

# **ZAŠTITIMO ĐECU – NAUČIMO IH DA PREPOZNAJU I POBIJEDE IZAZOVE NA DRUŠTVENIM MREŽAMA**

## *PRIJEDLOZI ZA AKTIVNI PRISTUP NASTAVI INFORMATIKE U OKVIRU PREVENCIJE ON-LINE NASILJA*

### **1. UVOD**

Školske 2005/06. godine započeo je Projekat „Škola bez nasilja - sigurno školsko okruženje“ u saradnji Ministarstva prosvjete i Kancelarije UNICEF-a u Crnoj Gori. Namijenjen je učenicima, nastavnom i vannastavnom osoblju, roditeljima i cjelokupnoj zajednici s ciljem da smanji i spriječi nasilje među školskom decom. Sprovedene su obuke, pripremljeni Priručnik za rad, Brošura za roditelje, Upitnik za procjenu vršnjačkog nasilja, Uputstvo „Podjela odgovornosti i postupanje u cilju prevencije i u slučajevima pojave nasilja“.

Kancelarija UNICEF-a u Crnoj Gori sprovodi inicijativu "Zaštita dece od seksualne zloupotrebe na internetu" (dio Unicef Globalnog programa). U okviru pomenute inicijative posebna komponenta predviđena je za jačanje svijesti dece i mladih u cilju zaštite i što boljeg i pametnijeg korišćenja interneta. U tom smislu, predviđena je izrada aplikacije za mobilne telefone i kompjutere koja će pružiti mladim ljudima, roditeljima mogućnost da se informišu o oblicima seksualne zloupotrebe dece na internetu i načinima prijavljivanja nadležnim službama.

Na osnovu istraživanja koje je kancelarija Zaštitnika ljudskih prava i sloboda u Crnoj Gori sprovela u 2013. godini, svako četvrto dijete je kazalo da je putem društvenih mreža primilo poruku ili sadržaj koji je seksualno uznemiravajući.

Stoga je cilj ovog materijala jačanje kapaciteta obrazovnog sistema kako bi odgovorio na pojavu različitih vidova nasilja nad/među decom, zapravo uspostavljanje i unaprjeđivanje međusektorske saradnje kao neophodnog uslova za blagovremeno i kvalitetno rješavanje problema nasilja, kao i osnaživanje dece i roditelja da prepoznaju nasilje i na adekvatan način postupaju u navedenim slučajevima.

## **2. PROGRAM: „PREVENCIJA NASILJA U ŠKOLAMA - 2016 GODINA“**

U saradnji sa kancelarijom UNICEF-a u Crnoj Gori je koncipiran Program: „Prevenција nasilja u školama - 2016 godina“ čija je jedna od komponenti: *ojačati vještine dece koje će doprinijeti prevenciji i zaštiti od onlajn nasilja kroz redovnu nastavu.*

Da bi đeca i mladi uspostavili vještine sopstvene zaštite tokom korišćenja interneta potrebno je razviti program prevencije nasilja na društvenim mrežama i obučiti nastavnike predmetnih programa Informatika za osnovnu i srednju školu u vezi sa tim.

Shodno tome, pripremili smo dodatni materijal za grupu predmetnih programa u osnovnom i srednjem obrazovanju koji uključuju ciljeve koji se tiču tematike prevencije nasilja na društvenim mrežama.

Materijal će sadržati uvodni, teorijski i programski dio, teorijski osvrt, definisanje pojma, regulative u Crnoj Gori i ponuđene ideje za izvođenje (dopunu) časa.

### 3. POLAZIŠTE U PREDMETNIM PROGRAMIMA

U skladu sa aktivnostima definisanim strukturnim reformama u oblasti obrazovanja i vaspitanja, na osnovu svakodnevne komunikacije sa obrazovno-vaspitnim ustanovama, rezultata analiza i istraživanja, revidirani su predmetni programi osnovne škole i za opšte obrazovanje (gimnazije), kao i opšte obrazovni predmetni programi za stručne škole. Proces ima za cilj da deci pruži više od poucnog i elementarnog čitanja, pisanja i računanja i podstakne razvoj znanja, vještina i stavova koji će omogućiti da odgovore na zahtjeve koje postavljaju srednja škola, porodica, tržište rada i društvo.

Među njima je i Informatika za VI razred osnovne škole. Kroz ovaj nastavni predmet učenici/ce treba da steknu osnovnu informatičku pismenost i afinitet za korišćenje informaciono-komunikacionih tehnologija i prednosti koje donose. Integrisanje informaciono-komunikacionih tehnologija u cilju efikasnijega obrazovanja neminovan je proces uslovljen društvenim i tehnološkim promjenama. Osnovna informatička pismenost dio je opšte pismenosti i kulture pojedinca u današnjem vremenu. U nastavi učenik/ca treba da, između ostaloga, sazna glavne koncepte ICT-a, spozna opasnosti od neumjerenoga i nepravilnoga korišćenja ICT-a, kao i destruktivnoga i kriminogenoga sadržaja s interneta. Dakle, učenicima se ukazuje na značaj bezbjednosti i zaštite podataka.

U skladu sa navedenim, u jednom operativnom cilju eksplicitno se ukazuje u okviru teme: Internetski servisi da *učenik/ca treba da*: zna principe sigurnog korišćenja interneta; umije da prepozna opasnosti od neadekvatnoga korišćenja interneta; zna principe zdravoga korišćenja interneta i načine zaštite dece na internet; zna načine zaraze računara malicioznim programima sa nesigurnih lokacija; razumije važnost nedavanja ličnih podataka (imena, adresa, šifri...) na nesigurnim lokacijama; razumije važnost obavještavanja roditelja/nastavnika o svim primijećenim problemima. Takođe, da zna principe sigurnosti pri online komunikacijama, kao što su: pojam lažne i neželjene pošte (spam); razumije osnovne načine krađe važnih informacija o korisniku (phishing); zna pravila lijepoga ponašanja na mreži (netquette).

Osim toga, *Strategijom razvoja informacionog društva Crne Gore do 2020* prepoznato je da je potrebno povećati broj obučenih nastavnika o IT bezbjednosti. U skladu sa tim i *ECDL standardima* obučeno je preko 2000 nastavnika da koriste računare, kao i 150 nastavnika za neposrednu primjenu i rad po standardu za IT bezbjednost.

#### 4. SIGURNOST ĐECE

Ministarstvo prosvjete značajnu pažnju i veliki broj aktivnosti usmjerava ka ovoj problematici. Na Školskom portalu nalazi se stranica o bezbjednosti dece na internetu: <http://www.skolskiportal.edu.me/Pages/Bezbjednostdjecenainternetu.aspx>

Osnovna funkcija mehanizma je sprječavanje širenja slika i video materijala na kojima je prikazana seksualna zlostreba dece, kao i fizički i psihološki napadi na decu. Nudi se niz uputstava u smislu potrebnih znanja, informacija, direktna pomoć u situaciji kada do deteta dođe poruka nelegalnog sadržaja ili kad se desi sajber incident.

Naime, deca i roditelji, ovde mogu prijaviti nelegalni sadržaj kojim se na internetu ugrožavaju prava, zdravlje i dostojanstvo deteta. Prijava se podnosi na jednostavan način, popunjavanjem elektronskog formulara. Opcija “Hrabro sanduče” omogućava da se sve vrste zlostrebe dece na Internetu prijave insituciji Zaštitnika ljudskih prava i sloboda u Crnoj Gori.

Takođe, ukoliko je došlo do sajber incidenta koji se tiče web sajta, društvenog naloga, krađe identiteta, online prevare i slično postoji opcija da se i to prijavi.

Prijava nelegalnog sadržaja ili računarskog incidenta se prijavljuje CINTR - timu za odgovor na računarske incidenate - [www.cirt.me](http://www.cirt.me).

U saradnji sa kancelarijom UNICEF-a razvijena je aplikacija za pametne telefone koja se zove *NET prijatelji*. Kroz ovu aplikaciju deca uzrasta od 9 do 11 godina mogu da nauče kako da koriste internet bezbjedno.

Aplikacija sadrži edukativnu igricu koja vodi decu kroz realne životne scenarije i uči ih da prepoznaju, spriječe, zaustave i prijave nasilje na internetu. Takođe, sadrži opciju da se on-line nasilje prijavi.

Ona nije namijenjena samo deci već i njihovim roditeljima i nastavnicama. Ova igrica može biti povod za razgovor sa nastavnicima i roditeljima ali, prije svega, nastavno sredstvo u preventivne svrhe.

Aplikacija NET Prijatelji je besplatna i može se učitati sa svake Iplay i Google play prodavnice. Baner aplikacije se nalazi na sajtu UNICEF-a [https://www.unicef.org/montenegro/campaigns\\_29976.html](https://www.unicef.org/montenegro/campaigns_29976.html), kao i na prethodno pomenutom portalu Ministarstva prosvjete.

## 5. IDEJE ZA IZVOĐENJE (DOPUNU) ČASA

U tekstu koji slijedi dajemo prijedloge koji se mogu prilagođavati za realizaciju nastave u okviru Predmetnoga programa Informatika sa ciljem jačanja kompetencija učenika da štite sebe i druge od nasilja na društvenim mrežama.

### 5.1. Aktivna nastava

Za uspješan čas neophodna je artikulacija nastavnog časa tj. strukturiranje obrazovno-vaspitnog procesa u jedinici vremena. Kako propisi i struka nalažu, nastavnici izrađuju pripreme ili scenarije za čas.

Putem scenarija se težište nastave pomjera sa nastavnika na učenike. Može se planirati jedan čas, ali u okviru veće cjeline (npr. bloka časova, ciklusa većeg broja časova).

Akcent je na tome što će raditi učenici tokom časa (opisuju se nastavne situacije u koje će biti uključeni, aktivnosti i zadaci na kojima će raditi). Dakle, fokus je na procesu (npr. kako pokrenuti određene aktivnosti učenika, kako olakšati pedagošku interakciju među učenicima ili između nastavnika i učenika).

Pitanja o kojima treba razmišljati prilikom izrade scenarija za čas:

---

Da li postoji više povezanih ciljeva učenja za čije ostvarenje je potrebno određeno vrijeme?

Da li je u scenariju opisano ono što rade učenici, a ne samo ono radi nastavnik?

Da li su u scenariju navedene aktivnosti učenika, a ne sadržaj koji treba obraditi (npr. predavanje)?

Da li su u scenariju naglašeni pokazatelji učenja (ciljeva), a ne sam sadržaj lekcije?

Da li je u scenariju nastavnik više u ulozi režisera nego predavača, prenosioca znanja?

## ***5.2. Prijedlozi za dopunu časa***

### **A. Scenario: Internet i mobilni telefoni - situacije**

*Cilj: Ukažati na moguće opasnosti zlorabotrebne interneta i mobilnog telefona; podučiti učenike pravilima sigurnog korišćenja; usmjeriti ih na podršku roditelja i drugih odraslih u situaciji uznemirivanja i elektronskog nasilja.*

Trajanje: 45 minuta

Potreban materijal: olovka, A4 papir, chart tabla i papir, bojice, flomasteri

- Aktivnost: Razgovor u velikoj grupi na temu koliko i na koji način koriste mobilni telefon i internet – 10 min
- Aktivnost: Crtanje - “Nacrtaj/napiši što ti može pomoći da se ošćaš sigurno dok koristiš mobilni telefon, kako se možeš zaštititi od neprijatnosti.
- Aktivnost: Kroz rad u malim grupama učenici diskutuju o pozitivnim i negativnim iskustvima u korišćenju telefona i interneta. Navode tri osobe kojima se mogu obratiti ako ih neko uznemirava putem telefona.” – 30 min
- Nastavnik skuplja radove, razvrstava ih i sumira preporuke – 5 min

## B. Scenario: Internet i mobilni telefoni – prednosti, opasnosti

*Cilj: učenici prepoznaju sa jedne strane prednosti, ali i opasnosti sa kojima se mogu suočiti tokom korišćenja društvenih mreža.*

Trajanje: 45 minuta

Potreban materijal: olovka, A4 papir, chart tabla i papir, bojice, flomasteri

- Aktivnost : pišu odgovore na pitanja:
  - Služiš li se mobilnim telefonom?
  - Za što ga koristiš?
  - Koliko često posećuješ internet stranice?
  - Koje su ti omiljene stranice?
  - Je li neko od roditelja prisutan kad ideš na internet? – 10 min
- Nakon toga se dijele u grupe, sažimaju i predstavljaju odgovore – 20 min
- Nastavnik na tabli piše dvije kolone koje popunjava kroz diskusiju na nivou odjeljenja. U lijevoj unosi dobre stvari, u desnoj prepoznaje rizike – 15 min

Zabavne i korisne strane korišćenja	Opasnosti ako nijesmo oprezni prilikom korišćenja.
-	-
-	-
-	-

### C. Scenario: Društvene mreže: prihvatljivo/neprihvatljivo! Što izbjegavati?

*Cilj: Da učenici prepoznaju prihvatljivo, ali i što treba izbjegavati na društvenim mrežama.*

Trajanje: 45 minuta

Potreban materijal: olovka, A4 papir, chart tabla i papir, bojice, flomasteri.

- Učenici, najprije, na nivou malih grupa smišljaju promotivni argument zbog čega treba i valja koristiti telefon i internet.
- U skladu sa tim treba da osmisle letke u kojima će biti poruke što nije prihvatljivo i što treba izbjegavati dok se koristi telefon i internet.
- Nakon toga sastavljaju *vodič za samozastitu*: učenike podstaći da sami kažu što više pravila i savjeta koji im pomažu da se osećaju sigurno dok se koristi telefon i internet. Kada završe ponuditi im sljedeću listu, kako bi odabrali stavke za sopstveni *vodič za samozastitu*:
  - Pažljivo odluči kome ćeš dati broj telefona i svoju *e-mail* adresu.
  - U redu je prekinuti razgovor ili dopisivanje zbog kojeg se osećaš loše ili neprijatno.
  - Oprezno koristi *chat* uslugu putem telefona i na internetu.
  - Ne odgovaraj na poruku s nepoznatog broja ili *e-mail* adrese niti s poznatog ako se zbog sadržaja poruke osećaš loše ili neprijatno.
  - Nemoj slati fotografije ili videozapise, kao ni sadržaje koji mogu uvrijediti druge ljude.
  - Razgovaraj s roditeljima ili nekom drugom odraslom osobom kad se pojavi problem, kako se ne bi pogoršao.
  - Ako ti neko pošalje zlonamjernu ili prijeteću poruku putem telefona (viber, sms) ili elektronske pošte (*e-mail, na fb*), nemoj odgovoriti. Pokaži je odrasloj osobi kojoj vjeruješ.
  - Budi pažljiv kada šalješ SMS i *chat* poruke drugima: nemoj slati ili prosljeđivati poruke koje mogu dovesti druge u neuprijatnu situaciju, osramotiti ih, izložiti ismijavanju, vrijeđanju...
  - Nemoj u ljutnji učiniti nešto što zbog čega ćeš kasnije zažaliti. Prije svega se zapitaj kako bi se ti osećao/la kada bi dobio tu poruku i može li ona uvrijediti ili na bilo koji način nanijeti štetu osobi kojoj šaljete. Oprez, jer i šala može uvrijediti.



- Zaštiti sebe lozinkom, pazi kome je daješ jer oni koji ti se predstavljaju kao prijatelji u nekom trenutku mogu postati neprijatelji.
- Ne navodi lične informacije, brojeve telefona, adresu, ime škole u koju ideš ili mjesta đe izlaziš osobama koje ne poznaješ uživo. Kada pišeš o sebi, piši uopšteno. Sve što napišeš i objaviš u sms poruci ili na internetu postaje javno i dostupno velikom broju ljudi i više ne možeš kontrolisati kako će drugi iskoristiti te podatke.
- Ne šalji i ne objavljuj svoje i fotografije prijatelja putem telefona i interneta. Jednom kada pošalješ ili objaviš fotografiju, nad njom više nemaš kontrolu, ne znaš što se dalje događa. Uz malo vještine i, sa osnovnim grafičkim programima, moguće su razne fotomontaže i zloupotrebe.
- Neki odrasli i vršnjaci lažno se predstavljaju i pretvaraju da su prijatelji jer ih zanimaju slike seksualnog sadržaja ili imaju seksualne namjere. Zbog toga budi oprezan/na, ne samo sa informacijama i fotografijama koje dijeliš, nego i pri upoznavanju internetskih prijatelja. Upozoravamo da sve što znaš o tom “prijatelju” je ono što ti je ta osoba rekla i ništa od toga ne mora biti istina.
- Ako želiš da uživo upoznaš svog internetskog prijatelja, dogovori prvi susret na javnom mjestu, đe ima dosta ljudi. Povedi nekoliko prijatelja/ca ili odraslu osobu kojoj vjeruješ – ne idi sam/a.
- Nemoj prikrivati nasilje - odmah obavijesti odrasle o tome što se događa.
- Čuvaj sebe i druge!

## D. Scenario: SMS poruka i poruke na internetu

*Cilj: da prepoznaju i suoče se sa time kako poruke mogu uticati na nekoga; osvijeste svoje ponašanje na društvenim mrežama, ličnu odgovornost.*

Trajanje: 45 minuta

Potreban materijal: Stikeri, olovke, list iz sveske

- ✓ Prva aktivnost – Poruke – 25 min
- Uputstvo za učenike: “Zamislite da pišete poruku drugu/ici. Uzmite papirić i napišite. Napisanu poruku ubaci u vrećicu. Sada izvlačimo poruke i definišemo ih u tabeli. Ukoliko su sve pozitivne, nastavnik pomaže da se osmisli primjer za neutralne ili uznemirajuće. – 15 min

Zabavna i podržavajuća poruka	Uznemirujuća i povređujuća poruka

- Slijedi razgovor o situacijama koliko često se susrijeću sa uznemirujućim i povređujućim porukama. A) Ko ih šalje? B) Kada? C) Kako reaguju u tim situacijama? – 10 min
- Nastavnik sumira u smjeru time kako poruke mogu uticati na nekoga; kako se neki ponašaju na društvenim mrežama, kako učenici/ce mogu i treba da prepoznaju ličnu odgovornost.
- Za kraj osmišljavaju igrokaz u kojem će prikazati primjeren način rješavanja situacije: a) Kako asertivno saopštiti da ti nešto ne prija i da sa time druga osoba treba da prestane?! b) Kome i kako bi se obratili?!

## **E. Scenario: Sigurno ponašanje - Vrijednosti, pravila i posljedice**

*Cilj: ojačati učenike/ce za sigurno ponašanje; dodati odjeljenskim vrijednostima, pravilima koja se tiču vršnjačkog zlostavljanja vrijednosti, pravila koja će štititi i od elektronskog nasilja.*

Trajanje: 45 minuta

Potreban materijal: plakat s odjeljenskim vrijednostima, pravilima, veliki papiri za izradu novih plakata, bojice, flomasteri i sl.

- Učenici nabrajaju što su naučili, kao i vrijednosti prema kojima žele da se ponašaju, kojih će se pridržavati kako bi spriječili zloupotrebe i da bi se svi osjećali sigurno i ugodno.
- Osmišljavaju precizne rečenice u formi pravila kojima definišu nepoželjno ponašanje, neprihvatljive i situacije koje treba izbjegavati?
- Istovremeno definišu što treba uraditi u slučajevima kada se zloupotreba dogodi.
- Od izlistanih rečenica/pravila izrađuju poster koji će biti postavljen na vidnom mjestu u učionici.

## 6. DODATNE KORISNE INFORMACIJE

Da bismo učenicima omogućili sigurno i bezbjedno okruženje za rast, razvoj i formiranje ličnosti u savremenom kontekstu nudimo još nekoliko korisnih informacija koje možete iskoristiti prilikom osmišljavanja i realizacije nastavne prakse.

Pri Odjeljenju za ICT Ministarstva prosvjete kreirani su on-line kvizovi za učenike osnovnih škola. Predlažemo ih kao interaktivni materijal u nastavi sa svom decom jer su koncipirani tako da ga svi mogu raditi. Adresa je [www.pokazistaznas.edu.me](http://www.pokazistaznas.edu.me). Sam kviz i rezultati koji se dobiju mogu se podijeliti i na facebook stranici/ama. Ovo može biti motivaciono i zanimljivo deci.

Takođe, za primjenu u crnogorskim školama moguće je koristiti program koji je pripremio UNICEF – Republika Hrvatska „Prekini lanac – zaustavimo elektroničko nasilje“. Link se nalazi na stranici Školskog portala o bezbjednosti dece na internetu: <http://www.skolskiportal.edu.me/Pages/Bezbjednostdjecenainternetu.aspx>.

Konačno, aplikacija za pametne telefone NET Prijatelji, kojom деца od 9 do 11 godina na jedan zabavan način uče kako da budu bezbjedna na internetu, biće uskoro dostupna svoj deci (na sajtu UNICEF-a i Ministarstva prosvjete). Kancelarija UNICEF-a u saradnji sa Ministarstvom prosvjete radi na izradi verzije za kompjutere. Na taj način će sva деца moći da je koriste na časovima informatike mnogo jednostavnije. Razvojno je adekvatna, zanimljiva, urađena u obliku video igrice sa duhovitim rješenjima koja deci drže pažnju tokom njenog trajanja. Međutim, ona ih uči da prepoznaju rizik i opasnost, kako da ga izbjegnu i kome da prijave nasilje na internetu. Dakle, može biti korisno nastavno sredstvo u okviru realizacija ciljeva predmetnih programa Informatika.

## 7. Prilog: ECDL – IT sigurnost: Nastavni plan (Syllabus) Verzija 1.0

### Modul 7–IT sigurnost

U modulu 7 IT sigurnost su navedeni koncepti i vještine koje se odnose na razumijevanje bezbjednog korišćenja ICT u svakodnevnom životu. Nastavni plan obuhvata korišćenje relevantnih tehnika i aplikacija za održavanje bezbjedne konekcije na mrežu, bezbjedno i sigurno korišćenje interneta, kao i upravljanje podacima i informacijama na odgovarajući način.

### Ciljevi modula

Kandidat bi trebalo da:

- Razumije ključne koncepte koji se odnose na važnost bezbjednosti informacija i podataka, fizičku sigurnost, privatnost i krađu identiteta
- Zaštiti računar, uređaj ili mrežu od zlonamjernih programa i neovlašćenih pristupa
- Razumije razne vrste mreža, konekcija i specifična pitanja vezana za mrežu uključujući i zaštitni zid (firewall)
- Pretražuje veb i bezbjedno komunicira putem interneta
- Razumije sigurnosna pitanja u vezi sa komunikacijom, uključujući e-mail i instant poruke
- Pravi kopiju podataka (back up), povrati (restore) podatke na odgovarajući i bezbjedan način i da bezbjedno raspolaže podacima i uređajima

POGLAVLJE	OBLAST	OZNAKA	CILJEVI
1. Koncepti bezbjednosti	1.1 Podaci	1.1.1	Praviti razliku između podataka i informacija.
		1.1.2	Razumjeti pojam sajber kriminal
		1.1.3	Razumjeti razliku između termina hakovanje, krekovanje i etičko hakovanje.
		1.1.4	Prepoznati prijetnje podacima kao što su: vatra, poplava, rat i zemljotres.
		1.1.5	Prepoznati prijetnje podacima od strane zaposlenih, servis provajdera i pojedinaca iz spoljnog okruženja.
	1.2 Važnost informacija	1.2.1	Razumjeti razloge za zaštitu ličnih podataka: krađa identiteta i prevara.
		1.2.2	Razumjeti razloge za zaštitu osjetljivih poslovnih informacija: krađa ili zloupotrebe detalja klijenata i finansijskih informacija.
		1.2.3	Identifikovati mjere za sprečavanje neovlašćenog pristupa podacima, kao što su šifrovanje (enkripcija) i lozinke.
1.2.4		Razumjeti osnovne karakteristike bezbjednosti informacija kao što su: povjerljivost, integritet i dostupnost.	

		1.2.5	Identifikovati vrste zaštite podataka i privatnosti, kontrolu pristupa podacima i sl. u vašoj zemlji.	
		1.2.6	Razumjeti važnost kreiranja i pridržavanja smjernica i politike korišćenja ICT.	
		1.3 <i>Lična sigurnost</i>	1.3.1	Razumjeti termin socijalni inženjering i implikacije kao što su: prikupljanje informacija, prevare, pristup sistemu računara.
			1.3.2	Identifikovati metode socijalnog inženjeringa kao što su: telefonski pozivi, phishing, „surfovanje preko ramena“ (shoulder surfing).
	1.3.3		Razumjeti značenje i implikacije termina krađa identiteta: ličnog, finansijskog, poslovnog i pravnog.	
	1.3.4		Identifikovati metode krađe identiteta kao što su: information diving („kopanje po podacima“), skimming („skidanje“ podataka sa magnetne trake), pretexting („Izmišljeni scenario“)	
	1.4 <i>Bezbjednost fajlova</i>	1.4.1	Razumjeti uticaj uključivanja/isključivanja makro naredbi.	
		1.4.2	Postaviti lozinke za fajlove kao što su: dokumenta, kompresovani fajlovi, tabelarne kalkulacije.	
		1.4.3	Razumjeti prednosti i ograničenja šifrovanja (enkripcije).	
<b>2. Zlonamjerni programi</b>	2.1 <i>Definicija i funkcija</i>	2.1.1	Razumjeti pojam zlonamjerni program (malware).	
		2.1.2	Prepoznati različite vrste prikrivenih zlonamjernih programa kao što su: trojans, rootkits i back doors.	
	2.2 <i>Vrste</i>	2.2.1	Prepoznati vrste zlonamjernih programa kao što su virusi i crvi.	
		2.2.2	Prepoznati vrste krađe podataka i zlonamjernih programa za iznudu kao što su: adware (programi za oglašavanje), spyware (špijunski programi), botnets, keystroke logging i diallers („birači“).	
	2.3 <i>Zaštita</i>	2.3.1	Razumjeti način rada i ograničenja antivirusnog programa.	
		2.3.2	Skenirati specifične diskove (drives), foldere, fajlove koristeći antivirus program. Zakazati skeniranje antivirus programa.	
		2.3.3	Razumjeti termin „karantin“ i njegov uticaj na zaražene/sumnjive fajlove.	
		2.3.4	Razumjeti važnost redovnog ažuriranja antivirus programa.	
	<b>3. Bezbjednost mreže</b>	3.1 <i>Mreže</i>	3.1.1	Razumjeti termin mreža i razumjeti vrste mreža kao što su: LAN, WAN i VPN.
			3.1.2	Razumjeti ulogu administratora mreže
3.1.3			Razumjeti funkciju i ograničenja zaštitnog zida (firewall).	
3.2 <i>Način povezivanja na mrežu</i>		3.2.1	Prepoznati opcije za povezivanje na mrežu - putem kabla ili bežično.	
		3.2.2	Razumjeti kako povezivanje na mrežu može uticati na bezbjednost: zlonamjerni programi, nedozvoljeni pristup podacima, zaštita privatnosti.	
3.3 <i>Sigurnost bežičnih mreža</i>		3.3.1	Prepoznati važnost zaštite bežične mreže.	
		3.3.2	Prepoznati različite načine zaštite bežične mreže kao što su WEP, WPA, MAC.	
		3.3.3	Biti svjestan da korišćenje nezaštićene bežične mreže može dovesti do neovlašćenog pristupa vašim	

			podacima.
		3.3.4	Pristup zaštićenoj/nezaštićenoj bežičnoj mreži.
	3.4 Kontrola pristupa	3.4.1	Razumjeti svrhu naloga na mreži i pristup korišćenjem korisničkog imena i lozinke.
		3.4.2	Razumjeti važnost i ispravan način kreiranja lozinke - lozinka treba da sadrži slova, brojeve i znakove i sl; treba je redovno mijenjati, ne treba je dijeliti ni sa kim.
		3.4.3	Identifikovati sigurnosne tehnike u kontroli pristupa kao što su: otisci prstiju ili skeniranje zenice oka.
4. Sigurno korišćenje veba	4.1 Veb pretraživanje	4.1.1	Razumjeti da se onlajn aktivnosti, kao što je kupovina ili finansijske transakcije, vrše preko sigurnih veb stranica.
		4.1.2	Identifikovati sigurne veb sajtove: https, lock symbol i sl.
		4.1.3	Razumjeti vrste sajber napada
		4.1.4	Razumjeti termin digitalni sertifikat. Provjeriti valjanost digitalnog sertifikata
		4.1.5	Razumjeti termin jednokratna lozinka.
		4.1.6	Izabrati odgovarajuća podešavanja za omogućavanje i onemogućavanje automatskog unosa i automatskog čuvanja podataka prilikom popunjavanja obrasca.
		4.1.7	Razumjeti termin „kolačić“ (cookie)
		4.1.8	Izabrati odgovarajuća podešavanja za dozvolu ili blokiranje kolačića (cookies).
		4.1.9	Obrisati lične podatke iz veb čitača kao što je: istorija pretraživanja, keširani internet fajlovi, kolačići, automatski unos podataka.
		4.1.10	Razumjeti svrhu, funkciju i vrste programa za kontrolu sadržaja: program za internet filtriranje, programi za roditeljsku kontrolu.
	4.2 Društvene mreže	4.2.1	Razumjeti zašto ne treba postavljati lične i privatne podatke na društvenim mrežama.
		4.2.2	Razumjeti da je potrebno primijeniti odgovarajuća podešavanja privatnosti na nalogima društvenih mreža.
		4.2.3	Razumjeti potencijalne opasnosti pri korišćenju društvene mreže kao što je: uznemiravanje putem interneta, lažni identiteti, zaraženi linkovi ili poruke i sl.
5. Komunikacije	5.1 E-mail poruke (Elektronska pošta)	5.1.1	Razumjeti svrhu šifrovanja (enkripcije) i dešifrovanja (decrypting) e-mail poruka.
		5.1.2	Razumjeti termin digitalni potpis.
		5.1.3	Napraviti i dodati digitalni potpis.
		5.1.4	Biti svjestan mogućnosti primanja lažne i neželjene pošte.
		5.1.5	Razumjeti termin i karakteristike Phishinga (pokušaj preuzimanja informacija) kao što je korišćenje imena ugledne kompanije, ljudi i lažnih linkova.
		5.1.6	Biti svjestan potencijalnih opasnosti uslijed otvaranja priloga koji sadrže makro naredbe ili izvršne fajlove.
	5.2 Instant poruke	5.2.1	Razumjeti termin i svrhu IM – Instant poruka.
		5.2.2	Razumjeti potencijalne opasnosti prilikom razmjene instant poruka kao što su: zlonamjerni programi (malware), backdoor pristup, pristup fajlovima i sl.

		5.2.3	Prepoznati metode obezbjeđivanja povjerljivosti prilikom razmjene IM kao što su: šifrovanje (enkripcija), neobjavlivanje važnih informacija i ograničenja u dijeljenju fajlova.
<b>6. Upravljanje sigurnošću podataka</b>	<i>6.1 Sigurnost i pravljenje sigurnosne kopije podataka</i>	6.1.1	Prepoznati načine za obezbjeđivanje fizičke sigurnosti uređaja - korišćenje brava za kablove, kontrola pristupa i sl.
		6.1.2	Prepoznati važnost procedure pravljenja kopije podataka u slučaju gubljenja podataka, finansijskih izvještaja, istorije pretraživanja i sl.
		6.1.3	Identifikovati karakteristike pravljenja kopije podataka kao što su: frekventnost, lokacija za čuvanje podataka, zakazivanje pravljenja kopije.
		6.1.4	Pravljenje sigurnosne kopije podataka.
	<i>6.2 Trajno uništavanje podataka</i>	6.2.1	Razumjeti razlog za trajno brisanje podataka sa diskova ili uređaja.
		6.2.2	Razlikovati brisanje i trajno uništavanje podataka.
		6.2.3	Identifikovati metode trajnog uništavanja podataka kao što su: korišćenje sjekača papira, uništavanje diskova/medija, razmagnetisavanje, korišćenje pomoćnog programa za uništavanje podataka.