Bosna i Hercegovina
Federacija Bosne i Hercegovine
ZENIČKO-DOBOJSKI KANTON
MINISTARSTVO ZA OBRAZOVANJE, NAUKU, KULTURU I SPORT

KURIKULUM NASTAVNOG PREDMETA
SIGURNOST INFORMACIJA

ZA GIMNAZIJE

Zenica, juni 2023.

Bosna i Hercegovina
Federacija Bosne i Hercegovine
ZENIČKO-DOBOJSKI KANTON
MINISTARSTVO ZA OBRAZOVANJE, NAUKU, KULTURU I SPORT

KURIKULUM NASTAVNOG PREDMETA

SIGURNOST INFORMACIJA

ZA GIMNAZIJE

Zenica, juni 2023.

Kurikulum nastavnog predmeta Sigurnost informacija za gimnazije

Izdavač: Ministarstvo za obrazovanje, nauku, kulturu i sport Zeničko-dobojskog kantona

Za izdavača: Draženka Subašić, ministrica

Voditeljica Stručnog tima:
Aida Salkić, direktorica Pedagoškog zavoda Zenica

Grupa za izradu predmetnog kurikuluma:
mr.sc. Adin Begić, voditelj
mr.sc. Edin Hadžikadunić, koordinator
dr.sc. Almir Sivro, koordinator
Mujo Zeničanin, dipl.ing., član
Zerina Šehović, prof., član
mr.sc. Mehmed Ahmetagić, član

Recenzenti:
prof.dr. Edin Berberović
Ajla Halilović, MA

Tehnička priprema i uređenje:
Pedagoški zavod Zenica

SADRŽAJ

A/ OPIS PREDMETA

Učenje predmeta Sigurnost informacija potiče učenike na stvaranje pozitivnog stava o intelektualnom vlasništvu i stvaranje osjećaja za privatnost u IT komunikaciji. Također, sigurnost informacija učenike potiče za korištenjem kripto zaštite vlastitih i tuđih informacija koje imaju za cilj zajedničko korištenje unutar jedne organizacije. Učenici će stvarati modele zaštite, kreirati će situacije u kojima će koristiti neki vid zaštite. Svjesni smo činjenice da danas postoji veliki broj zlonamjernih programa, pa će učenici naučiti korištenje antivirusnog softvera u skladu sa potrebama. Također, učenjem ovog predmeta učenici će opreznije pristupati društvenim mrežama i naučiti kako da se izražavaju na društvenim mrežama, kako da prepoznaju i spriječe cyberbullying, grooming, sexting i dr.

Pravilnim korištenjem softvera i poštivanjem autora i programera, učenici razvijaju sposobnost poštivanja tuđeg intelektualnog vlasništva. Također, kao budući informatičari, voditi će računa o tome kako da zaštite svoje intelektualno vlasništvo. Učenici će shvatiti da je sigurnost informacija živa materija, da zlonamjerne osobe svakodnevno razvijaju svoje hakerske vještine, tako da će morati konstantno pratiti razvoj novih modela u zaštiti sistema.

Sigurnost informacija predstavlja se kao jedan od najvažnijih strateških ciljeva mnogih razvijenih država svijeta. Bosna i Hercegovina iako zaostaje u ovome, ima za cilj razvoja institucija koje će se baviti zaštitom informacija i zaštitom intelektualnog vlasništva, jer to predstavlja jedan od uvjeta članstva u EU. Učenici će biti u mogućnosti da analiziraju trenutnu situaciju i da kreiraju vlastite ciljeve u razvoju sigurnosti informacija na internetu i na društvenim mrežama.

Učenjem sigurnosti informacija učenici razvijaju sposobnost kreativnog i kritičkog načina razmišljanja. Također, učenici razvijaju komunikacijske sposobnosti na internetu, što se pozitivno odražava na razvoj ličnosti.

Kroz podučavanje ovoga predmeta razvija se vještina pisanja poruka, čitanja informacija, prepoznavanja zamki kroz clickbait i slično. Također, prepoznavanje potencijalne opasnosti u sistemu je jedna od ključnih kompetencija koje će učenici steći učenjem predmeta Sigurnost informacija.

Znanja koja će učenici steći učenjem ovoga predmeta moći će primijeniti i u drugim oblastima kao što su programiranje i baze podataka. Programiranje je usko vezano za zaštitu intelektualnog vlasništva, bilo da samostalno ili u grupi razvijamo program. Također, baze podataka moraju biti zaštićene, jer danas predstavljaju nezaobilazan dio skladištenja podataka. Zamislimo bazu klijenata u jednoj banci, ili bazu artikala jednog trgovačkog lanca. Svi oni zahtijevaju da njihovi podaci budu zaštićeni na sve moguće načine, tako da učenjem ovoga predmeta učenici jačaju svoje kompetencije u ovome polju.

Poznavanjem i korištenjem sigurnosnih protokola i pravila, učenik povećava svoju konkurentnost na tržištu rada, jer ukoliko učenici vladaju ovim pojmovima, tačno znaju šta smiju a šta ne smiju koristiti tokom razvoja aplikacija, aplikativnih rješenja i slično. Također, zaštitom informacija učenici će biti u mogućnosti da pokažu svoju privrženost radnom timu u kojem se nalaze, što kao rezultat daje prednost u zapošljavanju.

Učenje ovog predmeta se odvija interakcijom s drugima u odjeljenju te se podstiče rad u grupama. U podučavanju ovog predmeta potrebno je stvoriti ugodno okruženje u kojem će se učenici lijepo osjećati i u kojem će biti maksimalno uključeni.
Sigurnost informacija pripada oblastima informacione i komunikacione tehnologije i oblastima digitalnog društva. Podučava se u trećem razredu gimnazija u informaciono-komunikacionom području, na bazi 35 nastavnih sati godišnje.

B/ CILJEVI UČENJA I PODUČAVANJA PREDMETA

Ciljevi učenja i podučavanja nastavnog predmeta Sigurnost informacija su:

1. Razviti osobine važne za prepoznavanje intelektualnog vlasništva, autorskog prava i licence softvera.
2. Analizirati i razmatrati stavove u vrijednosti ličnog i timskog rada, usvojiti potrebu stalnog usavršavanja i cjeloživotnog učenja, kritički vrednovati vlastiti i rad drugih.
3. Koristiti različite algoritme i alate vezane za zaštitu informacija, kriptovati i dekriptovati poruke na različite načine s ciljem upoznavanja vlastitih sklonosti i mogućnosti.
4. Razvijati i razumijevati kulturu ophođenja i komunikacije na društvenim mrežama iz različitih platformi (facebook, instagram, edukativne društvene mreže i dr.), analizirati zloupotrebu podataka i cyberbulling, mijenjati sigurnosne postavke na društvenim mrežama s ciljem bolje zaštite informacija.
5. Prepoznati zlonamjerni softver i adekvatno reagovati na prijetnju, primijeniti pravila zaštite, koristiti antivirusnu zaštitu, prepoznati špijunske prijetnje i otkloniti ih.
6. Razvijati znanja i vještine vezane za izradu rezervnih kopija, vraćanje podataka, arhiviranje te njihovu kompresiju.

C/ OBLASNA STRUKTURA PREDMETNOG KURIKULUMA

Uvod

1. Intelektualno vlasništvo.
2. Privatnost i društvene mreže.
3. Klasična kriptografija.
4. Kriptografski softver.
5. Zlonamjerni softver i zaštita od zlonamjernog softvera.
6. Rezervne kopije podataka.

A. Informacione i komunikacione tehnologije

IKT predstavlja najbolji alat koji nam je dostupan u svakodnevnom učenju, kao i za učenje i rad u online okruženju. Potrebno je stalno praćenje i usavršavanje u korištenju novih hardverskih i softverskih rješenja, da bi se pravilno izabrala tehnologija i odgovarajući softver za primjenu u nekoj oblasti. Da bi se efikasno koristila IKT potrebno je poznavati osnovne informatičke pojmove kao što su vrste memorija i dugotrajnost zapisa u njima, količina memorije koju zauzima neki fajl, brzina prenosa podataka, kreiranje rezervnih kopija. Od brzine koja nam je dostupna na mreži zavisi da li ćemo koristiti tekst, zvuk ili video u komunikaciji sa drugima, pa je potrebna pravilna procjena koja se temelji na navedenim osnovnim informatičkim pojmovima.

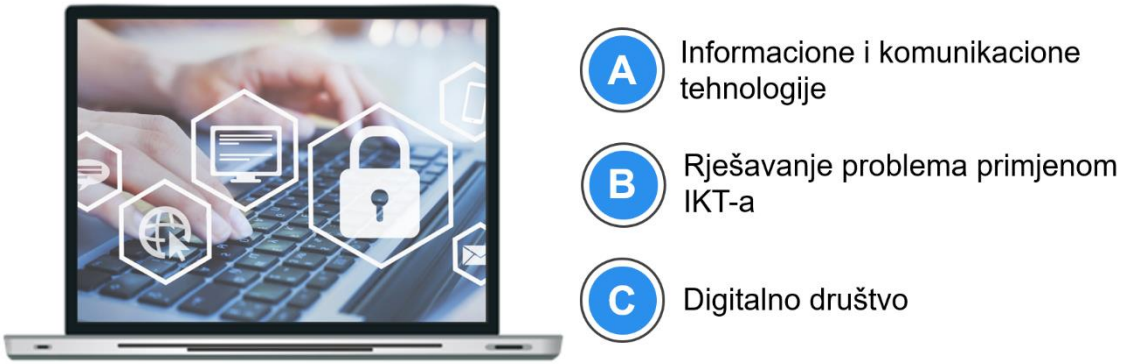
B. Rješavanje problema primjenom IKT-a

Za rješavanje problema koristimo razna softverska rješenja zavisno od toga da li radimo sa brojevima, tekstom, slikama, zvukom, videom. Poznavanje softvera i podataka koje on koristi jako je bitno za pravilan izbor metode za rješavanje konkretnog zadatka. Informacije su svima dostupne na internetu, ali ih je potrebno pronaći. Traženje informacija i postavljanje pravilnog upita je osnovni korak u pronalaženju rješenja za neki problem. Poznavanjem osnovnih pojmova, načela i zakonitosti zajedno sa vještinom pronalaženja informacija na internetu i logičkim povezivanjem i zaključivanjem može se doći do rješenja većine problema koji se postavljaju učeniku. Algoritamsko rješavanje problema predstavlja prevođenje nekog problema iz našeg okruženja u niz koraka koji su prilagođeni računaru. Rješavanje ovakvih problema razvija kod učenika logiku, modeliranje problema, indukciju, dedukciju i apstrakciju. Od korisnika učenik postaje kreator programa koje može dalje usavršavati i dijeliti. Stalno ispravljanje grešaka u programu i usavršavanje i poboljšavanje programa razvija samokritičnost i upornost kod učenika.

C. Digitalno društvo

Prelazak u digitalno društvo se desio toliko brzo da ga još nisu adekvatno regulisale ni države ni obrazovne institucije. Pristup digitalnom društvu bi trebao biti omogućen svakom odraslom čovjeku kao i učenicima, ali pod nadzorom roditelja. Potrebno je imati znanje i vještine za razmjenu informacija, ali i za zaštitu svojih prava i lične sigurnosti. Digitalno društvo olakšava mnoge aspekte života: učenje, podučavanje, bankarstvo, izdavaštvo, rad od kuće, informisanje.

S druge strane potrebna je stalna edukacija da bi se zaštitili od raznih zloupotreba i prevara poput krađe identiteta, phishing-a, nasilja na internetu i raznih drugih opasnih radnji na internetu.



Oblasna struktura predmetnog kurikuluma Sigurnost informacija

U nastavku slijedi dio koji se odnosi na odgojno-obrazovne ishode koji su okosnica predmetnog kurikuluma i razrađeni su za svaku od tri oblasti (domene) na kojima se temelji. Odgojno-obrazovni ishodi pomažu nastavnicima u praćenju napretka učenika i u vrednovanju učeničkih postignuća. Tokom pripremanja procesa učenja i podučavanja nastavnik treba povezati odgojno-obrazovne ishode sa sadržajima navedenim u kurikulumu i metodama podučavanja. U tabelama su odgojno-obrazovni ishodi označeni šiframa. Skraćenice poput A.III.1. ili B.III.2. označavaju redom: oblast kojoj ishod pripada (A. Informacione i komunikacione tehnologije, B. Rješavanje problema primjenom IKT-a i C. Digitalno društvo), godinu podučavanja predmeta (III. – treći razred gimnazije), te redni broj odgojno-obrazovnog ishoda koji se podučava u sklopu navedene oblasti (1. – prvi ishod, 2. – drugi ishod, ...). Skraćenice TIT 5.1.3. ili TIT 5.2.1. označavaju poveznice sa Zajedničkom jezgrom nastavnih planova i programa za tehniku i informacione tehnologije definisanoj na ishodima učenja.

D/ ODGOJNO-OBRAZOVNI ISHODI

GIMNAZIJA

3. razred gimnazije /35 nastavnih sati godišnje/

Oblast: A/Informacione i komunikacione tehnologije	
Ishod učenja	**Razrada ishoda**
A.III.1. Analizira pojam intelektualnog vlasništva i zaštite autorskih prava.	• Definiše intelektualno vlasništvo i pojmove vezane za zaštitu autorskih prava. • Opisuje licence i licenciranje softvera. • Razlikuje pojmove vezane za internet piratstvo.
Poveznice sa ZJNPP	**TIT 5.2.3.**
Ključni sadržaji	
Intelektualno vlasništvo. Zakoni i pravna zaštita. Autorsko pravo. Digitalni potpis. Licence i licenciranje softvera (demo, freeware, shareware, adware, open-source). Internet piratstvo. Torenti. Nedostaci korištenja piratskog softvera.	
Preporuke za ostvarenje ishoda	
Prilikom realizacije oblasti na temu intelektualnog vlasništva, poželjno je raditi u grupi i omogućiti učenicima da samostalno istražuju odgovore na tematske cjeline. Potrebno je učenike uvesti u aktuelne zakone koji su na snazi, vezani za zaštitu autorskih prava i intelektualnog vlasništva. Diskutovati sa učenicima na temu vlasništva i na temu autorskih prava. Kada govorimo o licenci i licenciranju softvera, moramo obratiti pažnju na prednosti pojedinih licenci, prednosti u kupovini softvera. Također, trebamo omogućiti učenicima da pokušaju pronaći besplatnu alternativu na neki softver čija je cijena visoka. Učenike trebamo upoznati sa torentima i internet piratstvom, te kako se zaštititi od piratskog materijala. Učenici bi trebali da daju odgovor na pitanje zašto je pogrešno koristiti i koji su sve nedostaci u korištenju piratskog softvera i drugog piratskog materijala koji je dostupan online. Ukoliko škola posjeduje neki licenciran program, bilo bi poželjno da učenici instaliraju isti taj program kao demo verziju ili kao piratsku verziju i da izvrše analizu kako se program ponaša u slučaju ako je instaliran kao demo ili kao piratska verzija u odnosu na licenciran program. Učenike bi bilo poželjno pratiti i vrednovati kroz rad u grupi i kroz intervju. Može se dati projektni zadatak ili laboratorijska vježba gdje će učenici pronaći neke često korištene sisteme za razmjenu piratskog materijala.	
A.III.2. Objašnjava važnost pojmova privatnost i elektronski identitet osobe kroz korištenje društvenih mreža i zaštitu informacija na društvenim mrežama.	• Definiše pojmove privatnost i elektronski identitet. • Koristi tehnologiju za zaštitu i identifikaciju korisnika. • Opisuje elektronsko poslovanje i online plaćanje. • Razlikuje društvene mreže. • Uočava sigurnosne rizike u korištenju društvenih mreža.
Poveznice sa ZJNPP	**TIT 5.1.2. TIT 5.2.1. TIT 5.2.4.**
Ključni sadržaji	
Privatnost. Elektronski identitet. Elektronsko poslovanje. Kripto valuta. Elektronsko plaćanje (plaćanje karticom, paypal-om, virtuelnim novcem, kripto valutom). Društvene mreže.	

Vrste društvenih mreža.
Pravila ponašanja na društvenim mrežama.
Zloupotreba podataka.
Cyberbullying.
Korištenje privatnih i tuđih informacija na društvenim mrežama (fotografije, pisani tekstovi).
Sigurnosne postavke na društvenim mrežama.
Clickbait i botovi.

Preporuke za ostvarenje ishoda

Kroz razne diskusije sa učenicima definisati i analizirati trenutno stanje kada je u pitanju privatnost na raznim društvenim mrežama (facebook, instagram, tiktok, neke edukativne društvene mreže ili sistemi i sl.). Jako je bitno da učenike upoznamo sa neophodnošću čitanja ugovora prilikom registracije na neku društvenu mrežu ili neki sistem jer klikom na dugme "I agree...", ugovor dobija pravnu moć. Uvesti učenike u temu elektronskog poslovanja i provjeriti da li su obavljali kupovinu ili prodaju na nekom sistemu (olx i slično) i poticati ih da opišu svoja iskustva. Provjeriti da li učenici poznaju sve više korišten termin kripto valuta i da li su je imali priliku koristiti. Kroz vježbu bi bilo poželjno da učenici provjere načine plaćanja na internetu i eventualno da otvore neki account sa malim iznosom sredstava i obave online kupovinu da bi se razbijala ta odbojnost i nesigurnost prilikom online plaćanja. Potrebno je uvesti učenike u pravilno korespondiranje i instant razmjene poruka na društvenim mrežama. Dati zadatak učenicima da istraže da li je došlo do zloupotrebe podataka na nekoj društvenoj mreži, npr. da li je neko nekoga neovlašteno fotografisao i sl. Također, dati učenicima da napišu sastav o cyberbullying-u i provjeriti da li su oni nekada bili žrtve nasilja na internetu. Učenike bi bilo poželjno pratiti i vrednovati kroz rad u grupi i kroz intervju. Može se dati projektni zadatak ili laboratorijska vježba gdje će učenici pronaći neke društvene mreže koje nisu popularne i nisu dovoljno zaštićene i izvršiti analizu istih. Također, učenici mogu izvršiti i istraživanje na temu kodeksa ponašanja na društvenim mrežama, ili na temu cyberbullying-a, ili na temu elektronskog poslovanja.

Oblast: B/Rješavanje problema primjenom IKT-a

Ishod učenja	Razrada ishoda
B.III.1. Kreira klasične algoritme za zaštitu informacija i podataka.	• Definiše kriptografiju i osnovne pojmove vezane za kriptografiju. • Opisuje vrste i algoritme za klasično šifriranje. • Opisuje načine kriptovanja i dekriptovanja poruka.
Poveznice sa ZJNPP	**TIT 5.2.2.**

Ključni sadržaji

Matematičke osnove kriptografije.
Pojam kriptografije.
Pojam javnog i privatnog ključa.
Klasična kriptografija (monoalfabetska, polialfabetska i poligramska zamjena).
Klasično šifriranje (Cezarova šifra, afina šifra, Vigenereova šifra, playfair šifra).

Preporuke za ostvarenje ishoda

Poželjno bi bilo da se prije prelaska na samu kriptografiju obrati pažnja na matematičke osnove vezane za šifriranje. Obraditi sa učenicima pojam kriptografije i napraviti kratak osvrt na razvoj kriptografije kroz historiju. Prije analize kriptografskih algoritama učenici bi trebali da analiziraju i da shvate privatne i javne ključeve, odnosno trebali bi shvatiti da kvalitet zaštite uveliko zavisi od kvalitetno definisanog ključa. Kroz različite vježbe obraditi sa učenicima klasično šifriranje. Recimo, dati im otvorenu poruku pa na osnovu algoritma i zadanog ključa da predstave kako izgleda šifrirana poruka. Na primjer, damo im zadatak da pomoću Cezarove šifre kriptuju neki tekst uz unaprijed dogovoreni ili slučajno odabrani ključ. Dalje bi mogli učenici da razmijene urađene zadatke i da dekriptuju šifriranu poruku u razumljivu poruku. Učenici jedni drugima mogu ostavljati nagovještaj o ključu šifriranja. Na ovaj način će učenicima biti interesantno da učestvuju u realizaciji nastavnog sata, jer ih može zaokupiti i zaposliti na duže vrijeme, a samim tim se razvija i takmičarski duh među učenicima, gdje bi oni što prije dolazili do rješenja. Učenike bi bilo poželjno pratiti i vrednovati kroz rad u grupi i kroz intervju. Može se dati projektni zadatak ili laboratorijska vježba gdje će učenici jedni drugima slati kripto poruke i pokušavati da ih dekriptuju.

B.III.2. Koristi kriptografski softver za simetrične blokovske algoritme.	• Koristi softver za modernu kriptografiju. • Koristi simetrične blokovske algoritme i kriptografiju sa javnim ključevima. • Analizira HEŠ funkcije.
Poveznice sa ZJNPP	**TIT 5.2.2.**
Ključni sadržaji	
Kriptografski softver. Simetrični blokovski algoritmi (DES, trostruki DES, IDEA, AES, algoritam). HEŠ funkcije. Kriptografija sa javnim ključevima.	
Preporuke za ostvarenje ishoda	
Potrebno je instalirati softver koji omogućava naprednu kriptografiju. Kada učenici pređu na simetrične blokovske algoritme, uvesti korištenje softvera u kriptovanju i dekriptovanju poruka (na internetu je mnogo programa koji omogućavaju kriptovanje i dekriptovanje poruka). Obraditi i analizirati sa učenicima DES, trostruki DES, IDEA, AES algoritam. Dati učenicima zadatak da kriptuju i dekriptuju poruke pomoću softvera. Dozvolite učenicima da samostalno istraže HEŠ funkcije i uz pomoć predavača da analiziraju upotrebu HEŠ funkcija. Učenike bi bilo poželjno pratiti i vrednovati kroz rad u grupi i kroz intervju. Može se dati projektni zadatak ili praktična vježba gdje će učenici jedni drugima slati kripto poruke i pokušavati da ih dekriptuju.	

Oblast: C/Digitalno društvo	
Ishod učenja	**Razrada ishoda**
C.III.1. Analizira zlonamjerni softver i mjere zaštite od zlonamjernog softvera.	• Definiše zlonamjerni softver. • Opisuje vrste zlonamjernog softvera. • Analizira špijunske programe. • Koristi softver za zaštitu od zlonamjernog softvera. • Objašnjava hakerske aktivnosti i etičko hakerisanje.
Poveznice sa ZJNPP	**TIT 5.2.2.**
Ključni sadržaji	
Zlonamjerni softver. Trojanski konji. Logičke bombe. Crvi (e-mail, IM, internet, file sharing crvi). Virusi (EPO, makro, skript virusi). Špijunski programi. Rootkit. Zaštita od zlonamjernog softvera. Hakeri i etičko hakerisanje.	
Preporuke za ostvarenje ishoda	
Uvesti učenike u dio zlonamjernog softvera kroz definisanje i razvoj zlonamjernog softvera kroz historiju. Odgovoriti na pitanje šta je to navelo ljude na ideju da neki sistem učine nesigurnim odnosno da ga naruše svojim programima. Navesti učenike da o svim klasama zlonamjernog softvera razmišljaju kao o programima koji narušavaju druge programe ili datoteke. Učenici bi mogli kroz bat datoteke da kreiraju neki mali zlonamjerni softver, recimo da izbriše neke datoteke u nekom vlastitom direktorijumu. Omogućiti učenicima da na nekim računarima namjerno "inficiraju" sistem i da analiziraju šta se dešava sa datotekama i programima koji su zaraženi softverskom "infekcijom". Možemo namjerno zaraziti zlonamjernim softverom neki prenosivi medij i provjeriti kako se virus širi kroz mrežu. Pošto se očekuje da učenici posjeduju predznanje iz programiranja, omogućiti im da u svom programu naprave logičke bombe, odnosno da tempiraju rad nekih funkcija u programu. Omogućiti učenicima da instaliraju na nekom sistemu i špijunski softver i da provjere njegove mogućnosti, do kojih podataka mogu doći i kako ih mogu iskoristiti. Nakon analize zlonamjernih programa, potrebno je učenike voditi u drugom smjeru, odnosno da nauče kako koristiti antivirusne i antispajver programe. Omogućiti im instalaciju više besplatnih antivirusnih programa na različitim sistemima i provjeriti kako oni reaguju na "inficiran" medij. Ukoliko je moguće, analizirati i ponašanje licenciranog	

antivirusnog programa. Također, namjerno smanjiti bazu virusa u nekom antivirusnom programu i onda ga "inficirati" s ciljem shvatanja učenika da antivirusni program sam sebi nije dovoljan, nego da je potrebno i redovno obnavljanje baze virusa. Učenike je potrebno naučiti da hakeri nisu samo zli informatičari koji uništavaju sisteme, nego da postoje i etički hakeri odnosno ljudi koji svojim radom doprinose na zaštiti sistema. Učenike bi bilo poželjno pratiti i vrednovati kroz rad u grupi i kroz intervju. Ovdje bi bilo interesantno vrednovati učenike u smislu da iznalaze načine kako da se zaštite od zlonamjernog softvera ili eventualno ocijeniti njihovu analizu izloženosti nekog sistema.

C.III.2. Kreira rezervne kopije za različite dijelove računarskog sistema.	• Koristi tehnologiju za izradu rezervnih kopija. • Koristi arhiviranje, kompresiju podataka i vraća podatke sa rezervnih kopija. • Koristi cloud sisteme za arhiviranje i čuvanje rezervne kopije.
Poveznice sa ZJNPP	**TIT 5.1.3.**

Ključni sadržaji

Rezervne kopije.
Vraćanje podataka.
Arhiviranje podataka.
Kompresija podataka.
Zaštita i arhiviranje baza podataka.
Backup i restore operativnog sistema.
Cloud pohrana.

Preporuke za ostvarenje ishoda

Učenike kroz praktične vježbe stimulisati da kreiraju rezervne kopije negdje na lokalnoj mreži u neki direktorijum koji će biti njihovo vlasništvo. Također koristiti softver za vraćanje podataka, ukoliko smo nešto izbrisali trajno. Analizirati tu vrstu programa. Zatim kroz praktične zadatke raditi arhiviranje podataka u različitim programima. Koristiti različite vrste kompresija i omogućiti učenicima da analiziraju odabrani sistem kompresije. Bilo bi poželjno da učenici odrade zaštitu baza podataka kroz praktične vježbe, jer u ovom dijelu se već podrazumijeva da učenici znaju napraviti neku manju bazu podataka u MS Accessu. Također, pokazati učenicima kako se radi backup i restore operativnog sistema s ciljem vraćanja sistema kada je radio na zadovoljavajućem nivou. Dati učenicima zadatak da pohrane neke svoje podatke na nekom cloud servisu za pohranu podataka. Motivisati učenike da instaliraju više servisa i da ih uporede, da pronađu prednosti i nedostatke u korištenju istih.

E/ UČENJE I PODUČAVANJE

Učenje i podučavanje predmeta Sigurnost informacija organizira se prema zadanim odgojno-obrazovnim ciljevima i ishodima učenja. Nastavnici imaju mogućnost odabira različitih pristupa u skladu sa potrebama, interesima i nivoima znanja i vještina učenika kao i uslovima rada. Uvažavajući postavljena načela učenja i podučavanja, svaki nastavnik ovog predmeta može osmisliti izvedbu kurikuluma u najboljem interesu učenika.

Učenje i podučavanje usmjereno je na kreativnost učenika, samostalno istraživanje, prikupljanje podataka i povezivanje sadržaja. Učenici prikupljaju podatke, obrađuju materijale, samostalno koriste kriptografske algoritme i stvaraju uvjete u kojima će sistem biti zaštićen. Uslovi podučavanja predmeta usmjereni su na metodičku raznovrsnost svih raspoloživih metodičkih sistema i metoda koje će osigurati konkretno i potpuno znanje. Učenje i podučavanje predmeta sigurnost informacija ostvaruje se procesima:

- prikupljanja informacija,
- pronalaženja materijala i softvera za kriptografiju,
- zaštite vlastitog elektronskog identiteta,
- pronalaženja stranica sa zlonamjernim softverom,
- uklanjanja zlonamjernog softvera iz računara,
- arhiviranja podataka,
- kreiranja rezervnih kopija.

Učenici su aktivni kreatori znanja koji uz pomoć nastavnika pronalaze, razumiju i koriste se znanjem kako bi donosili bolje odluke u realizaciji problema. Učenici međusobno razmjenjuju iskustva i pomažu jedni drugima u realizaciji problema. Učenici mogu raditi individualno, u paru ili u grupama u zavisnosti od teme. Podjelu u manje grupe je moguće primijeniti u projektnom radu, problemskoj nastavi, te timskom radu.

Nastavnik će u ostvarivanju odgojno-obrazovnih ishoda uzeti u obzir interese učenika i njihove sposobnosti. Aktivno će pratiti napredak svakog učenika i metodu rada će prilagoditi potrebama učenika i njihovim sposobnostima. Prilikom osmišljavanja zadataka, nastavnik može davati problemske i praktične zadatke. Ukoliko se daje zadatak iz oblasti koju učenici nisu prešli u dosadašnjem obrazovanju, nastavnik je dužan da učenicima objasni metode kojim će doći do rješenja. Nastavnik će poticati učenike na istraživanje, davati im praktične vježbe u kojima će iskustvenim učenjem ostvarivati zadane odgojno-obrazovne ishode učenja. Također, nastavnik savjetuje učenike i prati ih tokom realizacije zadataka te im pomaže u otklanjanju grešaka.

Poželjno je koristiti i razne edukativne platforme, poput npr. eTwinning-a koji nudi priliku za razvoj i jačanje novih vještina i kompetencija za 21. stoljeće (https://www.etwinning.net/bs).

Načini realizacije učenja i podučavanja:

- projektno učenje i podučavanje;
- problemsko učenje i podučavanje;
- praktično učenje i podučavanje.

Posebno je važno da nastavnik pokaže pravilnu upotrebu kriptografskog softvera i softvera za zaštitu računara. Vježbe se primjereno biraju od jednostavnih ka složenim. Bitno je da nastavnik na kraju rada razgovara sa učenicima, razmijeni utiske sa učenicima i da omogući učenicima da zajednički analiziraju potencijalna rješenja. Pojasniti učenicima koji nisu najbolje razumjeli zadatak ili koji nisu izveli zadatak do kraja gdje su napravili grešku i kako izbjeći istu grešku u narednoj vježbi. Prilikom realizacije nastavnih sadržaja izbjegavati dominantno frontalni rad. Potrebno je stvoriti radno okruženje gdje će učenici raditi u parovima ili će grupno rješavati zadate probleme.

Za učenje i podučavanje predmeta Sigurnost informacija potrebni su materijalni resursi koji uključuju opremljen kabinet informatike. Kabinet treba imati priključak na internet. Na svakom računaru treba biti instalirana antivirusna zaštita i kriptografski softver (softver pronaći na internetu). Poželjno bi bilo da jedan učenik sjedi za jednim računarom, ali ako to nije izvodivo, omogućiti da maksimalno dva učenika sjede za jednim računarom. Izvori učenja su udžbenici, radni materijali i razni izvori sa interneta.

Nastava iz predmeta Sigurnost informacija se izvodi u III razredu gimnazije u informaciono-komunikacionom izbornom području, jedan nastavni sat sedmično, odnosno 35 sati godišnje. Vrijeme potrebno za ostvarivanje postavljenih odgojno-obrazovnih ishoda unutar pojedine oblasti određuje nastavnik, vodeći računa o tome da obradi ključne sadržaje definisane kurikulumom.

F/VREDNOVANJE U PREDMETNOM KURIKULUMU

Vrednovanje je proces kojim se kontinuirano prati ostvarivanje postavljenih ciljeva učenja i podučavanja i odgojno obrazovnih ishoda. Poseban akcenat treba staviti na vrednovanje praktičnih radova i analize urađenih zadataka.
Postoje tri vrste vrednovanja:
Vrednovanje za učenje (formativno vrednovanje) bi trebalo biti povratna informacija o kvaliteti urađenog kojoj je svrha unaprijediti procesa učenja i podučavanja. Ova vrsta vrednovanja podstiče saradnju između nastavnika, učenika i roditelja.
Vrednovanje kao učenje podrazumijeva aktivno uključivanje učenika u proces vrednovanja uz stalnu podršku nastavnika, kako bi se podstakao razvoj samoregulisanog učenja, učeničke samoprocjene, samovrednovanja i samoocjenjivanja. Da bismo to postigli kriteriji za vrednovanje i ocjenjivanje moraju biti precizni, jasni i transparentni.
Vrednovanje naučenog (sumativno vrednovanje) podrazumijeva procjenu nivoa postignuća učenika nakon određenog perioda (nakon određene teme, polugodišta i sl.). Po pravilu se iskazuje zaključnom ocjenom.
Vrednovanje pomaže da se što bolje ostvare ishodi znanja, ali i direktno podstiče učenike za daljnje napredovanje. Učenici se manje trude i pasivniji su u radu ukoliko vrednovanje rješenja njihovih zadataka nije učestalo. Vrednovanje učeničkih postignuća je kontinuirana djelatnost. Informacija o onome što učenici nisu dobro uradili za učenike može biti korisna u smislu napredovanja za ubuduće.
Sigurnost informacija podrazumijeva teorijska i dominantno praktična znanja, stoga je neophodno da nastavnik daje što više praktičnih vježbi koje bi radili u učionici i projekata koje bi učenici radili kod kuće. Koristiti što više praktičnih primjera. Posebno je potrebno obratiti pažnju na vrednovanje učenika kroz rad u paru ili grupi. Također, nastavnik bi trebao da potiče učenike na samokritičnost i omogućiti učenicima da samostalno evaluiraju svoja znanja.
U svakoj oblasti predmeta Sigurnost informacija potrebno je u vrednovanju dati veću važnost ocjenjivanju praktičnih radova kroz:

- vrednovanje u pronalaženju materijala,
- vrednovanje sigurnosti vlastitih korisničkih računa i analize istih,
- vrednovanje poznavanja kriptografskih algoritama,
- vrednovanje korištenja kriptografskog softvera,
- vrednovanje cjelokupnih rezultata,
- vrednovanje rada u paru ili grupi,
- vrednovanje individualnih analiza zadataka i uklanjanja grešaka.

Veoma bitna stavka u vrednovanju je uključenost samog učenika u proces vrednovanja. Sistem ocjenjivanja treba biti transparentan i trebamo dati mogućnost učeniku samoprocjene po definisanom sistemu. Preporučuje se da prije evaluacije praktičnih radova učenici imaju na raspolaganju sve elemente vrednovanja da bi se bolje pripremali za nastavu i praktične zadatke. Uključivati učenike kao one koji će vršiti vrednovanje i procjenu praktičnih radova drugih učenika ili drugih grupa i timova.

Vršnjačko vrednovanje je posebno dobro kod grupnog i timskog rada na praktičnim vježbama, jer možemo ujedno vrednovati i učenike koji vrednuju tuđi rad. Učenici u tom slučaju trebaju poštovati definisana pravila i kriterije vrednovanja i ocjenjivanja.
Tehnike i indikatori kvaliteta vrednovanja:

- usmene provjere znanja,
- praktične vježbe,
- grupni projekti,
- aktivnost učenika,
- pismene provjere.

U zavisnosti od ciljeva oblasti biramo i načine vrednovanja i tipove zadataka. Prilikom zaključivanja ocjena treba obratiti pažnju na omjer reprodukcije teorijskog znanja, praktičnog rada i konačnog rezultata. Odnos bi trebao biti:

- 20% reprodukcija teorijskog znanja,
- 60% praktični radovi,
- 20% konačni rezultat.

Opći utisak nastavnika prilikom izvođenja ocjena ne smije biti subjektivan i treba se obrazložiti pred odjeljenjem u skladu sa detaljnim objašnjenjima onoga što je učenik u toku školske godine uspio da postigne kroz sve oblasti. Ovdje je neophodno da nastavnik vodi evidenciju o postignućima svakog učenika u toku školske godine kako bi mogao transparentno, precizno i objektivno iskoristiti svoja zapažanja u donošenju zaključne ocjene.

G/PROFIL I STRUČNA SPREMA NASTAVNIKA

- Nastavu sigurnosti informacija mogu izvoditi lica koja su završila odgovarajući četverogodišnji studij i stekla zvanje:
  - profesor informatike,
  - profesor matematike i informatike,
  - profesor matematike, smjer matematika s informatikom,
  - diplomirani inženjer informatike, s položenom pedagoško-psihološko-didaktičko-metodičkom grupom predmeta,
  - diplomirani inženjer elektrotehnike, smjer informatika ili računarstvo, s položenom pedagoško-psihološko-didaktičko-metodičkom grupom predmeta,
  - softver inženjer, s položenom pedagoško-psihološko-didaktičko-metodičkom grupom predmeta,
  - diplomirani inženjer informacijskih tehnologija, s položenom pedagoško-psihološko-didaktičko-metodičkom grupom predmeta,
  - diplomirani ekonomista, smjer informatika, s položenom pedagoško-psihološko-didaktičko-metodičkom grupom predmeta,
  - profesor ostalih predmeta uz završen dvogodišnji kurs Informatike na fakultetu koji obrazuje informatički kadar (kurs mora verifikovati Nastavno naučno vijeće fakulteta).
- Nastavu sigurnosti informacija mogu izvoditi i lica koja imaju završen najmanje II (drugi) ciklus Bolonjskog sistema studiranja u trajanju od jedne godine (60 ECTS bodova) ili dvije godine (120 ECTS bodova) – ukupno 300 ECTS bodova sa bodovima prvog ciklusa, koja su stekla akademsku titulu i zvanje magistra ili ekvivalenta za određenu oblast.
- Lica koja u toku studija nisu polagala ispite iz pedagoško-psihološko-didaktičko-metodičke grupe predmeta, dužna su ove ispite položiti u roku od godinu dana od dana stupanja na posao nastavnika.