Ненад Путник
Младен Милошевић
Владимир Цветковић
Универзитет у Београду
Факултет безбедности

УДК: 343. 851 (497.11)
Прегледни рад
Примљен: 5.12.2012.

ПРОБЛЕМ ЗАШТИТЕ ОБРАЗОВНО-ВАСПИТНИХ УСТАНОВА ОД ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА И ЕЛЕКТРОНСКОГ НАСИЉА[1]

Чланак је посвећен разматрању проблема заштите образовно-васпитних установа од високотехнолошког криминала и електронског насиља. Имајући у виду природу високотехнолошког криминала, може се констатовати да посебно рањиву категорију корисника Интернета представља популација младих: деце, адолесцената и студената. Образовно-васпитне установе представљају важан чинилац у процесу превенције и сузбијања безбедносних ризика којима су млади изложени у сајбер простору. Аутори анализирају постојеће нормативно и фактичко стање у овом домену и предлажу конкретне мере за редукцију ових безбедносних ризика, те указују на могућност и значај изградње и имплементације вишеслојног модела заштите.

У првом делу рада анализирана је домаћа правна регулатива у области високотехнолошког криминалитета. Имајући у виду специфичност предмета истраживања, аутори анализирају и одредбе законских и подзаконских прописа у области заштите деце од насиља, злостављања и занемаривања у образовно-васпитним установама, фокусирајући се на норме о тзв. електронском насиљу.

У другом делу рада аутори предлажу принципе и елементе за изградњу модела вишеслојне заштите и анализирају могућност њеове примене у образовним установама у Републици Србији, а у циљу превенције ризика из широког спектра високотехнолошког криминалитета.

Кључне речи: *образовно-васпитне установе, високотехнолошки криминал, електронско насиље, модел вишеслојне заштите.*

---

[1] Чланак представља део резултата рада на пројекту „Безбедност и заштита организовања и функционисања васпитно-образовног система у Републици Србији (основна начела, принципи, протоколи, процедуре и средства)“ број 47017, који финансира Министарство просвете и науке Републике Србије (2011–2014).

Увод

Глобална рачунарска мрежа отворила је нове могућности за извршавање криминалних дела. Интернет је, услед огромног броја корисника, отворености и правне нерегулисаности, постао полигон, али и идеално скровиште за криминалце различитог типа. Имајући у виду природу високотехнолошког криминала, може се констатовати да посебно рањиву категорију корисника Интернета представља популација младих: деце, адолесцената и студената. Приступ различитим садржајима на Интернету и данас веома популарним друштвеним мрежама, као што су Фејсбук и Твитер, млади не остварују само посредством персоналних рачунара и компјутерских мрежа, већ и захваљујући другим „паметним“ уређајима. Брз и бежичан приступ Интернету, путем ових уређаја, омогућава примање и слање е-маил порука као и комуницирање на друштвеним мрежама. Млади су, несумњиво, и најчешћи и најлаковернији корисници друштвених мрежа. Услед недостатка едукације у погледу опасности којима су изложени на друштвеним мрежама, неискусни корисници на своје профиле непромишљено остављају информације и мултимедијалне садржаје који могу бити злоупотребљени од стране различито мотивисаних корисника Интернета. Осим што су изложени ризику од нарушавања личне приватности и злоупотребе приватних садржаја, млади су изложени и ризику од политичке или идеолошке манипулације.

Високотехнолошки криминал је комплексан феномен под којим се подразумевају разноврсне криминалне активности. Оне најчешће подразумевају нападе на рачунарске системе и мреже, садржаје или интелектуалну својину.

Услед распрострањености и децентрализованости глобалне рачунарске мреже, активност криминалаца у сајбер простору постала је међународни проблем и промовисала је питања заштите информационих система, спровођења међународних истрага, екстрадиције и кажњавања извршилаца. Последњих година су, у том смислу, изражене интензивне активности на формирању широког одбрамбеног фронта, сачињеног од различитих субјеката међународних односа, у циљу супротстављања високотехнолошком криминалу. У супротстављању безбедносним претњама у сајбер простору на располагању су различите мере које могу помоћи да се успешно одговори на ове изазове, као што су: алати за заштиту, законска регулатива, безбедносни стандарди, промовисање безбедносне културе и компјутерске етике итд.

Досадашња искуства у супротстављању безбедносним претњама у сајбер простору указују на потребу стварања кохерентног оквира који подразумева примену како превентивних, тако и репресивних мера у стварању безбедног сајбер амбијента. Превентивне активности, на првоме месту, подразумевају унапређивање законске регулативе, како на националном тако и на међународном ни-

воу, као и осмишљавање различитих мера и стратегија заштите информационих система и њихову имплементацију.

Предмет нашег истраживања је проблем заштите школске деце и омладине, као и самих образовно-васпитних установа од овог вида угрожавања безбедности. Имајући наведено у виду, кренули смо са приказом правног оквира за борбу против високотехнолошког криминала (пре свега у образовно-васпитном систему), да бисмо се затим концентрисали на идентификацију и класификацију претњи којима су млади изложени у сајбер простору.

1. Високотехнолошки криминалитет и електронско насиље у законодавству Р. Србије

За означавање високотехнолошког криминалитета користе се различити термини – кибер или сајбер криминал, технолошки криминал, интернет криминал, дигитални криминал, електронски и др. У домаћој литератури се помиње и појам компјутерски криминалитет, који се дефинише као посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује као средство извршења или као објект кривичног дела, уколико се дело на други начин, или према другом објекту, не би могло извршити или би оно имало битно другачије карактеристике (Игњатовић, 1991:142). Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала - ЗОВК (2005) у домаћем законодавству је први пут дата дефиниција високотехнолошког криминала. Он се дефинише као "вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику." Класификација високотехнолошког криминалитета може се извршити узимајући у обзир различите критеријуме. Ми ћемо облике испољавања овог феномена класификовати ослањајући се претежно на најважније законодавне акте у предметној области: Кривични законик - КЗ (2005) и ЗОВК, не занемарујући значај других закона који на посредан начин третирају ову проблематику. То су: Закон о информационом систему Републике Србије (1996), Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела (2002), Закон о ауторским и сродним правима (2009), Закон о електронским комуникацијама (2010), Закон о електронском потпису (2004), Закон о забрани дискриминације (2009), Закон о заштити потрошача (2010), Закон о заштити података о личности (2008), Законик о кривичном поступку (2011). Правни оквир чине и ратификовани међународноправни акти од значаја у овој области (Закон о потврђивању конвенције о високотехнолошком криминалу, 2009 и Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком

криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, 2009). Потпуна слика о нормативном оквиру за супротстављање хетерогеним облицима високотехнолошког криминала и електронског насиља у Републици Србији може се добити тек уколико се анализирају одредбе законских и подзаконских аката који се баве заштитом школске деце и омладине од насиља, злостављања и занемаривања у школама, укључујући и безбедносне ризике у сајбер простору. Међутим, то не би било од велике користи за овај рад. Наиме, предмет нашег проучавања је врло специфичан и представља новост за наше законодавство, те се у поменутим актима не може наићи на концепт електронског насиља. Експлицитан појам електронског насиља као облика вршњачког насиља налазимо само у одредбама једног подзаконског акта, док се остали закони, прописи и општи акти у овој области баве сличном и сродном, али не и овом конкретном тематиком. Јасну и директну везу са концептом електронског насиља у школама видимо у законском акту који је уже везан за образовно-васпитни систем и заштиту деце од насиља, злостављања и занемаривања у образовно-васпитним установама.

Овде мислимо на Закон о основама система образовања и васпитања – ЗОСОВ (2009), као темељни закон у области образовно-васпитног система. Нама су одредбе ЗОСОВ првенствено важне јер се односе и на заштиту деце и ученика од насиља, злостављања и занемаривања у образовно-васпитним установама. Овај закон је, иначе, логичан и конзистентан наставак стратешких докумената у области заштите деце од насиља, злостављања и занемаривања – Националног плана акције за децу, Општег протокола за заштиту деце од злостављања и занемаривања и Посебног протокола за заштиту деце и ученика од насиља, злостављања и занемаривања у васпитно-образовним установама. Ови акти су, међутим, донети под утицајем међународноправних обавеза Републике Србије, које су преузете ратификацијом Конвенције о правима детета (Закон о потврђивању Конвенције о правима детета, 1990). Од значаја за проучавану проблематику је и Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица (2005), јер третира област кривичноправне заштите малолетника, иако у њему нема одредаба о електронском насиљу међу малолетницима.

Ступањем на снагу одговарајућих одредби ЗОСОВ-а Србија је започела са испуњавањем обавеза преузетих ратификацијом Конвенције о правима детета и обавезе поступања по препорукама Комитета за права детета из 2008. године (Нешић, Јовић, 2011:54). Ратификација Конвенције намеће држави обавезу да обезбеди остваривање свих права детета укључујући заштиту од свих облика насиља, злостављања и занемаривања, потпуну информисаност, правично поступање и заштиту приватности, као и да детету које је било изложено насиљу обезбеди подршку за физички и психички опоравак и социјалну реинтеграцију.

Управо на овом месту долазимо до јасне везе између одговарајућих одредби ЗОСОВ и наше теме – заштите деце и ученика од електронског насиља. Чланови 44 и 45 овог Закона експлицитно забрањују насиље, злостављање, занемаривање и дискриминацију у школама. Члан 103 став 1 тачка 4 ЗОСОВ прописује да је заштита од насиља, злостављања и дискриминације право детета. Члан 44 став 1 ЗОСОВ прописује да је у васпитно-образовној установи забрањено: физичко, психичко и социјално насиље; злостављање и занемаривање деце и ученика; физичко кажњавање и вређање личности, односно сексуална злоупотреба деце и ученика или запослених. Став 3 објашњава шта обухвата појам „физичко насиље“ - физичко кажњавање деце и ученика од стране запослених и других одраслих особа; свако понашање које може да доведе до стварног или потенцијалног телесног повређивања детета, ученика или запосленог; насилно понашање запосленог према деци, ученицима или другим запосленим, као и ученика према другим ученицима или запосленим. Психичко насиље, пак, подразумева свако понашање које доводи до тренутног или трајног угрожавања психичког и емоционалног здравља и достојанства детета и ученика или запосленог. Законодавац у ставу 7 уводи и појам „социјално насиље“ које се односи на искључивање детета и ученика из групе вршњака и различитих облика социјалних активности установе.

Став 2 овог члана дефинише појмове насиља и злостављања, подразумевајући под њима сваки облик једанпут учињеног или понављаног вербалног или невербалног понашања које има за последицу стварно или потенцијално угрожавање здравља, развоја и достојанства личности детета и ученика или запосленог. Став 3 дефинише занемаривање и немарно поступање као пропуштање установе или запосленог да обезбеди услове за правилан развој детета и ученика. Одредба става 8 истог члана прецизира да се забрана из става 2 односи и на ситуацију у којој ученици, њихови родитељи, односно старатељи или други одрасли, изврше неки облик насиља над наставником, васпитачем, стручним сарадником и другим запосленим.

Прецизирање одредби ЗОСОВ у смислу даље конкретизације дефиниција законом прописаних врста насиља, злостављања и занемаривања, учињено је доношењем Правилника о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање (2010). Правилник додатно прецизира појмове социјалног, психичког и физичког насиља и злостављања, занемаривања и немарног поступања, али посебно издваја и злоупотребу, сексуално насиље, експлоатацију детета и ученика и електронско насиље као облике претходних. За материју коју истражујемо најзначајнија је чињеница да Правилник дефинише појам електронског насиља: „електронско насиље и злостављање је злоупотреба информационих технологија која може да има за последицу повреду друге лично-

сти и угрожавање достојанства и остварује се слањем порука електронском поштом, СМС-ом, ММС-ом, путем веб-сајта (web сите), четовањем, укључивањем у форуме, социјалне мреже исл".

Електронско насиље се свакако не може изједначити са појмом високотехнолошког криминала. Вршење дела електронског насиља може подлегати санкцијама предвиђеним ЗОСОВ-ом, осим у случају да је њиме остварено биће неког кривичног дела, у ком случају ће се примењивати кривичноправне одредбе. Сматрамо добрим решењем увођење појма електронског насиља, јер оно даје нормативни основ за санкционисање понашања која се не могу обухватити појмом високотехнолошког криминала, али остављају негативне и друштвено штетне последице, те се на њиховом сузбијању и санкционисању треба озбиљно ангажовати.

2. Класификација претњи информационо-комуникационим системима и појмовно одређење ризика високотехнолошког криминала

Развој савремене информационо-комуникационе технологије и њене примене у пословним системима, организацијама па и образовно-васпитним установама довела је до тога да ова технологија постане незаменљива у обављању свакодневних радних процеса. Информационо-комуникационе технологије представљају веома осетљиву инфрастуктуру школе, те се на њих мора обратити посебна пажња приликом идентификације и процене критичних штићених вредности (Кешетовић, 2012:37). У домаћој и страној релевантној литератури из области безбедности и заштите рачунарских система могу се пронаћи бројне класификације претњи, извршене на основу различитих критеријума.

У домаћој литератури, иако оскудној, могуће је препознати неколико различитих приступа у класификацији претњи (Велашевић, 1996; Петровић, 2001; Плескоњић и сар., 2007).

У иностраним истраживањима посвећеним безбедности сајбер простора, могуће је пронаћи велики број различитих класификација претњи информационим системима. У научним тематизацијама овог проблема, улогу лидера имају амерички цивилни и војни институти, владине институције и корпорације које се баве заштитом рачунарских система. Улога ауторитета у овој области приписује се Мултинационалној компанији за информационе технологије (Consolidated Analysis Center, Incorporated – CACI) са седиштем у Арлингтону, Истраживачком одељењу администрације Конгреса САД (General Accounting Office – GAO) и Националном институту за стандарде и технологије (National Insitute of Standard and Technologies – NIST). Класификације које су сачиниле ове институције, доступне су на Интернету и данас се сматрају релевантним на пољу сајбер безбедности.

Једну од тешкоћа приликом сваког покушаја класификације представља чињеница да је број претњи које могу угрозити информациони систем практично неограничен, због чега их је и немогуће све предвидети. Другим речима, свакој се класификацији може замерити одређени степен непотпуности. Такође, треба имати у виду да међу појединим претњама постоји одређена међузависност која условљава да појава једне претње иницира и појаву друге претње, као и да повећање интензитета једне аутоматски утиче и на повећање интензитета друге претње.

Зато идентификација претњи захтева наглашену опрезност из простог разлога што се често претња која није била идентификована може показати катастрофалном. Из тог разлога се поставља и питање избора адекватног методолошког приступа, посебно што у вези са овим проблемом ни на нивоу теорије још увек не постоји јединствено мишљење, нити изграђено јединствено решење (Путник, 2009:67).

Са друге стране, разврставање претњи у групе које, у извесном смислу, представљају логичке целине јесте неизбежно јер омогућује њихову анализу, што је неопходан корак за формулисање сваке политике заштите.

Верујемо да би једна потпунија класификација безбедносних претњи информационим системима морала да садржи следеће категорије претњи: „виша сила“ (пожари, поплаве и земљотреси), кварови, људски фактор са атрибутом ненамерности, људски фактор са атрибутом намерности. У оквиру основних класификационих категорија може се вршити гранање на поткатегорије. Тако се категорија „људски фактор са атрибутом ненамерности“ може гранати на „грешке у пројектовању хардвера и софтвера“ и „грешке у коришћењу рачунарских система“, док се категорија „људски фактор са атрибутом намерности“ може делити на поткатегорије: „физички напади“, „електронски напади“ и „сајбер претње“.

Традиционални појавни облици претњи информационим системима, сврстани у категорије „виша сила“, „кварови“, „људски фактор са атрибутом ненамерности“ и део скупа „људски фактор са атрибутом намерности“, који обухвата „физичке“ и „електронске“ нападе, историјски посматрано, познати су стручњацима на пољу безбедности и заштите информационих система. За разлику од њих, нови појавни облици претњи, названи „сајбер претње“, још нису чак ни идентификовани у потпуности јер се њихов број, као и појавни облици, непрестано увећавају. Свакодневно повећање начина злоупотребе сајбер простора не само да представља тешкоћу у изналажењу адекватних мера за заштиту информационих система, већ и приморава на размишљање о могућим облицима угрожавања у будућности.

У најопштијем смислу, безбедносна претња у сајбер простору може се рашчланити на две компоненте: начин изазивања (технике и инструменти) и субјект (актер) претње. Начин изазивања претње представља прави механизам претње,

док је субјект претње особа или организација која иницира настанак претње или извршава акцију.

У односу на начин изазивања сајбер претњи, тј. технике и инструменте који се користе у циљу њиховог остваривања, претње је могуће груписати у одређене врсте. У досадашњим истраживањима у подручју сајбер безбедности, безбедносне претње у сајбер простору најчешће су поистовећиване са сајбер нападима техничког типа и оним нападима у сајбер простору који се заснивају на обмањивању других корисника сајбер простора и злоупотреби њиховог поверења. Под нападима техничког типа подразумевају се напади засновани на употреби малициозних програма (malware) као што су: вируси, црви, тројанци итд., као и напади усмерени на дистрибуирану опструкцију услуга (distributed denial of service ? DDoS). У категорију напада који се заснивају на обмањивању других корисника сајбер простора и злоупотреби њиховог поверења уобичајено се сврстава тзв. социјални инжењеринг (social engineering) и фишинг (phishing) као његова нејчешће коришћена техника (Ibid., 71).

Осим различитих врста сајбер напада, који, свакако, представљају веома широк спектар ризика по безбедност информационих система, евидентно је и специфично злоупотребљавање сајбер простора у односу на његову функцију средства за масовну комуникацију. Када циља популацију школског узраста овај вид злоупотребе се најчешће поистовећује са електронским насиљем али се може спроводити и кроз форму политичке и идеолошке манипулације младима (Кордић & Путник, 2012). Из тог разлога категорији безбедносних претњи у сајбер простору, осим већ поменута два аспекта сајбер напада, приписујемо и потткатегорију „злоупотреба сајбер простора као средства масовне комуникације", као посебну врсту претњи, с обзиром на њихов деструктивни потенцијал у односу на омладину и друштво у целини.

Тако, на пример, информације обзнањене на јавној друштвеној мрежи могу бити злоупотребљене од стране других корисника Интернета међу којима су и сајбер криминалци, ментално поремећене личности, политички и идеолошки мотивисане групе и слично. Најмлађи корисници, несвесни опасности, често остављају податке о адреси становања, бројеве телефона, обавештења о томе када су им родитељи на послу (када су сами код куће), у ком периоду ће бити на летовању и друге осетљиве информације. Твитер (Twitter), који је веома популаран међу овом популацијом, чак омогућава објављивање личног распореда активности током дана – када је дете у школи, куда иде после школских активности, где се тренутно налази и чиме се бави итд. Ове информације могу бити злоупотребљене за планирање и извршење широког спектра криминалних радњи: пљачке, киднаповања, физичког и психичког малтретирања итд. Нарушавање личне приватности, дакле, може водити и нарушавању физичког интегритета личности.

Најчешће информације које деца остављају на корисничком профилу бивају злоупотребљене од стране њихових вршњака. Реч је феномену тзв. *сајбер бу-*

линїа (cyber-bullying) односно задиркивања, кињења или, у тежим облицима, злостављања у виртуелном свету. Сајбер булинг је феномен који је у непрестаном порасту. Резултати истраживања, које је спроведено у пет средњих школа у Београду, показали су да је 10% ученика узраста од 11 до 15 година спроводило ову врсту активности према другим ученицима. Осим тога, истраживање је показало да је 20% ученика било жртва оваквих, виртуелних, кампања (Popovic-Citic et al., 2011: 412). Овај вид тортуре може оставити значајне психолошке последице, о чему се у стручној литератури водила широка дебата након откривања првог случаја виртуелног силовања (Џонсон, 2006).

Са друге стране, пак, регистровани су и случајеви да нападач преузима и виртуелни идентитет мете напада, тј. жртве у циљу појачања ефекта оцрњивачке кампање или, пак, постизања криминалних циљева.

Сваки појединац је рањив на различите врсте отворених и прикривених напада од стране злонамерних актера, било да за циљ имају прављење несланих шала или јасне криминалне намере. Осећај нарушавања и губитка личног мира и приватности може имати дуготрајне психолошке последице. Друштвене мреже на Интернету снабдевају агресора веома великом количином информација о жртви, што њему даје могућност да се упусти у психолошко ратовање. Сајбер клеветање или дигиталне кампање за озлоглашавање имају потенцијал да допру до невероватно великог броја људи, огромном брзином, и да, при томе, нанесу велике фрустрације и колатералну штету жртви. Поновно успостављање поверења и спасавање репутације у јеку виртуелних оцрњивачких кампања представљају велику тешкоћу за жртву. Мета напада се ставља у положај да се брани, и у стању је несигурности поводом нападачевог идентитета, мотива, локације, циљева, као и тога да ли је напад извршио појединац или група људи. Она, најчешће, и не зна коме се може обратити за помоћ у таквој ситуацији будући да је у већини држава изражена конфузија надлежности над оваквим деликтима.

Друга категорија ризика повезана је са пропагандним и интегративним својствима друштвених мрежа. Чињеница је да друштвене мреже представљају простор на коме се промовишу идеје, идеологије, подстичу кампање, мотивишу и групишу људи сличних ставова и жеља. Ова дигитална састајалишта омогућила су појединцима и различитим, најчешће, маргинализованим групама људи да размењују идеје. На друштвеним мрежама идентитет групе се може брзо оформити и ојачати - усамљени гласови лако и брзо добијају одјек. Корак који дели наизглед безазлено лобирање и ватрено критиковање стања у друштву од дигиталне анархије је врло мали.

Утицај Интернета и друштвених мрежа на стварање или промену политичких, социјалних или економских околности у државама, био је предмет бројних истраживања (Schmitt-Beck & Mackenrodt, 2010; Margetts et al., 2011; Bošković & Putnik, 2011). Са увећањем броја друштвених мрежа и усавршавањем графичких корисничких интерфејса, социјални и политички активисти имају још више мо-

гућности да одржавају дебате, доказују властите „истине“, сакупљају новчане фондове или врбују нове чланове. Религиозно или идеолошки мотивисане групације попут верских секти и терористичких организација сада на располагању имају технолошки напредна средства за вођење електронског рата.

Размена личних података путем друштвених мрежа и употреба ових система за ширење различитих идеолошких, верских и политичких уверења и позиве на активизам, представљају изазов за безбедносне структуре државе, како у погледу заштите националне безбедности тако и постизања личне сигурности корисника мрежа, нарочито малолетних лица (Asher et al., 2009; Shin, 2010 и Van Eecka & Truyens, 2010). У дигиталном окружењу су ризици од манипулације младима и њиховог врбовања у овакве организације постали знатно израженији јер је смањена могућност контроле понашања деце од стране родитеља и наставника (Forkosh-Baruch & Hershkovitz, 2012; DeAndrea et al., 2012).

Опште узев, можемо закључити да су претње информационо-комуникационим системима бројне и разноврсне, те да не постоји сагласност теоретичара по питању приступа проблему класификације ових претњи. Претња је, по природи, апстрактан концепт – она је нешто што има потенцијал да стави једну организацију, особу или друштво у ризичну ситуацију. Претња је могућност да се оствари нежељени догађај. Када се ова могућност актуализује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претњу уочио надлежни ауторитет или менаџмент она постаје део ризика, те као таква, предмет расподеле њиховог времена и расположивих ресурса (људских, техничких, финансијских итд.) ради супротстављања (Путник, 2009:62).

У односу на наш предмет истраживања, и на циљ који се жели постићи – пројектовање интегралног система заштите образовно-васпитних установа, било би корисно и сврсисходно формулисати и применити методологију која би на једнообразан начин категоризовала широк спектар разноврсних безбедносних ризика којима су изложене образовно-васпитне установе. Такву методологију је понудила група аутора у чланку „Проблеми идентификације и класификације безбедносних ризика у школама“ према којој се категоризација може засновати на подели свих ризика на две основне класификационе класе (физичко-техничке и социо-психолошке ризике). У оквиру основних класификационих класа може се вршити гранање на потклассе. У том смислу, класа физичко-техничких ризика обухвата потклассе „елементарне непогоде“ и „техничко-технолошке опасности“ док класа социо-психолошких ризика обухвата потклассе „људско понашање којим се свесно изазивају негативне последице“ и „људско понашање којим се несвесно изазивају негативне последице“. Основни критеријум овакве класификације је извор ризика (Кековић и сар., 2012).

У складу са овим приступом, и безбедносни ризици који могу нарушити интегритет информационо-комуникационих система, као и они које теже да наруше интегритет њихових корисника могу се сврстати у једну од четири наведене

потклаасе. Уколико би био прихваћен овакав приступ класификацији, на семантичкој равни би, у циљу усаглашавања приступа и нормирања ове области, било оправдано увођење појма *ризици високоїехнолошкоїа криминала* (*информаїички ризици*). Овај израз би, у том случају, представљао збирни појам који би по обиму обухватао све законима инкриминисане радње везане за злоупотребу рачунара и рачунарских технологија. Под њим би се, дакле, подразумевало: нарушавање приватности запослених и ученика, безбедности пословања, као и угрожавање школске имовине које се спроводи путем физичког уништавања (онеспособљавања или отуђења) школске информационо-комуникационе инфраструктуре, односно уништавања, модификовања или неовлашћеног присвајања софтвера или података садржаних у школским електронским архивама, без обзира на то да ли се овим штићеним вредностима приступа директно или посредно, преко рачунарске мреже.

3. Принципи и елементи за моделовање система вишеслојне заштите образовно-васпитних установа од високотехнолошких ризика

Ризици високотехнолошког криминалитета, који у усвојеној класификацији делом спадају у категорију физичко-техничких а делом у категорију социо-психолошких ризика, уколико се остваре могу нарушити интегритет не само школске информационо-комуникационе инфраструктре већ и њених корисника - особља, наставника и ученика. Због тога се руководство образовно-васпитне установе мора прилагођавати новој безбедносној реалности и предузети активности на пољу превенције, заштите и одговора на ове безбедносне ризике. Те активности подразумевају не само примену специфичних хардверских и софтверских алата, већ и пројектовање и имплементацију сложеног слојевитог система заштите.

Адекватан систем заштите морао би да има двојаку функцију: да одврати од злоупотребе рачунара, односно спречи његову злоупотребу и да, у случају да је злоупотреба извршена, омогући брзо откривање и доказивање учињеног дела (Петровић, 2007:171). Пројектант таквог система би морао да у обзир узме различите аспекте заштите. Мислимо да је оптималан метод заштите онај који би подразумевао вишедимензионалан (вишеслојан) приступ, усмерен на проактивно деловање. Овакав модел би требао да обухвати неколико аспеката:

• Физички (онемогућава физички приступ - физичко обезбеђење);

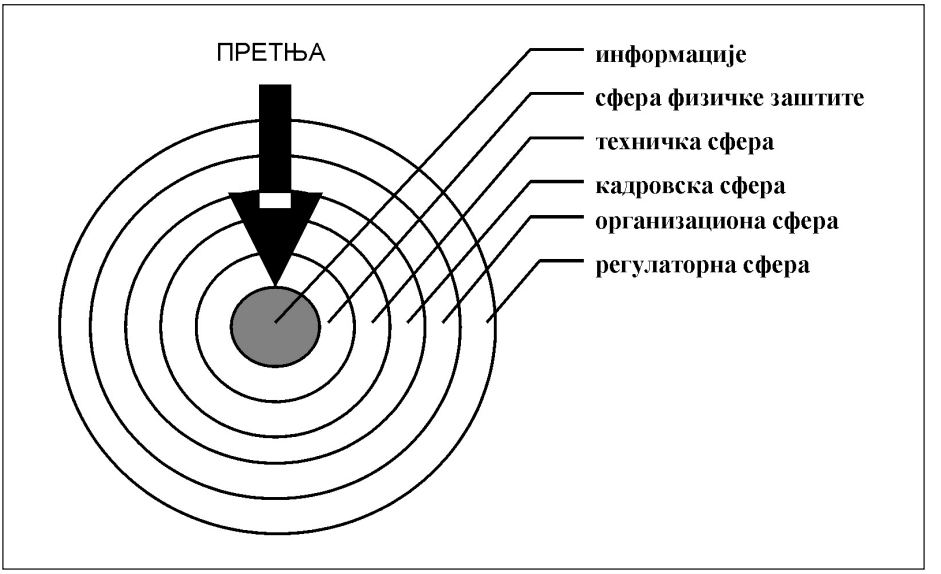
• Технички (техничко обезбеђење - електронско обезбеђење; заштита од електромагнетног зрачења; идентификација, верификација и ауторизација приступа; системи за детекцију и спречавање напада; криптографија);

• Организациони (организациона структура, дефинисање радног процеса, развој софтверских система, праћење смерница и стандардв, планирање итд);

• Кадровски (планирање и избор кадрова, руковођење, стручно усавршавање и безбедносно образовање итд.) и

• Регулаторни (упутства, планови и друга интерна регулатива која обавезује и прописује извршење неке радње и начин изршења те радње).

Схема бр. 1: Модел вишеслојне заштите



Сфере физичке и техничке заштите се, уобичајено, називају техничким аспектом заштите, док се организациона, кадровска и регулаторна сфера подводе под друштвени аспект заштите. Оба аспекта су подједнако значајна и само се њиховом комбинацијом, и синергијским ефектом, може постићи задовољавајући ниво заштите информационих система образовно-васпитних установа.

Технички аспекти заштите представља прву линију одбране информационих система. Овај аспект заштите подразумева коришћење мера које имају за циљ регулисање начина и техничких поступака којима се може умањити ризик од злонамерног нарушавања функционалности информационих система. У циљу спречавања приступа (физичког и путем мреже) штићеном систему, у употреби су различити технички уређаји и средства али и разноврсни информатички алати.

Приликом планирања физичког обезбеђења користи се неколико метода. Контрола приступа је термин који се користи када се говори о механизму који регулише приступ рачунарима, софтверу и другим ресурсима. Сервери који чувају важне податке, рутери и друге битне мрежне компоненте требало би да се налазе у закључаним орманима, или обезбеђеним рачунарским центрима. Добро обезбеђен цен-

тар или орман представља физичку препреку за сваку особу која није овлашћена да приступи серверу.

Инсталација са добром физичком безбедношћу требало би да користи концентричне прстенове прогресивних физичких препрека, при чему се најосетљивији ресурси постављају у централни прстен. Физичке препреке подразумевају примену класичних, временских или кодираних брава, постављање видео-интерфона, магнетних картица, видео камера и службеника физичко-техничког обезбеђења. Сваки улазак у рачунарски центар би требало да буде документован. Унутрашњи прстенови обезбеђеног подручја би требало да пружају заштиту са свих шест страна просторије. У неким случајевима се ове мере могу појачати алармним системима и камерама. Стандардни механизми за отварање врата попут металних кључева, магнетних картица и лозинки могу да буду недовољни за просторије које захтевају посебно обезбеђење. У таквим случајевима може се применити комбинација биометријских провера: провера отиска прста, геометрије руке, скенирање дужице, скенирање мрежњаче или фацијални термограм.

Употреба готових софтверских алата за заштиту, доступних на тржишту (попут антивирусних програма, firewall-филтера итсл.), свакако је од великог значаја на основном нивоу заштите. Информатички уско специјализовани методи и технике за откривање и супротстављање сајбер нападима укључују коришћење специјалних софтверских апликација за заштиту персоналних рачунара и рачунарских мрежа, употребу криптографских и енкриптичких метода, техника и система, као и система за откривање и спречавање упада.[2]

Друштвени аспекти заштите. Будући да информациони системи нису пројектовани тако да се могу штитити само техничким средствима (јер је њихов домет ограничен), ефикасна заштита се мора базирати на одговарајућим управљачким политикама и процедурама у погледу: дефинисања радног процеса, развоја софтверских система, праћења смерница и стандардв, планирања и избора кадрова, руковођења, стручног усавршавања и безбедносног образовања запослених, као и доношења интерне регулативе која обавезује и прописује извршење неке радње и начин изршења те радње.

---

[2] Системи за откривање и спречавање упада се деле на системе за детекцију напада (Intrusion Detection System - IDS) и системе за превенцију напада (Intrusion Prevention System - IPS). Детектовање напада је процес надгледања и процене догађаја у рачунару и мрежног саобраћаја, са циљем да се открију знаци напада. Систем за детекцију напада је хардверски уређај са софтвером, или софтвер, који се користи за откривање неовчашћених активности на мрежи. Уређај се може имплементирати на појединачне рачунаре, сервере, на мрежној периферији или целој мрежи. Системи за превенцију напада су знатно напреднији од система за детекцију напада. Они су фокусирани на то шта напад ради, што је у основи непроменљиво. Основне функције система су: идентификација неовлашћених активности на основу потписа и детектованих аномалија, вођење евиденције и слање аларма администраторима у реалном времену, прикупљање форензичких података и спречавање напада.

Са организационог аспекта посебно је значајна имплементација међународних и националних безбедносних стандарда у овој области. У последњој деценији XX века, и првој деценији овог века публиковани су, или прерађени, бројни национални и међународни стандарди који се односе на управљање безбедношћу података у рачунарским системима. Ови стандарди се, према намени, могу поделити на: стандарде за безбедност производа, стандарде за безбедност процеса и стандарде безбедности система (Кукрика, 2002:102).

Чување информација, као мере знања и суштинског ресурса је добило свој оквир у серији стандарда ISO 27000, где су спецификовани захтеви које треба да поштује установа како би остварила систем за заштиту информација. У октобру 2005. године објављен је стандард ISO 27001 под називом Системи управљања безбедношћу информација – Захтеви (Information Security Management System /ISMS/ requirements).[3] Српска верзија овог стандарда (SRPS ISO/IEC 27001 Информационе технологије - Технике безбедности - Системи менаџмента безбедношћу информација – Захтеви, 2011) објављена је 28. новембра 2011. године. Он дефинише захтеве које мора да испуни систем за управљање безбедношћу података, да би га акредитована организација могла сертификовати. Развој овог стандарда је тесно повезан са стандардом ISO 9001.

Група стандарда ISO 27000 је значајана за све организације које се баве услугама у областима које су на било који начин повезане са информационим технологијама и које имају потребу за очувањем поверљивости информација. Његова имплементација и примена омогућавају бољу сарадњу са сличним организацијама широм света које послују по овом моделу. Овим стандардом организације демонстрирају својим корисницима да је пословна политика усмерена на стална побољшавања у систему менаџмента за безбедност информација. Значајне су користи које модел за уређење система за безбедност информација ISO 27001 остварује код свих који га усвоје, пре свега у смислу побољшавања организационих перформанси. Овај модел представља најбољу праксу у области заштите и безбедности информација, која је преточена у захтеве стандарда.

Са аспекта превентивног деловања и заштите информационих система, посебну пажњу заузима изградња и развој етичких норми и принципа у домену информатике. Успостављање и развој ових норми и принципа је од изузетног значаја, јер они могу пронаћи примену у свим оним случајевима нарушавања безбедности који нису у супротности са правом али се перципирају као неприхватљиво понашање.

---

[3] Српска верзија овог стандарда под ознаком SRPS ISO/IEC 27001 Информационе технологије - Технике безбедности - Системи менаџмента безбедношћу информација – Захтеви, објављена је 3. новембра 2011. Према: Институт за стандардизацију Србије, http://www.iss.rs/news/news_33.html

Развој и све већа употреба Интернета довели су до, наизглед, бескрајног низа етичких питања, пошто је Интернет временом попримао све значајнију примену у различитим доменима живота. Интернет је покренуо и спектар важних етичких питања попут: питања приватности, демократичности, својинских права итд (Џонсон, 2006:19). Глобални опсег комуникације многих са многима, анонимност и могућност репродукције су црте комуникације на Интернету које стварају низ могућих предности и потешкоћа. Пред организацијама које спроводе урађивачку политику на Интернету стоји изазов да, до максимума, остваре позитивне потенцијале ове технологије и да, истовремено, ограниче могућности за њену злоупотребу. Изазов се, између осталог, састоји у томе да се приступи решавању проблема криминала и злоупотребе на Интернету, а да се за то примене стратегије које не би умањиле моћ коју он пружа појединцима.

Разматрајући везу између технологије и етике, може се доћи до закључка да је, кроз историју, поље компјутерске етике напросто следило развој компјутерске технологије (Ibid., 16). У историјском смислу, дакле, поље компјутерске етике је било реактивно у односу на технологију – компјутерски етичари су пратили технолошки развој и тек накнадно реаговали на њега. Свакако да би било боље када би технологија следила етику. Тада би се, сигурно, посвећивало више пажње оним технологијама које повећавају степен заштите приватности корисника рачунарских система.

Закључак

И поред тога што образовне установе у Републици Србији не спадају у категорију оних високо информатизованих, обављање појединих административних, логистичких али и наставних процеса се заснива на употреби информационо-комуникационих технологија те се ова врста ризика не би смела занемарити. С обзиром на савремене тенденције развоја и процес прогресивне информатизације друштва, може се очекивати да ће ова врста ризика бити све присутнија и у образовно-васпитним установама.

У том смислу, образовно-васпитне установе треба да постану једна од кључних карика система друштвене заштите деце и омладине, што се може постићи озбиљним и планским приступом овом проблему. Полазна тачка у овом правцу била би изградња јединственог, функционалног и прагматичког модела вишеслојне (друштвене и техничке) заштите школске популације и инфраструктуре.

Руководство школе би требало да уложи одређени напор и да примени барем основне стандардизоване хардверске и софтверске безбедносне алате и мере у циљу заштите своје информационо-комуникационе инфраструктуре, будући да то не изискује велика материјална издвајања.

Ипак, најбоља заштита од електронског насиља и других облика узнемиравања или криминала на мрежи је – знање. Константне иновације у области техноло-

гије и виртуелних комуникација, захтевају и сталну едукацију како о њиховом свр-сисходном, тако и безбедном коришћењу, односно о опасностима које безрезервно понашање корисника у односу на технологију, носе. У односу на интересовања, старост и улогу у заједници (дете, родитељ, запослени), едукација захтева различите приступе и знања и вештине које је корисницима потребно пренети. Заједничко начело у едукацији свих категорија корисника јесте да треба бити опрезан, али не и плашити се. Интернет и друштвене мреже својом применом могу корисницима донети мноштво корисних информација, побољшати мотористику, помоћи у учењу и усавршавању језика, размени искустава. Тиме, ове технологије не треба да посматрати као „јахаче апокалипсе", већ као корисну ризницу знања, података и могућности, али којој треба приступати одговорно, зрело и безбедно. Једино недовољно развијена безбедносна култура, скромна сазнања о опасностима и неопрезно поступање „на мрежи", могу ове технологије учинити извором најразличитијих опасности, које често не остају само у „виртуелној стварности", већ се могу и остварити/реализовати у „стварном" свету.

ЛИТЕРАТУРА

Asher, C., Aumasson, J., R.C-W. (2009). Security and Privacy Preservation in Human-Involved Networks. *IFIP Advances in Information and Communication Technology* 309: 139-148.

Bošković, M., Putnik, N. (2011). Uloga druљtvenih mreћa u savremenim socio-politickim i bezbednosnim pojavama. U: *XIX TELEKOMUNIKACIONI FORUM TELFOR 2011. Zbornik radova sa medunarodne konferencije, 22-24.11.2011*, (str. 110-113). Beograd: Druљtvo za telekomunikacije – DT, Beograd, Elektrotehnicki fakultet Univerziteta u Beogradu i IEEE Serbia&Montenegro COM CHAPTER.

DeAndrea, D. C., Ellison, N. B., LaRose, R., Steinfield, C., Fior, A. (2012). Serious social media: On the use of social media for improving students' adjustment to college. *The Internet and Higher Education* 15 (1): 15-23.

Игњатовић, Ђ. (1991). Појмовно одређивање компјутерског криминалитета. *Анали Правног факултета у Београду*, бр. 1-3/1991.

Џонсон, Д. (2006). *Компјутерска етика*. Београд: Службени гласник.

Forkosh-Baruch, A., Hershkovitz, A. (2012). A case study of Israeli higher-education institutes sharing scholarly information with the community via social networks. *The Internet and Higher Education* 15 (1): 58-68.

Кековић, З., Милошевић, М., Путник, Н. (2012). Проблеми идентификације и класификације безбедносних ризика у школама. У: Б. Поповић-Ћитић, С. Ђурић, Ж. Кешетовић (Ур.), *Безбедносни ризици у образовно-васпитним установама.* (стр. 51-69). Београд: Факултет безбедности.

Кешетовић, Ж. (2012). Кризне ситуације и управљање ризиком у образовно-васпитним установама. У: Б. Поповић-Ћитић, С. Ђурић, Ж. Кешетовић (Ур.), *Безбедносни ризици у образовно-васпитним установама*. (стр. 31-51). Београд: Факултет безбедности.

Кордић, Б., Путник, Н. (2012). Друштвене мреже на интернету и безбедност ученика. У: Б. Поповић-Ћитић, С. Ђурић, Ж. Кешетовић (Ур.), *Безбедносни ризици у образовно-васйишним усйановама*. (стр. 203-223). Београд: Факултет безбедности.

Кукрика М. (2002). *Уйрављање сиїурношћу информација*. Београд: INFOhome Press.

Кривични законик (*Службени їласник РС*, бр. 85/05, 88/05 - исправка, 107/05 - исправка, 72/09 и 111/09).

Margetts, H., John, P., Escher, T., Reissfelder, S. (2011). Social information and political participation on the internet: an experiment. *European Political Science Review* 3: 321-344.

Нешић, С., Јовић, Н. (2011). *Заштита деце од насиља у школама – извештај заштитника їрађана и їанела младих саветника*. Београд: Заштитник грађана.

Петровић, С. (2001). *Комйјуйерски криминал*. Београд: МУП Р. Србије.

Петровић, С. (2007). *Полицијска информайика*. Београд: Криминалистичко-полицијска академија.

Плескоњић, Д., Мачек, Н., Ђорђевић, Б., Царић, М. (2007). *Сиїурносй рачунарских сисйема и мрежа*. Београд: Микро књига.

Popović-Citic, B., Đurić, S., Cvetković, V. (2011). The Prevalence of cyberbullying among adolescents: A case study of midlle schools in Serbia. *School Psychology International* 32 (4): 412-424.

Правилник о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање (2010). *Службени їласник РС*, бр. 30/10.

Путник, Н. (2009). *Сајбер йросйор и безбедносни изазови*. Београд: Факултет безбедности.

Schmitt-Beck, R., Mackenrodt, C. (2010). Social networks and mass media as mobilizers and demobilizers: A study of turnout at a German local election. *Electoral Studies* 29 (3): 392-404.

Shin, D. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers* 22 (5): 428-438.

SRPS ISO/IEC 27001 Информационе технологије - Технике безбедности - Системи менаџмента безбедношћу информација – Захтеви (2011). *Службени їласник*, 94/11.

Урошевић, В., Ивановић, З., Уљанов, С. (2012). *Мач у world wide web-у*. Београд: Eternal mix.

Van Eecke, P., Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review* 26 (5): 535-546.

Велашевић, Д. (1996). Заштита података у рачунарским системима. *Info Science* 4 (1), 4-15.

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала (2005). *Службени їласник РС*, бр. 61/05, 104/09.

Закон о информационом систему Републике Србије (1996). *Службени їласник РС*, бр. 12/96.

Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела (2002). *Службени їласник РС*, бр. 42/02, 27/03 , 39/03 , 67/03 , 29/04 , 58/04 - др. закон, 45/05 , 61/05 , 72/09 ,72/11 - др. закон, 101/11 - др. закон.

Закон о ауторским и сродним правима (2009). *Службени їласник РС*, бр. 104/09, 99/11.

Закон о електронским комуникацијама (2010). *Службени їласник РС*, број 44/10.

Закон о електронском потпису (2004). *Службени їласник РС*, број 135/04.

Закон о забрани дискриминације (2009). *Службени їласник РС*, број 22/09.

Закон о заштити потрошача (2010). *Службени їласник РС*, бр. 73/10.

Закон о заштити података о личности (2008). *Службени їласник РС*, бр. 97/08, 104/09 - др. закон, 68/12 – УС.

Законик о кривичном поступку (2011). *Службени їласник РС*, бр. 72/11, 101/11.

Закон о основама система образовања и васпитања (2009). *Службени їласник РС*, бр. 72/09, 52/11.

Закон о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица (2005). *Службени гласник РС*, број 85/05.

Закон о потврђивању Конвенције о правима детета, (1990). *Службени лист СФРЈ-Међународни уговори*, бр.15/90.

Закон о потврђивању конвенције о високотехнолошком криминалу (2009). *Службени гласник РС*, бр. 19/09.

Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система (2009). *Службени гласник РС*, бр. 19/09.

Nenad Putnik
Mladen Milošević
Vladimir Cvetković
Belgrade University-Faculty of Security Studies

Summary

THE PROTECTION OF EDUCATIONAL INSTITUTIONS FROM CYBER CRIME AND CYBERBULLYING- PROBLEMS AND DILEMMAS

The article analyses the problems that appear in the process of protecting the educational institutions from the security risks in cyber space - cyber crime and cyberbullying. Due to main characteristics and nature of security risks in cyber space, children, adolescents and students are particularly vulnerable category of Internet users. Having this on mind, we can conclude that educational institutions are an important factor in the process of prevention and control of security risks that young people face in cyber space. The authors analyze the legal framework and the actual situation in this domain and propose concrete measures for the reduction of security risks in cyber space, and consider the capacities and importance of building and implementing the unique, funtional and pragmatic multi-layer protection model. The first part of thi article is dedicated to the analyses of the legal framework for countering cyber crime, with the consideration of the normative legal acts that regulate the protection of children and students from the violence, malestation and neglection in the school environment. The authors also focuse on the legal definition of cyberbullying. In the second part of the article, the authors propose the principles and elements for building a model of multi-layer protection and analyze the possibility of its application in educational institutions in the Republic of Serbia, as an efficient tool for the prevention and reduction of security risks in the cyber space.

Key words: educational institutions, cyber crime, cyberbullying, the model of multi-layer protection.