ги зголемат своите знаења и вештини за безбедно користење на интернетот во обид да изгради отпорност кон онлајн радикализацијата, а изготви и Прирачник за сајбер безбедност во училиштата за зголемување на отпорноста кон онлајн радикализација.

Во однос на рамката за јавни политики, Националната стратегија за спречување на насилен екстремизам ги регулира релевантните цели, како што се: стратешката цел 1.1. Зајакнати институционални капацитети; стратешката цел 1.4: Спречување на радикализација преку интернет и стратешката цел 3.1: Воспоставен сет од мерки за рано откривање на радикализацијата. Стратегијата е усогласена со Глобалната стратегија за борба против тероризмот на Обединетите нации, којашто меѓу нејзините приоритетни активности предвидува „неопходност за поддршка на „образование, развој на вештини и олеснување на вработувањето“ како средство за поттикнување почит кон човечката разновидност и подготвување на младите за вработување”[30]. Понатаму, Стратегијата е усогласена со Стратегијата на ЕУ за борба против тероризмот и РАН (Мрежа за свесност за радикализација) Манифестот за образование – зајакнување на обучувачите и училиштата“[31].

[30] Глобалната стратегија за борба против тероризмот на Обединетите нации (A/RES/60/288), усвоена од Генералното собрание на ОН на 8 септември 2006, е уникатен глобален инструмент за зајакнување на националните, регионалните и меѓународните напори за борба против тероризмот. Повеќе за ова на : https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy

[31] РАН Манифестот за образование е достапен на: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-

Поконкретно, Стратегијата за сајбер безбедност со право посочува дека сајбер просторот може да се користи за тероризам и го идентификува како можна закана за националната безбедност, како дел од поширокиот пристап кон принципите на сајбер безбедноста[32]. Сепак, Стратегијата не предвидува цели ниту активности што конкретно се насочени кон младите, нивниот капацитет или отпорност кон радикални идеи или компјутерски промовиран тероризам. Предизвикот за решавање на онлајн радикализацијата ги одразува општите предизвици поврзани со институционалните капацитети за електронско управување. На пример: независна евалуација на капацитетите за сајбер безбедност во земјата, водена од Светска банка и Глобалниот центар за капацитети за сајбер безбедност во 2018 година, тврди дека „не беше можно да се добие јасна слика за управување со кризи…“ во текот на сајбер закани[33].

do/networks/radicalisation_awareness_network/docs/manifesto-for-education-empowering-educators-and-schools_en.pdf

[32] Влада на Република Северна Македонија, Република Македонија, Национална стратегија за сајбер безбедност 2018 – 2022, стр. 12 достапна на: https://mioa.gov.mk/sites/default/files/pbl_files/documents/strategies/cyber_security_strategy_macedonia_2018-2022_-_eng.pdf

[33] Светска банка и Глобален центар за градење капацитети за сајбер безбедност (2018), „Преглед на капацитетите за сајбер безбедност во БЈРМ“, стр. 9 достапно на: https://mioa.gov.mk/sites/default/files/pbl_files/documents/reports/cmm_fyrom_report_final_13_august2018_2.pdf

Стратешкиот план за образование 2020-2022[34] предвидува стратешка цел *2.2 Квалитетно и инклузивно средно образование,* што е согласно Стратешкиот документ „Реформа во образованието и инвестиции во иновации и технологија на информатичко општество“, но нема приоритет, активности и клучни индикатори за успешност во врска со зголемена отпорност за онлајн безбедноста на учениците, а ниту пак ја споменува онлајн безбедноста на учениците.

Концептот за учење од далечина[35] на Министерството за образование посветува дополнително внимание на безбедноста на технологијата што се користи во учењето од далечина, но исто така и на заштитата на личните податоци и приватноста, како и заштитата на здравјето и благосостојбата на студентите и наставниот кадар и заштита на животната средина. Сепак, документот не ја оценува онлајн радикализацијата како еден од ризиците за имплементација на системот за учење на далечина, ниту предлага мерки за зголемување на безбедноста на интернет и зајакнување на отпорноста на младите кон радикалните идеи до кои тие можат да пристапат на интернет. Ова е особено значајно затоа што извештајот на „Јуридајс“[36] утврдува дека повеќето европски образовни системи имаат вметнато дигитални компетенции како хоризонтална тема, но во многу земји од Источна Европа прашањата за безбедност на интернет и градење на отпорност на младите се третираат со похолистички пристап, како дел од стратегија, додека во Западна, Централна и Северна Европа овие прашања се решаваат со посебна стратегија. Во Македонија, дигиталните компетенции се стекнуваат преку два предмети, еден задолжителен и еден изборен, но прашањата за безбедноста на интернет се само покриени со наставната програма.[37]

Во петто одделение, македонскиот образовен систем на основно образование предвидува предмет Работа со компјутер и основи на компјутерско програмирање, што според наставната програма

---

[34] МОН (2019) Стратешки план 2020-2022, достапен на https://mon.gov.mk/stored/document/Strateski%20plan%20%202020-2022.pdf
[35] МОН (2020) Концепт за развивање на систем за образование од далечина во основните и средните училишта во Република Северна Македонија https://mon.gov.mk/content/?id=3262
[36] Eurydice (2019) Digital Education at School in Europe, достапен на: https://eacea.ec.europa.eu/national-policies/eurydice/content/digital-education-school-europe_en
[37] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO-trigodishno-mkd.pdf

вклучува само една содржина поврзана со безбедноста на интернет: дискусија за интернет-комуникација и безбедносни прашања поврзани со интернет-комуникацијата.

Во шесто одделение, македонскиот образовен систем на основно образование предвидува курс Информатика, кој според наставната програма има седум цели, од кои четири се поврзани со компјутерски науки, една е поврзана со информатичката технологија и две се фокусираат на дигиталните компетенции. Една од целите на дигиталните компетенции што е најрелевантна за градење на отпорност на интернет е користење на технологијата етички и одговорно и безбедно чување лични информации. Во врска со ова, одредбите од наставната програма дека правилата за безбедност ќе ги одредуваат учениците за во училницата каде што се одржува часот по информатика и ќе се разбуди дискусија со учениците за да се утврди етиката во употребата на компјутер и можната злоупотреба. Во однос на безбедноста на интернет, исто така, се планира дискусија за безбедносни прашања во комуникацијата преку интернет во вториот семестар. Сепак, проценката на информациите, податоците и дигиталните содржини и нивниот ризик за радикализација преку интернет не е предвидена.

Во VII одделение[38], предметот Информатика е задолжителен предмет кој опфаќа 5 часови поврзани со онлајн живеењето и кои индиректно ја допираат и темата „безбедноста на интернет“. Индиректно, наставната програма не вклучува содржини за безбедноста и знаење за проценка на дигитална содржина, туку гради вештини за креирање веб-страници, блогови и сл. Од тука следува дека, помеѓу содржините за онлајн живеењето, се препорачува и вклучување наставни материјали кои нудат препораки за безбедно користење на интернет, како што се веб-страниците www.bezbednonainternet.org.mk, www.dzlp.mk и www.iSafe.org.

Согласно македонскиот систем за основно образование, во VIII и IX одделение информатиката не се нуди како задолжителен или изборен предмет.

Во средното образование, гимназијалците имаат информатика како задолжителен предмет во I година, при што се стекнуваат со основни

[38] https://www.bro.gov.mk/wp-content/uploads/2020/09/Skratena_programa-Informatika-VII_odd-2020.

познавања за хардвер, софтвер и вовед во програмирањето[39], но не и со наставни содржини поврзани со безбедноста на интернет и дигитални вештини со кои би се намалила нивната ранливоста од радикализација на интернет. Во II година, овој предмет, како и информатичка технологија[40], се нуди како изборен предмет, додека во III[41] и IV[42] четвртата година се нуди задолжителен предмет Програмирање. Во ниту една од наставните програми не се предвидени дигитални вештини, особено не теми поврзани со безбедноста, како што се заштита на уредите, заштита на лични податоци и приватност, заштита на здравјето и благосостојбата, како што впрочем се бара во Рамката за дигитални вештини за граѓаните подготвена од страна на Европската комисија[43].

Рамката за дигитални вештини е усвоена во 2016, а ажурирана во 2018 година и предвидува 5 клучни области што ги мери и следи Европската унија: (i) дигитална писменост; (ii) комуникација и соработка; (iii) развој на дигитални содржини; (iv) безбедност; и (v) решавање на проблеми. Од анализата на наставната програма претставена погоре, се добива впечаток дека македонското основно образование е насочено кон градење вештини и унапредување на знаењето за дигитална писменост, како и комуникација и соработка. Од друга страна, во средното образование акцент се става на развојот на дигиталните содржини и до извесен степен на решавање на проблеми, но она што несомнено недостасува во двете нивоа на образование е фокусот на безбедноста. Имајќи ги предвид резултатите од воведната проценка од студијата на ЦИКП „Премин кон превенција: употреба на образование за спречување на онлајн радикализација кај младите“, кои патем покажуваат дека околу 30% од средношколците во општини кои беа вклучени во истражувањето споделуваат лични информации

[39] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatika-I_SSO4-mkd.pdf
[40] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Informatichka_tehnologija-II_GO-mkd.pdf
[41] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-III_GO-PMA-mkd.pdf
[42] https://www.bro.gov.mk/wp-content/uploads/2018/02/Nastavna_programa-Programski_jazici-IV_GO-mkd.pdf
[43] European Commission. *Digital Competence Framework for Citizens* (DigComp 2.0). 2018. https://op.europa.eu/en/publication-detail/-/publication/bc52328b-294e-11e6-b616-01aa75ed71a1/language-en

со непознати лица преку интернет комуникација[44] (како што се име, возраст, е-пошти, училиште, лични фотографии и друго), како и фактот што голем дел од нив посочија дека ретко или никогаш не ја проверуваат веродостојноста на информациите на интернет (40,7%), упатува на тоа дека сето ова ги прави ранливи на лажни вести, дезинформации и радикални идеи на интернет. Според тоа, повторно се враќаме на безбедноста на интернет-приоритет што треба да се реши преку законски измени или измените во наставната програма, градење капацитети и друг вид справување преку училишни политики. Поради тоа Рамката DigiComp2.0 може да послужи како патоказ за постигнување на оваа цел.

Во овој процес учениците и нивните семејства, како и севкупното општество, се корисници, додека училиштата и наставниците/просветните работници имаат улога на чинители кои делуваат како посредници. Наставниците особено треба да бидат директно опфатени бидејќи воведната проценка од студијата на ЦИКП „Премин кон превенција: употреба на образование за спречување на онлајн радикализација кај младите“ покажува дека кога учениците се чувствуваат загрозени на интернет, 61% од нив би зборувале со своите родители/старатели, 20% избираат да разговараат со пријател, 16% би пријавиле закана во полицијата, а само 1% би разговарале со наставници/професори.

Ова укажува на недостиг од доверба во наставниците или на тоа дека нивната улога во градењето отпорност и дигитални вештини не е видлива и препознаена од учениците. Ова може да се должи на немање познавања од областа или недостиг од училишни политики за обезбедување безбедност на интернет. Според тоа, средношколците кои учествуваа во истражувањето на ЦИКП сметаат дека нивните родители имаат повеќе знаење (79% од испитаниците) отколку наставниците, за кои пак 63,6% од нив изјавиле дека имаат некакви познавања за интернетот и неговите можности. Висок процент ученици (16,7%) сметаат дека на нивните наставници им недостасува знаење, па затоа подигнувањето на знаењата кај наставниците треба да биде еден важен дел од сеопфатната политика за зголемена

[44] Истражувањето покажува, 32,6% од испитаниците изјавиле дека го споделиле своето име со некој што го запознале преку Интернет, 31,8% ја споделиле својата возраст, 29,5% споделиле информации за училиштето во кое учат, додека 23,8% ги споделиле своите фотографии. 21,1% од средношколците споделиле информации со некој што го запознале само преку Интернет за тоа каде се снаоѓаат.

отпорност од онлајн радикализација. Европската рамка за дигитални вештини на воспитувачите/наставниците[45] може да послужи како водилка кон таа цел. Рамката DigiComp2.0 вклучува шест области во кои треба да се градат вештините на наставникот: (i) професионален ангажман; (ii) дигитални ресурси; (iii) образование и учење; (iv) проценка; (v) поддршка на учениците и (vi) подобрување на дигиталните вештини на учениците во поглед на информациите и медиумската писменост, комуникацијата, развојот на содржини, одговорното користење на интернетот и решавањето проблеми.

На линија на гореспоменатото, освен едно скопско училиште, останатите 41 училиште опфатени со проектот немаа политика за дигитална безбедност ниту каква било спроведена мерка кон оваа цел. Во врска со тоа дали треба да има политика/упатство за употреба на паметни телефони/уреди и интернет во училиштето договорена/о помеѓу наставниците, учениците и родителите/старателите, што би вклучувало и водич за одделни аспекти за употреба, 73% од средношколците/испитаниците од воведната проценка од студијата на ЦИКП „Премин кон превенција: употреба на образование за спречување на онлајн радикализација кај младите“ главно одобруваат ваков водич. За тоа кои специфични аспекти треба да бидат опфатени во водичот, поддршката изнесува: а) заштита на интернет-содржини (78,8%); б) несподелување лични информации и податоци (70,3%); в) однесување на интернет во поглед на заштита од сајбер насилство (78,8%); и г) проверка на информации (66,9%). Имајќи го ова предвид, Министерството за образование треба да преземе иницијатива за развој и усвојување училишни политики за онлајн безбедност со цел да се намали ранливоста од онлајн радикализација. За таа цел, Рамката за дигитални вештини во образовни организации[46] може да послужи како водилка бидејќи опфаќа седум клучни елементи, вклучително и алатката SELFIE[47], со која училиштата можат да ги развијат своите дигитални стратегии за подобрување на наставата, односно учењето и безбедноста на интернет. Алатката може да се користи и на македонски јазик.

---

[45] European Commission. *Digital Competence Framework for Educators*. 2017, достапна на: https://ec.europa.eu/jrc/en/digcompedu

[46] https://ec.europa.eu/jrc/en/digcomporg

[47] Училиштата се дигитализираат https://ec.europa.eu/education/schools-go-digital_mk

Наставниците, како и родителите, се важни затоа што можат да ги надгледуваат активностите на нивните ученици/деца додека се прикачени на интернет. Во воведната проценка од студијата на ЦИКП „Премин кон превенција: употреба на образование за спречување на онлајн радикализација кај младите“ 69,3% од испитаниците изјавиле дека се пријатели со нивните наставници на социјалните мрежи, а 85,9% со своите родители. Без да се наруши слободата на мисла и говор во онлајн активностите на нивните ученици, наставниците може да играат значајна улога во следењето на нивните ученици уште при раните фази на радикализација. Споделените содржини и коментарите, односно дискусијата на интернет може да бидат некои од показателите за радикални идеолошки промени кај учениците. Наставниците исто така можат да создадат дигитален простор за младите, со што би ги одвратиле од понатамошните чекори до радикализацијата. Дополнително, во нивните активности на социјалните мрежи, наставниците кои се мотивирани и сакаат да бидат активни носители на промени можат да ги користат сопствените профили за споделување алтернативна, односно позитивна содржина (слики, видеа и блогови) кои содржат пораки против радикализацијата.

Кон политики за онлајн безбедност

За да се воспостави политика за онлајн безбедност, мора да се спроведе сеопфатен пристап кој би се состоел од законски измени, барања за професионален развој и политики за справување на ниво на училиште. Препораките подолу може да ги преземат Министерството за образование како тело кое ги развива политиките, Бирото за развој на образованието како орган кој нуди обука на наставници и развој на наставни програми, но и училиштата како единици кои нудат образовни услуги, а сé со цел во следниот период да се изгради отпорност од онлајн радикализација.

Законски измени

Законот за основно образование[48] и Законот за средно образование[49] не предвидуваат никакви мерки за онлајн безбедност, приватност или заштита на личните податоци, освен податоците собрани и чувани од самите училишта (т.н. образовна статистика). За таа цел, потребни се законски измени во двата закона, со што би се уредила онлајн безбедноста на учениците, барањата што секое училиште треба да ги исполни за да обезбеди дигитално безбедна средина за учење и дигиталните вештини што треба да ги стекне наставниот кадар. Рамката ***DigiComp2.0***, како и Рамката ***DigiEduComp*** треба да послужат како патокази за овие реформи. Дополнително, треба да се ревидира и испитот за директор на училиште со вклучување теми поврзани со политиките за онлајн безбедност на училиштата, и тоа во модулот „Теорија на организација“, согласно Рамката ***DigiCompOrg***.

[48] https://mon.gov.mk/download/?f=zakon%20za%20osnovnoto%20obrazovanie%208.10.docx
[49] https://mon.gov.mk/download/?f=Zakon%20za%20srednoto%20obrazovanie%20%2008.10.2020.docx

Професионален развој и измени во наставните програми

Како што впрочем покажа и анализата погоре, во наставните програми недостасуваат важни содржини поврзани со онлајн безбедноста. Бирото за развој на образованието треба тие да ги развие и да ги вклучи во задолжителните предмети, особено содржини поврзани со безбедноста, како што се: заштита на уредите, заштита на личните податоци и приватноста и заштита на здравјето и благосостојбата. Примери за радикална содржина треба да се користат како вежби за градење вештини за критичко размислување, а кога се размислува за развој на дигитална содржина, да се стимулира создавање алтернативни позитивни наративи.

Дигиталната писменост на наставниот кадар треба да се подигне преку обуки, но нивната активна улога како носители на онлајн за безбедноста треба да биде пропишана и во училишните политики за безбедност. Ова ќе ја зголеми видливоста на наставниците, со што нивната улога дополнително ќе биде препознаена од страна на учениците, која во моментов е многу мала, како што впрочем покажува и истражувањето. Во овој процес, изборот на наставник како носител на е-безбедноста би помогнало во спроведувањето на политиките во секое училиште. Штом се развијат политиките за е-безбедност на ниво на училиште, училиштата треба да размислат за што поголемо привлекување и приклучување на наставниот кадар преку објаснување на важноста на е-безбедноста, организирање обуки за нивно безбедно и одговорно користење на интернетот, како и обуки за училишните политики за е-безбедност.

Политиката за е-безбедност на ниво на училиштата

Секое училиште треба да развие својата политика за е-безбедност користејќи ја алатката SELFIE или следејќи ја листата за проверка приложена во Анекс 1 од овој труд, а таа треба да вклучува задолжени наставници за координација и спроведување на политиката за е-безбедност. Сепак, бидејќи станува збор за училишна политика, дискусијата околу општите принципи за е-безбедноста, како и за тоа

кои чекори треба да се преземат доколку се појави проблем, може да се одвива и за време на наставнички совети, како и за време на класните часови со учениците. Вклучувањето на темата е-безбедност за време на родителските средби и состаноците на училишните одбори ќе ја зголеми видливоста на политиката за е-безбедност на училиштето, но ќе придонесе и кон зајакнување на отпорноста од онлајн радикализацијата. Со ова би се дале дополнителни објаснувања зошто училиштата се заинтересирани за е-безбедност во училиштата, како и во домовите на учениците, со што, од друга страна, пак ќе се зголеми довербата во наставниците од страна на учениците.

Училиштата треба да се осврнат на е-безбедноста и на организациско ниво. За таа цел, секое училиште треба да има обезбедено заштита од вируси и криптирање лични податоци, а веб-страниците на училиштата треба да бидат заштитени и да не содржат лични податоци за вработените или учениците, ниту пак слики на кои може некој/а да се препознае. Понатаму, училиштето треба да избере помеѓу „заклучување“ на одредена штетна содржина или користење помалку филтри, со што со второво ќе им се помогне на учениците во справување со онлајн ризиците. Сепак, тоа што нема да наидат на штетна содржина („заклучена“) на училиште, не значи дека не постои ризик да наидат на штетни содржини надвор од училиштето.

Училишните политики треба да вклучуваат и алатки, како што се „домашните договори“[50] и на оние на училиште, кои се потпишани од родител, ученик и наставник (види пример во Анекс 2) и Договорот за начинот на користење од страна на училишниот кадар, кој предвидува што е соодветно и професионално за вработените во однос на нивните онлајн активности. Повратните информации од наставниците и учениците за „домашните договори“, промовирани во рамките на проектот спроведен од ЦИКП, се многу позитивни. Имено, обете страни изјавија дека им помогнале за понатамошна дискусија околу онлајн безбедноста во училиште и дома, како и дека генерално придонеле кон јакнење на нивната свест поврзана со сајбер безбедноста.

Конечно, училиштата исто така треба да ги земат предвид Политиките за прифатлива употреба и да размислат за предностите од нивно годишно ажурирање со цел да се вклучат сите идни дигитални

[50] Домашните договори се начин на уредување на користењето на интернетот дома, помеѓу членовите на семејството. Види Анекс 2 за содржината на овие договори.

предизвици. Политиките за прифатлива употреба обично вклучуваат правила и совети за учениците поврзани со: исклучување на екранот и информирање на возрасен човек ако наидат на непријатна или вознемирувачка онлајн содржина; пребарување низ датотеки кои не се нивни; онлајн почит кон другите луѓе; испраќање навредливи или несоодветни СМС-пораки; давање лични податоци и детали што можат да ги идентификуваат нив или нивната локација; онлајн прикачување лични фотографии; забрана за пристап на непознати лица; блокирање несакани комуникации; и поставки за приватност, безбедност и лозинки.

Анекс 1: Листа за проверка на училишните политики за е-безбедност

	Дефинитивно донесено	Потребно е дополнително разгледување и внимание	Не е донесено
Посветен носител на политики за е-безбедност			
Политика за е-безбедност која редовно се ажурира			
Прифатлива политика за употреба за учениците			
Договор за корисници од наставниот кадар			
Одржувани ИКТ системи			
Ажурирана и редовна обука на наставниот кадар			
Е-безбедноста како точка на дневниот ред на наставничките совети			
Обука за сите групи на вработени			
Домашни договори			
Е-безбедност на дневен ред на родителските средби			
Е-безбедност на дневен ред на состаноците на училишниот совет			

Анекс 2: Домашни договори

Овој договор ја регулира употребата на паметни уреди, компјутери и интернет во семејството на _____
Правилата утврдени со овој договор се применуваат на членовите на семејството наведени подолу:

Родители _____ и _____
скриптирање деца _____ и _____
и _____ .

Правилата утврдени во овој договор важат и за гостите во семејството кои го користат интернетот.

Компјутерите, паметните уреди и интернетот ќе се користат за информирање, учење и комуникација, со најдобри намери и на начин што никому нема да наштети.

Компјутерите, паметните уреди и интернетот ќе се користат во разумно време во текот на денот и во времетраењето одредено од страна на родителите.

Не се дозволени веб-страници кои имаат несоодветна и насилна содржина која може да ги вознемири децата. Родителите треба да бидат известени кога ќе се наиде на таква содржина.

Несоодветната и насилна содржина не е дозволена да се презема, ниту пак да се чува на компјутер или паметен уред. Ако тоа се случи, родителите треба да бидат известени.

Сите профили што децата ги користат на социјалните мрежи треба да бидат пријавени кај родителите.

Користењето тајни и лажни профили на социјалните мрежи не е дозволено.

Не се споделуваат лични информации и податоци на сомнителни веб-страници или со непознати лица на социјалните мрежи.

Да се избегнуваат физички средби со непознати лица. Доколку има предлог за ваква средба, родителите треба да бидат информирани, а доколку е потребно, средбата да биде во присуство на родител или возрасен на јавно место.

Да не се споделуваат телефонски броеви со непознати лица преку интернет, ниту пак да се одговора на повици од непознати лица. Ако има таков повик или барање за повик, да се известат родителите.

Комуникацијата преку интернет или социјалните мрежи треба да биде учтива, без навредливи зборови и содржина. Употребата на такви зборови и содржина треба да се пријави кај родителите.

Не е дозволено преземање и инсталирање софтвер, како и незаконска содржина од веб-страниците без дозвола на родителите.

Придржувањето до овие правила важи и кога се користи интернет на друго место (кај пријател, интернет-кафе, училишта, јавни места итн.)

Прекршувањето на овие правила, ќе повлече казни наведени подолу[51]:

_____

_____

Долупотпишани деца:	Долупотпишани родителите:
_____	_____
_____	_____
_____	

[51] Зависно од тежината на повредата, примери за казни вклучуваат: одземање компјутер или паметен уред во определен временски период или на неодредено време, забрана за користење интернет, ограничување на времето поминато на интернет, итн.

Анекс 3: Договор за користење за наставничкиот кадар [52]

Пополнете, потпишете се и наведете го датумот во овој образец - **Договор за користење за наставничкиот кадар**, со што се обврзувате за доследно почитување на обврските и одговорностите наведени во овој договор. Клучни обврски и одговорности се:

- Севкупната употреба на ИКТ мора да биде соодветна согласно училишната средина;
- Лозинките се чуваат во тајност;
- Се применуваат принципите на доверливост, приватност и авторско право.

Ако имате какви било прашања во врска со договорот пред да се потпишете, Ве охрабруваме да разговарате за нив со управителот за онлајн безбедност или со директорот. Откако ќе се потпише, овој договор треба да се однесе во училиштето и да се предаде на управителот за онлајн безбедност, каде што се чува и архивира целата евиденцијата на вработените.

Како една од договорните страни, ќе добиете примерок од потпишаниот договор.

Ве молиме, одберете го соодветното поле -

❑ Сметам дека имам доволно знаење за безбедно да ја надгледувам употребата на училишната компјутерска мрежа, местата за пристап до интернет, компјутерите и останатата училишна ИКТ опрема/уреди од страна на учениците за коишто сум одговорен/а.

❑ Потребна ми е дополнителна обука и професионален развој со цел безбедно да ја надгледувам употребата на училишната компјутерска мрежа, местата за пристап до интернет, компјутерите и останатата училишна ИКТ опрема/уреди од страна на учениците за коишто сум одговорен/а.

[52] Ова е пример за кориснички договор на вработените од Нов Зеланд, достапен на: http://www.cybersafety.org.nz/kit/Use%20Agreements/agreements/staff_ua.html

Изјава

Ги прочитав и свесен/а сум за обврските и одговорностите наведени во овој **Договор за користење и онлајн безбедност за наставничкиот кадар**, чиј примерок ќе задржам и тој ќе ме потсетува на нив. Овие обврски и одговорности се однесуваат на онлајн безбедноста на учениците, училишната заедница и училишната средина.

Исто така сум свесен/а и разбирам дека прекршувањата на **Договорот за користење и онлајн безбедност за наставничкиот кадар** ќе бидат истражени и тоа може да доведе до дисциплинска постапка, а каде што е применливо и до соодветна законска постапка.

Име: _____

Улога во училиштето: _____

Потпис: _____

Датум: .....

Анекс 4: Политики за прифатлива употреба[53]

Цел

Целта на оваа Политика за прифатлива употреба (ППУ) е да се осигури дека учениците ќе имаат полза од можностите за учење што ги нудат училишните интернет-ресурси на безбеден и ефикасен начин. Користењето и пристапот до интернет се смета за училиштен ресурс и привилегија.

Предвидено е претставниците на училиштето и родителите редовно да ја ревидираат ППУ. Пред примената, ППУ треба внимателно да се прочита за да се осигури дека условите за употреба се прифатени и разбрани. Се претпоставува дека родителот ги прифаќа условите на ППУ, освен ако училиштето не е посебно известено.

Политика за онлајн безбедност во училиштето

Училиштето применува низа алатки во рамките на својата политика за онлајн безбедност.

Општи одредби

- Интернет активностите секогаш ќе бидат надгледувани од страна на наставник.
- Училиштето редовно ќе ја следи употребата на интернет кај учениците.
- На учениците и наставниците ќе им се обезбеди обука од областа на интернет безбедноста.
- Прикачувањето и преземањето на неодобрен софтвер е недозволено.
- Ќе се користи софтвер за заштита од вируси и тој редовно ќе се ажурира.

[53] Ова е пример на Политика за прифатлива употреба од Powerstown Educate Together National School од Ирска

- За употребата на USB, CD-ROM или други дигитални уреди за меморија ќе се бара претходна дозвола од наставникот.
- Учениците ќе се однесуваат кон соучениците со почит во секое време и нема да преземаат никакви активности што може да го доведат во прашање угледот на училиштето.
- Важно е родителите/старателите и учениците да бидат свесни за нашата Политика за спречување врсничко насилство во контекст на социјалните мрежи;
- Изолирани или еднократни инциденти на свесно и негативно поведение/акт, вклучително и еднократна навредлива СМС-порака или друга приватна порака, не спаѓаат во дефиницијата за вознемирување и треба да се решат согласно Кодексот на однесување во училиштето.
- Сепак, во контекст на оваа политика, поставување на еднократно навредлива или штетна јавна порака, слика или изјава на социјална мрежа или друг јавен форум каде што пораката, сликата или изјавата можат да ја видат и/или да ја повторат други луѓе ќе се смета како вознемирување.

Интернет

- Учениците нема свесно да посетуваат интернет-страници кои содржат непристојни и незаконски содржини, содржини кои содржат омраза и друг вид непристојни материјали.
- Учениците ќе пријават случајно пристапување до несоодветен материјал согласно училишните процедури.
- Учениците ќе го користат интернетот за образовни цели само за време на часот. Одделенскиот/класниот раководител ќе ги провери сите веб-страници.
- Учениците нема да копираат информации во училишните задачи без да го наведат изворот (плагијаризам и кршење на авторските права).
- Учениците никогаш нема да откриваат или да објавуваат лични информации.
- Преземањето материјали или слики кои не се релевантни за нивните предмети ќе претставува директна повреда на Прифатливата политика за употреба на училиштето.
- Учениците се свесни дека секоја употреба, вклучително и дистрибуција или примање информации поврзани за училиштето или од лична природа може да биде следена поради сомнеж од

невообичаени активности, од безбедносни причини и/или поради причини поврзани со одржување на мрежата

Е-пошта / Google Drive / Интернет разговор

- Пред да пристапат до е-пошта, учениците мора да потпишат писмен домашен договор со родителите и одделенскиот наставник на годишно ниво.
- Доколку ученик добие несоодветна е-пошта, тој/таа треба да ги извести одделенскиот наставник и родителот/старателот.
- Учениците нема да испраќаат или примаат каков било материјал кој е незаконски, непристоен, клеветнички или има цел да вознемири или заплаши трето лице.
- Учениците нема да ги откриваат своите лични податоци или податоци на други луѓе, како што се адреси или телефонски броеви, слики или лозинки.
- Учениците никогаш нема да договорат средба „лице в лице“ со некој што го познаваат само преку е-пошта или интернет.
- Учениците нема да имаат пристап до местата за разговор (chat), форуми за дискусии, пораки или други форуми за електронска комуникација.

Веб 2.0

Со напредокот на Веб 2.0, интернетот стана двонасочен систем на комуникација како за училиштето така и за поширокатa заедница. Услугите како што се Scribd, Class Dojo, Facebook, Wordpress, Twitter и останатите социјални мрежи се користат од страна на училиштето за комуникација со родителите, но и од родителите за комуникација со училиштето. Овие услуги се само дел од севкупната содржина што е поставена на овие платформи и подлежи на оваа политика. На пример: секоја содржина поставена на училишниот профил на Scribd подлежи на истите правила за безбедност, како на пример: прикажувањето фотографии, видео и сл.

- Многу веб-страници на социјалните мрежи имаат праг на возраст под кој не може да се отвори профил. Бидејќи училиштето не може да го следи ова, ги советуваме родителите да не дозволуваат нивните деца да имаат лични профили на Фејсбук, Твитер итн. сè додека не ја достигнат соодветната возраст. Низа социјалните

мрежи ќе ги користат наставниците на час, како што е на пример: Твитер, но сепак, сите активности ќе бидат под надзор на наставникот.

- Родителите и старателите се охрабруваат редовно да ја проверуваат онлајн активноста/дигиталниот траг на нивното дете, вклучително и апликациите на социјалните мрежи (на пр.: Facebook, Snapchat, Viber, WhatsApp, Instagram итн.) на мобилни телефони и електронски уреди за да се осигурат дека се свесни за онлајн интеракцијата на своето дете со другите и таа да ја одобрат.
- Ве молиме не означувајте фотографии (tag) или каква било друга содржина со што би се идентификувале деца или вработени во училиштето.
- Ако поставувате фотографија, осигурете се дека не го идентификува детето на кој било начин, а нејзината големина да биде што е можно помала (не поголема од 800x600 пиксели).
- Ве молиме, осигурете се дека пораките и онлајн коментарите за училиштето се пристојни. Сите пораки на социјалните мрежи се третираат на ист начин како и било која писмена порака до училиштето.
- Избегнувајте какви било негативни разговори на социјалните мрежи за деца, вработени или родители.
- Ве молиме, не поставувајте објави на нашиот sид без претходно одобрение од директорот.
- Неисполнувањето на горенаведените правила ќе резултира со Ваше трајно блокирање на нашите профили на социјалните медиуми.

Училишна веб-страница

- Имајте предвид дека следните одредби се однесуваат на училишната веб-страница и профилите на социјалните медиуми, вклучително, но не ограничувајќи се на Facebook, Twitter, YouTube, Scribd и Google+.
- На учениците ќе им се даде можност да објавуваат проекти, уметнички/креативни дела и друг вид дела поврзани со училиштето на училишната веб-страницата во согласност со јасни политики и постапки на одобрување на содржината која може да се прикачи на веб-страницата.

- Училишната веб-страницата редовно ќе се проверува за да се осигури дека нема содржина што ја загрозува безбедноста на учениците или вработените.
- Училишната веб-страницата која користи алатки, како што се „книги“ за посетители, табли за белешки/пораки или веб-блогови, често ќе се проверува за да се осигури дека тие не содржат лични податоци.
- Објавувањето дела на учениците ќе го координира наставник.
- Делата на учениците ќе се објавуваат во образовен контекст на веб-страниците.
- Училиштето ќе настојува да користи дигитални фотографии, аудио или видеоклипови со фокус на училишните групни активности. Ќе се користат фотографии, аудио и видеоклипови. Видеоклиповите нема да бидат заштитени со лозинка.
- Личните информации за ученикот, вклучително и адресата на живеење и контакт-информациите ќе бидат изоставени од веб-страниците.
- На училишната веб-страница ќе се избегне објавување на презимето на поединци на дадена фотографија.

Мобилни телефони/електронски уреди

- Користењето мобилни телефони/електронски уреди мора да биде согласност Политиката за мобилни телефони/електронски уреди.
- Училиштето ја препознава корисноста и практичноста на мобилните телефони/електронските уреди, вклучително и нивниот потенцијал како образовен ресурс.
- Многу од опциите на мобилните телефони/електронските уреди, како што се: организатор (календар, калкулатор, конвертор итн.), дел од апликациите (диктафон, стоперка, уредувач на слики, снимање видео), па дури и будилникот/алармот, се многу полезни и може да се користат согласно насоките на одделенскиот наставник. Доколку и кога ќе се одвиваат вакви активности, родителите ќе бидат претходно известени.
- Учениците кои користат сопствена технологија во училиште, како што е оставање вклучен мобилен телефон или негово користење за време на час, чинат директна повреда на Прифатливата политика за употреба на училиштето.

- Учениците кои испраќаат непристојни СМС-пораки чинат директно кршење на Прифатливата политика за употреба на училиштето.
- Неовластено сликање со камера од мобилен телефон или електронски уред, во мирување или во движење, претставува кршење на Прифатливата политика за употреба на училиштето.