УДК 351.78:373.2/.5(497.11)

Прегледни рад

Српска политичка мисао
број 1/2013.
год. 20. vol. 39.
стр. 215-234.

Зоран Ђ. Кековић

Универзитет у Београду - Факултет безбедности, Београд

Ненад Р. Путник

Универзитет у Београду - Факултет безбедности, Београд

ПОЛИТИКА ЗАШТИТЕ ОБРАЗОВНО-ВАСПИТНОГ СИСТЕМА - АНАЛИЗА И ПРЕДЛОЗИ ЗА УНАПРЕЂЕЊЕ*

Сажетак

Текст је посвећен разматрању и критици постојећих политика и нормативних приступа проблему безбедности образовно-васпитног система Р. Србије. Аутори представљају, анализирају и критикују постојећа решења и предлажу конкретне мере којима би био дат значајан допринос процесу идентификације, анализе и оцене безбедносних ризика у образовно-васпитним установама, полазећи од холистичког приступа. У овом смислу, аутори предлажу усвајање јединственог методолошког инструмента за процену ризика, оличеног у националном стандарду СРПС А.Л2:003, указујући истовремено на потребу за његовим редефинисањем у појединим доменима, а у циљу његовог потпуног прилагођавања актуелним претњама образовно-васпитном систему. При томе, аутори су пошли од идеје да су информатички ризици „карика која недостаје“ мозаику процене ризика предвиђеном наведеним стандардом. Имајући ово у виду, аутори су спровели емпиријско истраживање међу ученицима средњошколских домова којим су

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

потврдили оправданост хипотезе о реалности и значају информатичких ризика у савременом друштву, а посебно међу школском омладином.

Кључне речи: политика заштите образовно-васпитног система, безбедносни ризици, процена ризика, информатички ризици, стандард СРПС А.Л2:003

Психо-физички интегритет ученика и запослених, имовина и критична инфраструктура, али и интерперсонални односи и социјална клима у образовно-васпитним установама изложени су различитим безбедносним ризицима и претњама. Вршњачко насиље, злоупотреба алкохола и дрога, сексуални деликти и злоупотребе овлашћења и положаја, суморна су и потресна реалност неких домаћих образовно-васпитних установа.

На постојање озбиљних безбедносних проблема у српским основним и средњим школама указују истраживања спроведена у последњих петнаестак година. Резултати појединих истраживања су потврдили тезу да школа није заштићена средина, већ су ученици у њој више изложени вршњачком насиљу него ван ње.[1)]

У прилог овом закључку говори и веома интересантно истраживање спроведено од стране Заштитника грађана и Панела младих саветника 2011. године, које је резултовало извештајем насловљеним „Заштита деце од насиља у школама“. Резултати студије су били прилично забрињавајући. Наиме, свега 6% деце у основним школама је изјавило да се никад нису срели са насиљем у својој школи (и 23% деце у средњим школама је изјавило исто). Потврђена је и теза да је насиље старије над млађом децом учестала појава.[2)] Забрињавајући су и закључци о насиљу наставника према ученицима, које се чешће одвија у средњим школама и креће се у распону од 20% до 30%. Истраживање доноси и податак да је 23% ученика било сведок неког облика насиља наставника према ђацима.[3)]

Да је проблем безбедности школа присутан показује и анонимна анкета коју је међу наставницима спровео Форум београд-

1) Слободанка Гашић–Павишић, „Насиље над децом у школи: функција образовних установа у превенцији и заштити деце од насиља“, у зборнику: *Насиље над децом* (уредник : М. Милосављевић), Факултет политичких наука, Београд, 1998, стр. 159–186.

2) Снежана Нешић, Наташа Јовић, *Заштита деце од насиља у школама – извештај заштитника грађана и панела младих саветника*, Заштитник грађана, Београд, 2011, стр. 20.

3) *Ibid.*, 21.

ских основних школа 2008. године. Резултати су показали да је 39% наставника доживело насиље од ученика и исто толико процената од родитеља, док свега око 25% никад није доживело насиље у школи. Од анкетираних наставника који су трпели насиље 8% је изјавило како је доживело физичко насиље, док је четвртина била изложена непосредним претњама насиљем.[4)]

АКТУЕЛНИ ПРИСТУПИ ПРОБЛЕМУ БЕЗБЕДНОСТИ ОБРАЗОВНО-ВАСПИТНИХ УСТАНОВА У СРБИЈИ

И поред наведеног, терминолошки корпус ове сложене безбедносне проблематике није добио задовољавајуће теоријско одређење у релевантној научној и стручној литератури.

Основ система заштите образовно-васпитних установа чине закони, прописи и други општи правни акти. Темељни закон у области образовно-васпитног система је Закон о основама система образовања и васпитања.[5)] Осим њега, права детета и ученика се регулишу у складу са потврђеним међународним уговорима (Закон о потврђивању Конвенције о правима детета[6)]), Уставом Републике Србије, Кривичним закоником,[7)] Закоником о кривичном поступку,[8)] Законом о малолетним учиниоцима кривичних дела и кривичноправној заштити малолетних лица,[9)] Законом о прекршајима,[10)] Породичним законом,[11)] Законом о општем управном поступку,[12)] и Законом о забрани дискриминације.[13)]

Чланови 44 и 45 овог Закона експлицитно забрањују насиље, злостављање, занемаривање и дискриминацију у школама. Члан

4) Драган Попадић, *Насиље у школама*, Институт за психологију и УНИЦЕФ, Београд, 2008, стр. 106.

5) *Службени гласник РС*, бр. 72/09, 52/11.

6) *Службени лист СФРЈ - Међународни уговори*, бр. 15/90.

7) *Службени гласник РС*, бр. 85/05, 88/05 - исправка, 107/05 - исправка, 72/09 и 111/09.

8) *Службени лист СРЈ*, бр. 70/01, 68/02, *Службени гласник РС*, бр. 58/04, 85/05 - др. закон, 85/05, 115/05, 49/07, 20/09 - др. закон, 72/09, 76/10, 72/11 - др. закон. Од 15. јануара следеће године у примени ће бити: Законик о кривичном поступку, *Службени гласник РС*, бр. 72/11, 101/11).

9) *Службени гласник РС*, бр. 85/05.

10) *Службени гласник РС*, бр. 101/05 и 116/08.

11) *Службени гласник РС*, бр. 18/05.

12) *Службени лист СРЈ*, бр. 33/97 и 31/01.

13) *Службени гласник РС*, бр. 22/09.

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 образовно-васпитној 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.. 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.

На основу темељног закона у области, донет је и важан подзаконски акт усмерен на заштиту деце од злостављања, занемаривања и насиља у школама. Реч је о Правилнику о протоколу поступања у установи у одговору на насиље, злостављање и занемаривање („Службени гласник РС“, бр. 30/10). 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. Врло је занимљиво да, у складу са захтевима савременог доба, Правилник дефинише појам електронског насиља: „електронско насиље и злостављање је злоупотреба информационих технологија која може да има за последицу повреду друге личности и угрожавање достојанства и остварује се слањем порука електронском поштом, SMS-ом, MMS-ом, путем веб-сајта (*web site*), четовањем, укључивањем у форуме, социјалне мреже исл“.

Правилник уводи појам превенције насиља, подразумевајући под њим мере и активности којима се у установи ствара сигурно и подстицајно окружење, негује атмосфера сарадње, уважавања и конструктивне комуникације. Установа програмом заштите од насиља, злостављања и занемаривања одређује мере и активности које обезбеђују развијање и неговање позитивне атмосфере и безбедно окружење. Програмом заштите дефинишу се превентивне и интервентне активности, одговорна лица и временска динамика остваривања.

Предвиђене мере и активности делују као добро осмишљен систем. Међутим, оправдано је запитати се на који начин ће установе моћи да испуне обавезе предвиђене одредбама Правилника. Почнимо од основне – како школа или друга образовно-васпитна установа анализирају стање безбедности? Да ли постоје прописани критеријуми за утврђивање стање безбедности? Темељи ли се она на претходној процени ризика и, ако да, који пропис или стандард се узима као полазиште приликом анализе, оцене и квантификаци-

је ризика? Да ли се зна који орган управљања или запослени је заиста компетентан да на стручно заснован начин процени стање безбедности у установи? Ко онда може и треба да састави адекватан Програм заштите, барем у елементима који се тичу безбедности? Ко од наставника или другог особља треба да прати учесталост и дистрибуцију насиља, злостављања и занемаривања, те да о њима води евиденције? Има ли смисла наметати обавезе установама, а при том не водити рачуна о постојању људских и материјалних ресурса за њихово испуњавање? Вреди ли нам добро осмишљен систем мера ако немамо субјекте дорасле процесу њихове имплементације?

Сматрамо да процес идентификације ризика мора да укључи ризике чија учесталост, интензитет и степен остварења у школском амбијенту заврђују посебну пажњу. Покушај стварања такве методологије учињен је у чланку „Проблеми идентификације и класификације безбедносних ризика у школама“ према којој категоризација безбедносних ризика треба да обухвати 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.[14)]

У закључку наведеног истраживања аутори износе запажање да су тзв. информатички ризици (који претежно спадају у категорију социо-психолошких ризика) готово потпуно занемарени, што с обзиром на савремене тенденције развоја и процес информатизације друштва представља озбиљан недостатак досадашњих класификација.

Следећа полазна тачка везана је за разматрање могућности примене постојећих националних стандарда из области друштвене безбедности на проблем безбедности образовно-васпитних установа. У чланку „Процена и одговор на ризике у образовно-васпитним установама применом стандарда СРПС А.Л2.003” група аутора је разматрала могућност примене стандарда СРПС А.Л2.003

14) Зоран Кековић, Младен Милошевић, Ненад Путник, „Проблеми идентификације и класификације безбедносних ризика у школама“, у зборнику: *Безбедносни ризици у образовно-васпитним установама* (уредници: Бранкица Поповић-Ћитић, Слађана Ђурић, Желимир Кешетовић), Факултет безбедности, Београд, 2012, стр. 51-69.

на образовно-васпитне установе у Р. Србији.[15] Аутори закључују да јединствен и системски утемељен законски оквир за процену и контролу ризика у образовно-васпитним установама, који би омогућио хармоничну и осмишљену активност државних органа и установа није присутан. Главни проблем лежи у чињеници да нису предвиђени стручни школски органи задужени за анализу, праћење и оцену стања безбедности у школама, као и прописа, техничких стандарда, протокола и упутстава који би формулисали процедуре и критеријуме за стварну процену безбедносних ризика у школама и створили основ за глобалан приступ проблему безбедности деце у образовно-васпитним установама. Безбедносни ризици нису карактеристични за образовно-васпитни систем, већ су део постојања сваког система и организације. Системски и холистички приступ проблему процене и контроле безбедносних ризика у организацијама уопште представља норматив коме треба тежити као „крову" под којим ће се сабрати различити специфични приступи безбедности појединих типова организација.

Идеја нашег истраживања је да допринесе постављању темеља нове безбедносне политике у образовно-васпитним установама. Нови приступ проблему безбедности школа и осталих образовно-васпитних установа подразумева ослањање на научно засноване процедуре, методе и технике којима би се свестрано, детаљно и систематично приступило откривању основних узрока настајања безбедносних ризика, те идентификацији и класификацији главних извора опасности и хазарда који погодују њиховом појављивању, а затим приступило процесу процене ризика и, коначно, њиховом менаџменту.

МОГУЋНОСТ ПРИМЕНЕ НАЦИОНАЛНИХ СТАНДАРДА ИЗ ОБЛАСТИ ДРУШТВЕНЕ БЕЗБЕДНОСТИ

Национални стандард СРПС А.Л2:003 је јединствен инструмент који омогућава глобалан приступ безбедности организације, јер његова методологија подразумева анализу и оцену свих аспеката организацијске безбедности, од опасности везаних за систем менаџмента безбедношћу и здравље на раду, преко противпожарне заштите до опасности везаних за унутрашњу нормативну регула-

15) Зоран Кековић, Младен Милошевић, Ненад Путник, Ненад Комазец, *Процена и одговор на ризике у образовно-васпитним установама применом стандарда СРПС А.Л2.003*, у: Кордић и сар. (уредници), Реаговање на безбедносне ризике у образовно-васпитним установама, Факултет безбедности, Београд, 2012, стр. 55-93.

тиву и противправно деловање унутар и/или ван организације. У стандард су уграђени принципи и упутства садржани у одговарајућим међународним документима и стандардима за управљање ризицима, прилагођени нормативноправном, економском и друштвеном амбијенту Републике Србије и, нарочито, специфичностима домаћег тржишта.

Идеја групе аутора је била да испитају у којој мери се овакав инструмент може користити као основ процене и контроле ризика у организацијама образовно-васпитног типа? Општи циљ пилот истраживања је био да се утврди тренутно стање безбедносних ризика једног дела образовно-васпитног система – ученичких средњошколских домова, пратећи одабране параметре, а на основу „субјективних“ процена учесника у процесима. Прелиминарни резултати спроведеног пилот истраживања показали су да је стандард добра полазна основа те да би могао бити применљив уз одређене модификације. Оцењивање ризика по принципу комплементарних индикатора квалитативног типа, уз додавање квантитативних по потреби (мерљивих сетовима исказа), следећи концепте дефинисане стандардом СРПС А.Л2.002:2008 је применљиво на образовно-васпитни систем.

ИНФОРМАТИЧКИ РИЗИЦИ У ОБРАЗОВНО-ВАСПИТНИМ УСТАНОВАМА

Информационо-комуникационе технологије представљају веома осетљиву инфрастуктуру школе, те се на њих мора обратити посебна пажња приликом идентификације и процене критичних штићених вредности.[16] У домаћој и страној релевантној литератури из области безбедности и заштите рачунарских система могу се пронаћи бројне класификације претњи информационо-комуникационој технологији, извршене на основу различитих критеријума.[17] 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. Зато идентификација претњи захтева наглашену опрезност из простог разлога што се често претња која

16) Don Philpott, Michael W. Kuenstle, *Education facility security handbook*, Government Institutes, Plymouth, 2007.

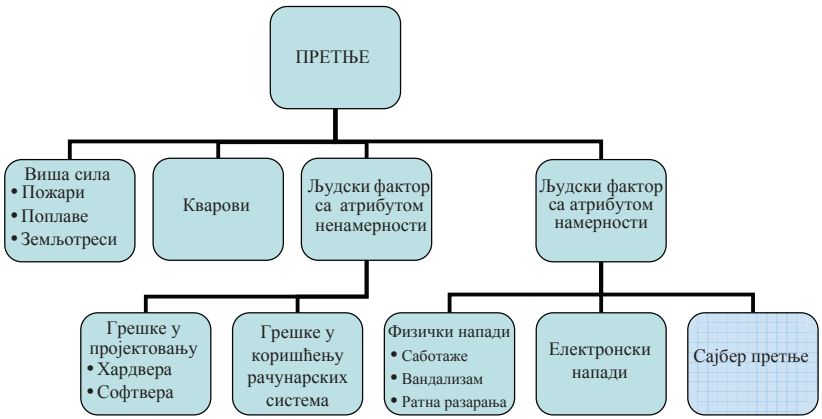
17) Видети шире: Душан Велашевић, „Заштита података у рачунарским системима“, *Info Science*, Београд, бр. 4(1), 1996; Слободан Петровић, *Компјутерски криминал*, МУП Р. Србије, Београд, 2001; Драган Плескоњић, Немања Мачек, Борислав Ђорђевић, Марко Царић, *Сигурност рачунарских система и мрежа*, Микро књига, Београд, 2007.

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.[18)]

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.

У схематском приказу који следи (Схема бр.1) понудили смо, на основу увида у досадашња истраживања, верујемо, једну од потпунијих класификација безбедносних претњи информационим системима.

Схема бр. 1:
Класификација претњи информационим системима



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.

18) Ненад Путник, *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009, стр. 67.

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 најчешће коришћена техника.[19)]

Када циља на популацију школског узраста овај вид злоупотребе се најчешће спроводи кроз форму политичке и идеолошке манипулације младима.[20)] Из тог разлога категорији безбедносних претњи у сајбер простору, осим већ поменута два аспекта сајбер напада, приписујемо и поткатегорију „злоупотреба сајбер простора као средства масовне комуникације“, као посебну врсту претњи, с обзиром на њихов деструктивни потенцијал у односу на појединце и друштво у целини. У следећем схематском приказу (Схема бр. 2) покушали смо да, на основу увида у досадашња истраживања, али и властитих запажања, графички представимо једну, по нашем мишљењу, систематичнију класификацију безбедносних претњи у сајбер простору.

Напади на рачунарске системе и мреже, као и злоупотреба садржаја који су у њима похрањени и интелектуалне својине, инкриминисани су домаћом нормативом у области виокотехнолошког криминалитета – Кривичним закоником Републике Србије и Законом о организацији и надлежности државних органа за борбу против високотехнолошког криминала[21)], али и другим законима у Републици Србији који на посредан начин третирају ову област (Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких

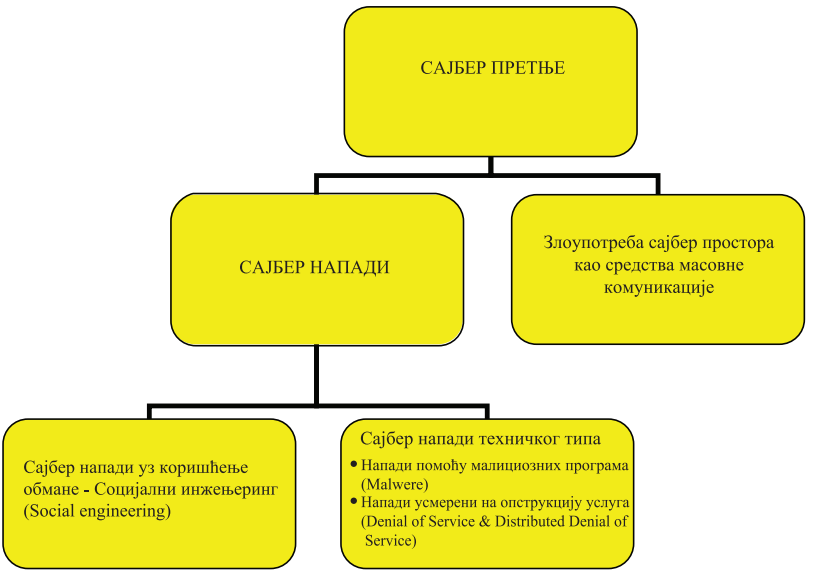
19) *Ibid.*, стр. 87.

20) Борис Кордић, Ненад Путник, „Друштвене мреже на интернету и безбедност ученика“, у зборнику: *Безбедносни ризици у образовно-васпитним установама* (уредници: Бранкица Поповић-Ћитић, Слађана Ђурић, Желимир Кешетовић), Факултет безбедности, Београд, 2012, стр. 203-223.

21) *Сл. гласник РС*, бр. 61/05, 104/09.

кривичних дела,[22] Закон о ауторским и сродним правима,[23] Закон о електронским комуникацијама,[24] Закон о електронском потпису,[25] Законик о кривичном поступку,[26] Закон о заштити потрошача,[27] Закон о оглашавању,[28] Закон о информационом систему Републике Србије,[29] Закон о заштити података о личности[30]).

Схема бр. 2:
Класификација безбедносних претњи у сајбер простору



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

22) *Сл. гласник 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).

23) *Сл. гласник РС*, бр. 104/09, 99/11.

24) *Сл. гласник РС*, бр. 44/10.

25) *Сл. гласник РС*, бр. 135/04.

26) *Сл. гласник РС*, бр. 72/11, 101/11.

27) *Сл. гласник РС*, бр. 73/10.

28) *Сл. гласник РС*, бр. 79/05.

29) *Сл. гласник РС*, бр. 12/96.

30) *Сл. гласник РС*, бр. 97/08, 104/09 - др. закон, 68/12 – УС.

категоризовала широк спектар разноврсних безбедносних претњи и ризика образовно-васпитним установама. Такву методологију је понудила група аутора у поменутом чланку „Проблеми идентификације и класификације безбедносних ризика у школама".

Уважавајући поменути приступ групе аутора, и безбедносне претње које циљају интегритет информационо-комуникационих система, као и оне које теже да наруше интегритет њихових корисника могу се сврстати у једну од четири предвиђене поткласе. Уколико би био прихваћен овакав приступ класификацији, на семантичкој равни би, у циљу усаглашавања приступа и нормирања ове области, било оправдано увођење појма *информатички ризици*. Под њим би се, дакле, подразумевали и они ризици који се везују за „вишу силу", „кварове", „људски фактор са атрибутом ненамерности" као и они који се односе на различите видове злоупотребе информационо-комуникационе технологије у физичком и виртуелном свету, без обзира на то да ли су оне у важећем кривичном законодавству проглашене кривичним делима.[31)]

МОГУЋНОСТ УНАПРЕЂЕЊА СТАНДАРДА СРПС А.Л2.002:2008 - ИНФОРМАТИЧКИ РИЗИЦИ У ОБРАЗОВНО-ВАСПИТНОМ СИСТЕМУ РЕПУБЛИКЕ СРБИЈЕ

Процес имплементације стандарда у пракси подразумева спровођење већег броја активности које су саставни део процене ризика. Међу такве активности спада и спровођење анкета како би се дошло до свеобухватног сазнања о безбедносним ризицима који су присутни у организацији. Осим тога, једном примењени стандард подразумева и периодично анкетирање запослених у организацији – евалуацију стандарда, што представља један вид контроле испуњености стандарда.

У намери да подробније проценимо могућност проширења стандарда СРПС А.Л2.003 категоријом информатичких ризика, покушали смо да сачинимо упитник који би испитао ставове ученика о информатичким ризицима у образовно-васпитним установама. Затим смо упитник тестирали у пилот истраживању којим су обу-

31) Појмови *сајбер претња* и *сајбер ризик* су шири по обиму од појма *сајбер криминал* будући да они реферирају и на инкриминисане радње али и на оне које у важећим кривичним законицима још увек нису проглашене кривичним делима. Ово појашњење је неопходно узети у обзир како би се избегле семантичке забуне.

хваћена три дома ученика средњих школа како бисмо сазнали њихове ставове о присутности и значају ових ризика.

Методолошки оквир истраживања

Општи циљ пилот истраживања је био да се утврди тренутно стање информатичких ризика једног дела образовно-васпитног система – ученичких средњошколских домова, пратећи одабране параметре, на основу „субјективних" процена учесника у процесима

Дистинкција карактеристика узорка је урађена на нивоу пола и узраста, као структуралних детерминанти. Пратећи статистичке податке у Републици Србији утврђен је приближан однос мушког и женског пола (49%:51%) у стратуму, а намера код узрасне структуре је била да млађих испитаника (1. или 2. разред средње школе) буде приближно исто као и старијих (3. или 4. разред средње школе) – 54% : 46%.

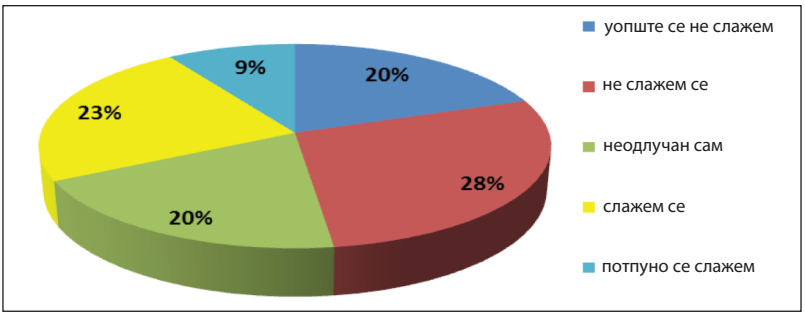
Применом одабраних статистичко-аналитичких метода (дескрипција путем конфигурације појаве и хомогености и инференцијална статистика на нивоу тестирања хипотезе путем т-теста средњих вредности) су квалитативно изражена мишљења респондената превођена у квантитативно изражене показатеље.

Као непосредно средство за евидентирање ставова испитаних лица коришћен је анкетни упитник. Подаци су прикупљени методом анкетирања лицем у лице. Први део упитника, базиран на затвореним питањима, са оценама у виду Ликертове скале (1 – потпуно се слажем, 2 – слажем се, 3 – неодлучан сам, 4 – не слажем се, 5 – уопште се не слажем) садржао је сет од четрдесет тврдњи, док је у другом делу испитаницима дата могућност да у форми отвореног одговора, својеврсног коментара на тематику/упитник, допишу своја запажања.

Узорак је обухватио 163 респондента, а само теренско истраживање обављено је у периоду 03.09.- 17.09. 2012. У циљу ефикасне анализе података формирана је електронска база података у коју су евидентирани сви прикупљени подаци, а потом је извршена њихова нумеричка обрада. Показатељима дескриптивне и делом инференцијалне статистике индиковане су све оцене и ставови испитаника.

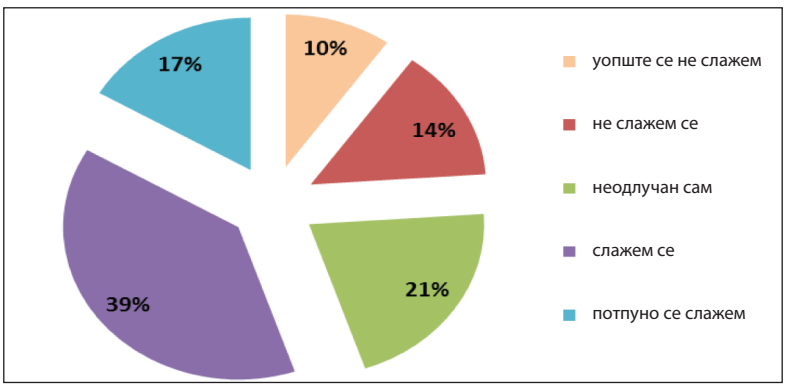
Преглед резултата истраживања и закључци

Дистрибуција одговора испитаника на исказ: *Ученици у дому могу постати жртве криминала и других злоупотреба које се изводе путем Интернета*



Иако највећи број испитаника (48%) сматра да ученици у дому не могу постати жртве криминала и других злоупотреба које се изводе путем Интернета, податак да 32% ученика сматра да може постати жртва криминала и других злоупотреба у сајбер простору никако није статистички занемарљив. Такође, значајан је број неодлучних испитаника који чине 20% од укупног броја. Треба имати у виду да општа слика о неодлучности испитаника (средња оцена 2.74) није репрезентативна, јер је коефицијент варијације висок и износи 46%, као и стандардна девијација која износи 1.27.

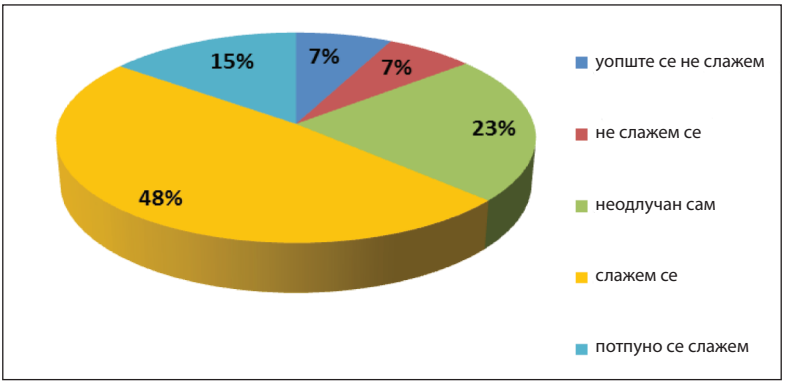
Дистрибуција одговора испитаника на исказ: *Ученици су довољно обавештени о опасностима од криминала и других злоупотреба које се изводе путем Интернета*



Забрињавајуће је да 24% ученика мисли како нема довољно информација о опасностима у сајбер простору. Поново се јавља ситуација високог степена неодлучности испитаника, где се тако изјашњава њих 21%. Просечна оцена од 3.38 показује управо поменути став, али није поздана слика популације, јер су високе вредности и стандардне девијације (1.20) и коефицијента варијације (36%). Узимајући у обзир овај податак, можемо закључити ка-

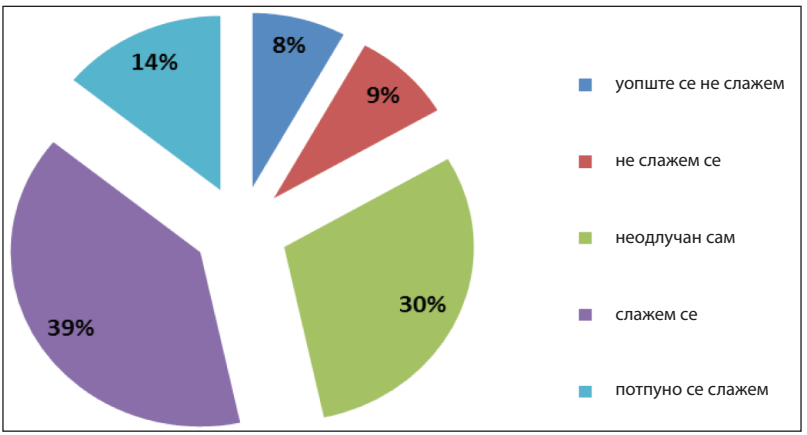
ко готово половина ученика не тврди да је довољно обавештена о ризицима коришћења Интернета.

Дистрибуција одговора испитаника на исказ: *Сматрам да би боља обавештеност ученика значајно смањила опасност од злоупотреба и криминала путем Интернета*



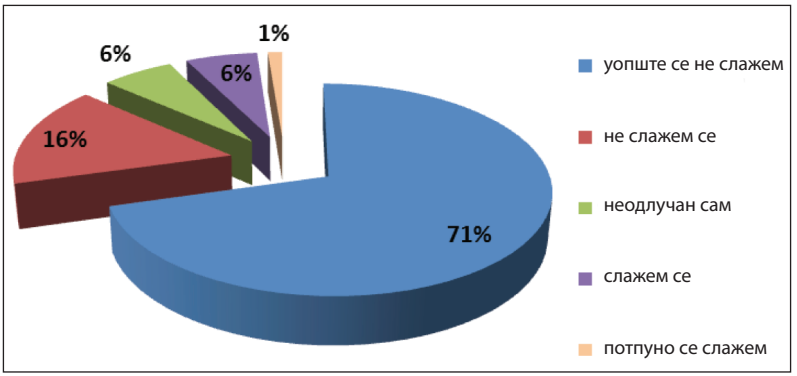
Већина испитаника (63%) сматра да би боља обавештеност ученика значајно смањила опасност од злоупотреба и криминала путем Интернета, али поново са значајно високим степеном неодлучности код испитаника (23%). Просечна вредност од 3.56 може се сматрати поузданом, иако са граничном вредношћу (стандардна девијација 1.06; коефицијент варијације 30%).

Дистрибуција одговора испитаника на исказ: *Сматрам да би боља обавештеност васпитача значајно смањила опасност од злоупотреба и криминала путем Интернета*



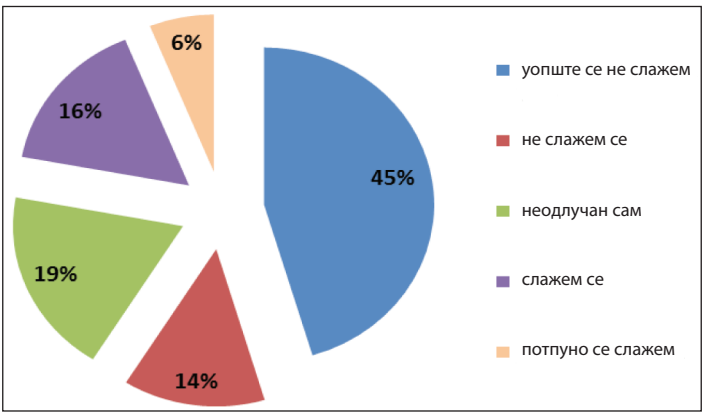
Већина испитаника (53%) сматра да би боља обавештеност васпитача значајно смањила опасност од злоупотреба и криминала путем Интернета, а велики је број неодлучних испитаника по овом питању, чак 30% њих. Средња вредност од 3.43 указује управо на недостатак става испитаника по поменутом исказу, али није поздани репрезент серије података, јер је стандардна девијација 1.09, а коефицијент варијације 32%. На неравномерну расподелу посебно утиче чак 30% неодлучних испитаника.

Дистрибуција одговора испитаника на исказ: *Ја сам био жртва сајбер насиља (узнемиравања, вређања, прогањања и клеветања на Интернету и друштвеним мрежама)*



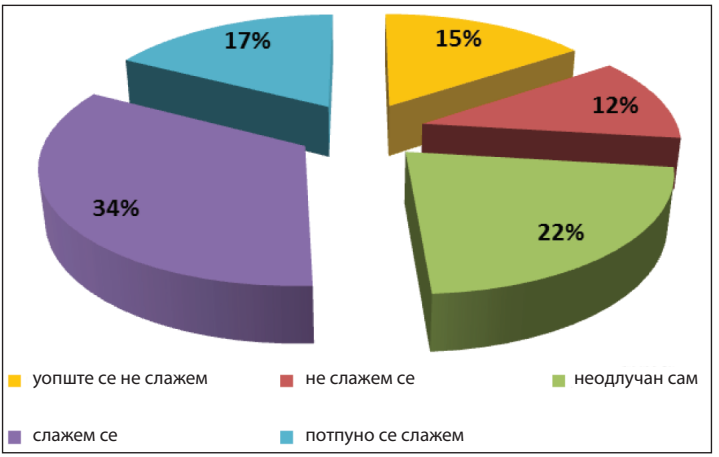
Индикативан је податак да је 7% испитаника изјавило како је било жртва сајбер насиља. Међутим, коначан став о овом проблему можемо да заузмемо тек након анализе следећег одговора.

Дистрибуција одговора испитаника на исказ: *Сматрам да не бих постао жртва сајбер насиља да сам био боље информисан о опасностима које вребају Интернетом*



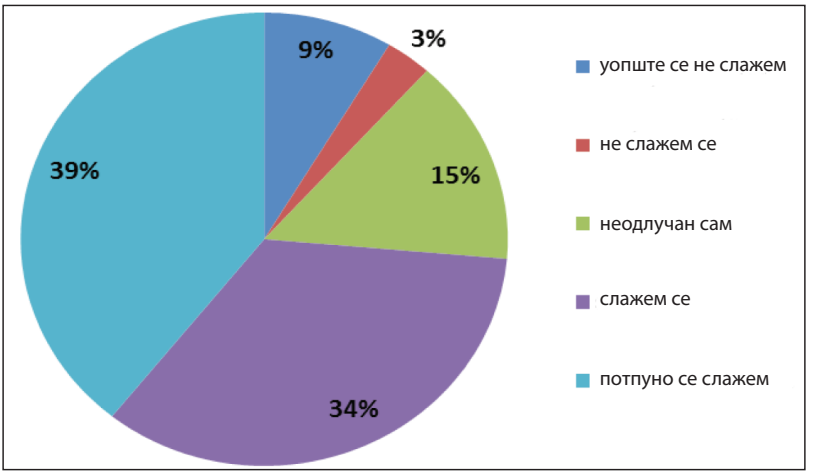
Готово исти проценат као у претходном одговору снажно подржава тврдњу да би додатна едукација значајно смањила опасност од сајбер насиља. Уз то, занимљиво је да још 16% испитаника увиђа потребу за додатном едукацијом, што говори да је број оних који препознају опасности које произлазе из неинформисаности значајно већи од броја оних који су били жртве сајбер насиља. Треба узети у обзир и чињеницу да став испитаника није хомоген - средња вредност од 2.24 не представља адекватно комплетну серију података, јер је висок коефицијент варијације и износи 60%, а стандардна девијација је 1.34.

Дистрибуција одговора испитаника на исказ: *Некима од мојих другова је украдена лозинка за приступ e-mail-у, друштвеној мрежи или програму за „четовање“*



Већина испитаника (51%) наводи да зна за случајеве да је њиховим друговима украдена лозинка за приступ e-mail-у, друштвеној мрежи или програму за четовање.

Дистрибуција одговора испитаника на исказ: *Сматрам да крађа лозинке или виртуелног идентитета на друштвеној мрежи може створити реалну опасност по ученика (физичка опасност, нарушавање психичког интегритета)*



Већина испитаника (73%) сматра да крађа лозинке или виртуелног идентитета на друштвеној мрежи може да створи реалну опасност по ученика (физичка опасност, нарушавање психичког интегритета). Наведени податак сматрамо веома важним. Ипак, просечна оцена од 3.93 не може се сматрати поузданим репрезентом серије података, јер је стандардна девијација 1.20 и коефицијент варијације 31%.

Сумирајући резултате нашег истраживања, можемо да констатујемо како информатички ризици представљају реалну претњу савременом образовно-васпитном систему јер их ученици препознају као озбиљан и незанемарљив безбедносни ризик.

Zoran C. Kekovic, Nenad R. Putnik

PROTECTION POLICIES OF THE EDUCATIONAL SYSTEM - ANALYSIS AND SUGGESTIONS FOR IMPROVING

Summary

This paper is dedicated to the analyses of the political approaches and legislative framework in the domain of security risks in the school environment. The authors present, criticize and analyze standards, politics and legal acts and suggest concrete ideas and approaches that could improve processes of identification, analyses and assessment of the security risks in schools. Having that on mind, the authors suggest the adoption of a unique methodological instrument for assessment

of security risk - the national standard SRPS A.L2:003. Simultaneously, the authors propose redefinition of this instrument in certain domains, trying to adjust it to the needs of contemporary educational system. The category of IT risks should, by the authors opinion, became the important part of the risk assessment standard. Finnaly, the authors conducted empiricall study among high school students, confirming the hypotheses about the reality and importance of IT risk in modern society, especially among school-age youth.

Key Words: protection policies of the educational system, security risk, risk assessment, information risks, national standard SRPS A.L2:003

ЛИТЕРАТУРА

Велашевић, Душан, „Заштита података у рачунарским системима“, *Info Science*, Београд, бр. *4(1)*, 1996.

Гашић–Павишић, Слободанка, „Насиље над децом у школи: функција образовних установа у превенцији и заштити деце од насиља“, у зборнику: *Насиље над децом* (уредник : М. Милосављевић), Факултет политичких наука, Београд, 1998.

Кековић, Зоран, Милошевић, Младен, Путник, Ненад, „Проблеми идентификације и класификације безбедносних ризика у школама“, у зборнику: *Безбедносни ризици у образовно-васпитним установама* (уредници: Бранкица Поповић-Ћитић, Слађана Ђурић, Желимир Кешетовић), Факултет безбедности, Београд, 2012.

Зоран Кековић, Младен Милошевић, Ненад Путник, Ненад Комазец, *Процена и одговор на ризике у образовно-васпитним установама применом стандарда СРПС А.Л2.003*, у: Кордић и сар. (уредници), Реаговање на безбедносне ризике у образовно-васпитним установама, Факултет безбедности, Београд, 2012, стр. 55-93

Кордић, Борис, Путник, Ненад, „Друштвене мреже на интернету и безбедност ученика“, у зборнику: *Безбедносни ризици у образовно-васпитним установама* (уредници: Бранкица Поповић-Ћитић, Слађана Ђурић, Желимир Кешетовић), Факултет безбедности, Београд, 2012.

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

Нешић, Снежана, Јовић, Наташа, *Заштита деце од насиља у школама – извештај заштитника грађана и панела младих саветника*, Заштитник грађана, Београд, 2011.

Петровић, Слободан, *Компјутерски криминал*, МУП Р. Србије, Београд, 2001.

Плескоњић, Драган, Мачек, Немања, Ђорђевић, Борислав, Царић, Марко, *Сигурност рачунарских система и мрежа*, Микро књига, Београд, 2007.

Попадић, Драган, *Насиље у школама*, Институт за психологију и УНИЦЕФ, Београд, 2008.

Породични закон (*Службени гласник РС*, бр. 18/05).

Путник, Ненад, *Сајбер простор и безбедносни изазови*, Факултет безбедности, Београд, 2009.

Philpott, Don, Kuenstle, W. Michael, *Education facility security handbook*, Government Institutes, Plymouth, 2007.

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

Закон о електронским комуникацијама (*Службени гласник РС*, бр. 44/10)

Закон о електронском потпису (*Службени гласник РС*, бр. 135/04)

Закон о забрани дискриминације (*Службени гласник РС*, бр. 22/09).

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

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

Законик о кривичном поступку (*Службени лист СРЈ,* бр. 70/01 и 68/02 и *Службени гласник РС*, бр. 58/04, 85/05 - др. закон, 115/05, 46/06, 49/07, 122/08, 20/09 - др. закон и 72/09)

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

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

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

Закон о оглашавању (*Службени гласник РС*, бр. 79/05)

Закон о општем управном поступку (*Службени лист СРЈ,* бр. 33/97 и 31/01).

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

Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела (*Службени гласник 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 основама система образовања и васпитања (*Службени гласник РС*, бр. 72/09, 52/11).

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

Закон о прекршајима (*Службени гласник РС*, бр. 101/05 и 116/08).

Resume

Considering the existing security policies in educational system, expressed through legal acts and the dominant theoretical approaches, the authors have recognized the need for a holistic approach to the problem of educational system security. Having this on mind, they propose the adoption of a common methodological instrument for assessment of security risks in schools, along with its expansion and adaptation to the needs of educational system. Starting from this idea, the authors have conducted empirical research that has confirmed the presence of IT risks among school youth. Identifying relevant and valid indicators on the basis of which the system of measurable outcomes can be established, indicated the following conclusions in the area of IT risks:

- Students, as well as educators / teachers/ employed in educational institutiones, are not sufficiently educated on the key elements of managing IT risks.
- The majority of respondents believe that cyber crime is a real danger because, according to their assessment, the security measures are not sufficient. The respondants also believe that training and education in this domain are very important.
- Most students consider themselves sufficiently informed about the dangers of the Internet usage (crime, different types of abuse), but also belive that additional education in the area could significantly reduce or prevent risks that arise in the cyber space.

Considering the structure and type of the questionnaire that have been used in this study, the authors concluded:

- The Likert scale, that includes the statement "I am undecided" as one of the options, is not appropriate for the younger population when it comes to topics that they are not thoroughly familiar with or/and when the process is not very well prepared previously.
- The use of questionnaires with the dominant choice questions is appropriate for the needs of risk assessment in the field of security.
- Assessment of risk based on the principle of complementary indicators of qualitative type, with the addition of quantitative as appropriate (measurable sets of testimony), following the concepts defined in the standard SRPS A.L2.003, with the inclusion of the IT risks, is applicable to the educational system.

* Овај рад је примљен 10. фебруара 2013. године а прихваћен за штампу на састанку Редакције 04. марта 2013. године.