Priručnik

„Rješavanje problema prilikom korištenja i korištenjem digitalne tehnologije”

Zagreb, 2018. godina

e-Škole
USPOSTAVA SUSTAVA RAZVOJA DIGITALNO ZRELIH ŠKOLA
(PILOT PROJEKT)

CARNET
znanje povezuje

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Sadržaj

SAŽETAK **3**

UVOD **4**

1. poglavlje: Usporavanje računala i nestabilnost u radu **5**
1.1 Hardverska nestabilnost računala uzrokovana neispravnim sastavnicama ili degradacijom funkcionalnosti određene sastavnice 6
1.2 Hardverska nestabilnost računala izazvana upravljačkim programima 14
1.3 Softverski uzrokovana nestabilnost u radu 17

2. poglavlje: Rješavanje tehničkih problema **19**
2.1 Prijetnje na internetu 20
2.2 Pravodobna zaštita računala 23
2.3 Upotreba kontrole korisničkih računa 26
2.4 Rješavanje problema s nepouzdanim radom računala uz pomoć sistemskih alata 28

3. poglavlje: Stvaranje baze znanja i unapređenje procesa **32**

4. poglavlje: Spajanje na mrežu **35**

ZAKLJUČAK **39**

POPIS LITERATURE **40**

IMPRESSUM **41**

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Značenje oznaka u tekstu:

Sažetak

Priručnik je izrađen za realizaciju istoimenog webinara koji se održava tijekom šk. god. 2017./2018. u sklopu projekta „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot-projekt)“.

Primjena digitalnih tehnologija u školama sve je češće nezaobilazna pa je svrha ovog priručnika pomoći polaznicima webinara u rješavanju svakodnevnih računalnih problema koji mogu ometati primjenu IKT-a.

Uporaba digitalnih tehnologija trebala bi olakšati svakodnevne zadaće, međutim često njezina kompleksnost može uzrokovati suprotne situacije. Uzroke problema možemo, radi jednostavnosti, podijeliti na one uzrokovane hardverom te one uzrokovane softverom. U ovom se priručniku daje pregled najčešćih problema i njihovih uzroka u obje kategorije. Računalo je uređaj koji za svoj rad koristi električnu energiju. Upravo zbog toga uvijek moramo na umu imati sigurnost korisnika računala. Kada rješavamo probleme koji su povezani s naponskom jedinicom ili kada moramo pristupiti unutrašnjosti računala, najbolje je kontaktirati stručnu osobu. Manje hardverske ili softverske probleme povezane s upravljačkim programima ili periferijom možemo probati riješiti sami.

Pri korištenju digitalnih tehnologija nikako se ne smiju zaboraviti ni sigurnosni problemi vezani za digitalni sadržaj. Sigurnosne probleme rješavamo odgovarajućom zaštitom poput vatrozida, s pomoću sigurnosnih protokola za komunikaciju te uporabom antivirusnih programa, a od gubitka podataka štitimo se sigurnosnom pohranom. Spominjemo da je korisno pratiti preporuke CARNET-ovog CERT-a (engl. *Computer Emergency Response Team*). Korisno je pratiti preporuke koje se mogu naći na poveznici http://cert.hr/. Preporučamo i brošuru Sigurnije na Internetu dostupnu na http://cert.hr/dokumenti/sigurnije_na_internetu te pregled dostupnih predložaka za školski Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko komunikacijske tehnologije, koji je dostupan na https://www.e-skole.hr/hr/rezultati/digitalna-zrelost-skola/dokumenti-za-skole/.

Kada skupimo operativno i korisno znanje vezano uz do sada navedene teme, pogodno je kreirati bazu znanja pomoću koje možete podijeliti stečeno znanje sa svojim kolegama ili učenicima. Jedan od alata koji možemo koristiti je Wikipedija unutar OneDrive aplikacije.

Spajanje računala na mrežu nosi svoje rizike kojih moramo biti svjesni. Kako smo napomenuli, to se posebno odnosi na digitalnu razmjenu podataka. Zbog toga je bitno poznavati osnove sigurnosti na internetu i znati prepoznati koju vrstu zaštite koriste bežične mreže te kako se spajati na njih.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Uvod

U svakodnevnom radu s računalom mogući su različiti problemi. Uglavnom je riječ o lako rješivim situacijama poput neispravnog monitora ili pogrešno postavljene rezolucije prikaza. No neki problemi mogu biti mnogo složeniji i opasniji poput krađe osobnih podataka, korisničkog imena ili zaporke. Većina se može spriječiti, manji se mogu riješiti, a za rješavanje složenijih problema najbolje je potražiti pomoć ovlaštene i stručne osobe.

Sve većom dostupnošću prijenosnika, tableta te pametnih telefona raste i količina razmijenjenih podataka, informacija i sadržaja. Upravo zbog ove dostupnosti korištenje digitalnim tehnologijama može dovesti u pitanje sigurnost povjerljivih podataka. Većina operativnih sustava dolazi s ugrađenim funkcionalnostima koje pomažu u sprečavanju takvih problema.

Ovim priručnikom želi se razjasniti i razlika između problema povezanih s hardverskom nestabilnosti računala (neispravne sastavnice računala) ili pak problema uzrokovanih upravljačkim programima odnosno aplikacijama.

U prvom poglavlju „Usporavanje računala i nestabilnost u radu“ ukratko je opisana arhitektura računala s osvrtom na osnovne sastavnice kao i potencijalne probleme povezane s njima. Drugo poglavlje „Rješavanje tehničkih problema“ upoznaje s nekim od prijetnji na internetu te načinima zaštite računala. Opisani su glavni ugrađeni alati poput Windowsova vatrozida, Windowsova Defendera i kontrole korisničkog računa. Navedeno čini osnovne alate za zaštitu digitalnog sadržaja. Obrađuju se i nestabilnosti povezane sa softverskim instalacijama i zarazom zlonamjernim programima. Treće poglavlje „Stvaranje baze znanja i unapređenje procesa“ govori o stvaranju baze znanja s pomoću funkcionalnosti Wikipedije SharePointa Online koji nalazimo u sklopu sustava Office 365 za škole. Četvrto poglavlje „Spajanje na mrežu“ daje osnove računalnih mreža te opisuje vrste mrežnih veza.

Europska unija
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
ESF UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

1. poglavlje: **Usporavanje računala i nestabilnost u radu**

U ovom poglavlju naučit ćete:

- ☑ o sastavnicama računala
- ☑ koje su nestabilnosti povezane sa sastavnicama računala
- ☑ što je BIOS.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

1.1 Hardverska nestabilnost računala uzrokovana neispravnim sastavnicama ili degradacijom funkcionalnosti određene sastavnice

U ovom poglavlju opisane su poveznice između čovjeka, operativnih sustava i hardverskih sastavnica računala. Dan je kratki prikaz o tome kako se problemi sa sastavnicama mogu odraziti na nastavni proces. Važno je napomenuti da dobar dio problema koje spominjemo u ovom poglavlju zahtijeva pomoć stručnih osoba. No bitno je upoznati se sa što većim spektrom potencijalnih problema te razlikovati one koje možemo sami riješiti od onih gdje je bolje i sigurnije potražiti stručnu pomoć.

Arhitektura računala

S obzirom na to da je sama građa računala poprilično složena, opisuju se samo osnovna načela funkcioniranja najvažnijih sastavnica, kao i poveznice između njih i stabilnosti računala. Govoreći o građi računala, osim memorije i procesora koji se najčešće spominju, potrebno je još izdvojiti ulazno-izlazne uređaje.

Najprije valja povezati sastavnice računala i čovjeka kao korisnika računala.

Da bi se čovjek mogao koristiti računalom, mora mu zadati određenu naredbu, ali tako da je računalo može izvršiti. Takav oblik zadavanja naredbi nazivamo **instrukcijama**, koje računalo izvodi jednu za drugom.

Naravno da čovjek ne komunicira s računalom tako da izravno zadaje takve instrukcije jer bi ih za najmanji posao svaki put trebao napisati mnogo, što oduzima vrijeme i posljedično se gubi smisao računala kao tehnologije koja olakšava svakodnevne zadatke. Uobičajeni se zadaci stoga prethodno pripreme u obliku slijeda instrukcija koje nazivamo aplikacijama.

Sve aplikacije pripremaju se tako da se napišu u nekom od programskih jezika. Aplikacije se pohranjuju u računalu preko tzv. instalacijskih procedura.

Danas nam je na raspolaganju izniman broj aplikacija. S nekima se susrećemo na dnevnoj razini, a s nekima rjeđe. Primjeri su „svakodnevnih“ programa npr. aplikacije iz paketa Microsoft Office: razni web-preglednici, programi za reprodukciju i stvaranje multimedije itd.

Čovjek s računalom komunicira preko vanjskih elemenata računala koje nazivamo **ulazno-izlaznim uređajima**. Primjer **ulaznih** uređaja jesu tipkovnica i miš, a u novije vrijeme to može biti i monitor osjetljiv na dodir. Primjerice, dvoklikom na ikonu Worda koja se nalazi na radnoj površini (engl. *Desktop*) taj će se program pokrenuti, tipkanjem po tipkovnici u odabranom će se prozoru pojaviti tekst i sl.

Povratnu informaciju čovjek dobiva preko **izlaznih** jedinica kao što su monitor, zvučnici i pisač.

Programi se koriste i odgovarajućim podacima, a ne samo instrukcijama. Podaci mogu biti pohranjeni dijelom uz program (kao jedna cjelina) ili u dodatnim zasebnim cjelinama (datotekama). Uobičajeno se i program i podaci s kojima programi rade trajno zapisuju u prikladne spremnike podataka.

Najčešće korišten spremnik podataka, koji zadržava podatke i nakon isključivanja računala, jest čvrsti disk (engl. *hard disk*). Osnovna jedinica podataka na disku (s motrišta korisnika i njegovih programa) jest datoteka (engl. *file*).

Osim programa koji obavljaju zadane operacije, u računalnom sustavu moraju postojati mehanizmi za pokretanje takvih programa, što uključuje barem:

- rezervaciju spremničkog prostora za program
- učitavanje programa s diska u spremnik
- pokretanje programa
- omogućavanje interakcije korisnika s programom
- zaštitu pokrenutog programa od već prisutnih programa u sustavu i obrnuto.

Takvi mehanizmi ostvaruju se pomoćnim programima koji omogućuju izvođenje operacija na računalu, a spojeni čine **operativni sustav** (Car, 2015).

Operativni sustav

Kako bi se ostvarile osnovne funkcije računala, odnosno, unos podataka, njihovo pohranjivanje u memoriju te potom obrada i izlaz (npr. na monitoru, pisaču ili projektoru) potreban je skup osnovnih programa koji upravljaju sklopovljem računala.

Zadaća operativnog sustava jest upravljanje cjelokupnim sustavom, i to od upravljanja datotekama na disku, zatim upravljanja programima i njihova pokretanja do komunikacije s korisnikom te drugim programima i ostalim komponentama. Osim toga, zadaća je operativnog sustava olakšati uporabu računala korisniku preko standardiziranih sučelja.

Operativni je sustav posrednik između krajnjih korisnika i hardverskih sastavnica koje se nalaze u računalu. S jedne strane olakšava korištenje računalom, a s druge omogućava primjerice obradu podataka (Car, 2015).

Hardverske sastavnice

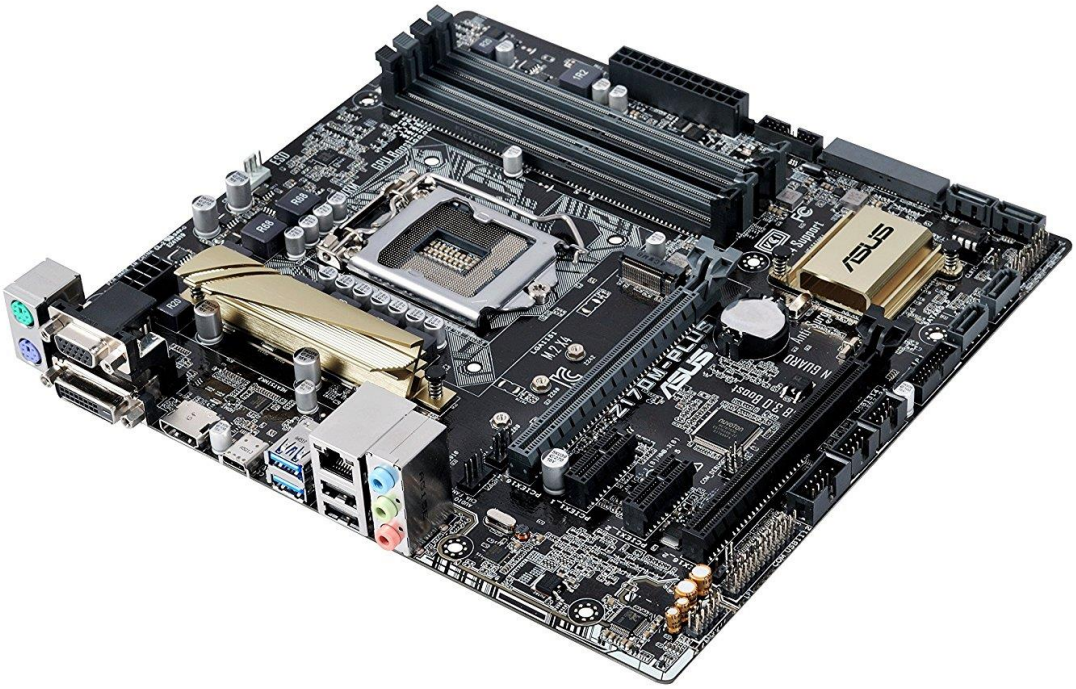
Nakon utvrđivanja poveznica između računalnih sastavnica, operativnog sustava i čovjeka, možemo se posvetiti osnovnim sastavnicama čije je ispravno funkcioniranje iznimno bitno za stabilnost i pouzdanost računala.

Matična ploča

Prva sastavnica koju ćemo obraditi je matična ploča, za koju možemo reći da čini okosnicu bilo kojeg računala. Ona je „središnje mjesto“ na koje su povezane sve ostale komponente, a na njoj su se smjestile središnja procesorska jedinica i radna memorija. Sve su komponente osobnog računala ili smještene izravno na matičnoj ploči, ili spojene na nju.

Osnovu matične ploče čine dva međusobno povezana čipa koja se zajedničkim imenom nazivaju **chipset**, a povezuju procesor, memoriju, grafički karticu te kontroliraju promet koji se ostvaruje između ostalih ulaznih i izlaznih uređaja. Na matičnoj ploči nalaze se:

- utor za procesor
- priključnice za memoriju
- priključnice u koje se stavljaju uređaji izrađeni u obliku kartica (PCI, PCI-Express) te priključnice za čvrsti disk i optičke uređaje
- ulazno-izlazni panel koji uključuje USB ulaze (engl. *Port*), zatim ulaze za miša i tipkovnicu, serijski i mrežni (engl. *ethernet*) ulaz itd.
- čip s BIOS-om.



Slika 1. Matična ploča (https://images-na.ssl-images-amazon.com/images/I/91NyrUTXnhL._SL1500_.jpg, 2.5.2018.)

Problemi s matičnom pločom vrlo su rijetki i zahtijevaju servis ili zamjenu od strane ovlaštene osobe, a očitovat će se najčešće u nemogućnosti pokretanja računala.

Naponsku jedinicu nismo posebno razradili, iako je ona temelj koji opskrbljuje sve komponente računala električnom energijom. Razlog tome je što sve probleme koji dolaze od njezine neispravnosti moramo ostaviti **samo** stručnim osobama. Kako smo naveli, glavni problem vezan za matičnu ploču iskazuje se kao nemogućnost pokretanja računala i stručne će osobe najprije provjeriti ispravnost naponske jedinice.

Središnja jedinica za obradu (CPU)

Obrada podataka, upravljanje protokom podataka između pojedinih dijelova sustava te usklađivanje i nadzor cijelog sustava zadatak je središnje (centralne) procesorske jedinice (CPU) odnosno procesora.

Sastoji se od:

- aritmetičko-logičke jedinice
- upravljačke jedinice.

Procesori odjednom mogu obraditi više bitova (bit, – engl. **bi**nray digi**t** – osnovna je informatička jedinica u računalstvu i digitalnoj komunikaciji). Što više bitova procesor odjednom može obraditi, to će više podataka moći obraditi u jedinici vremena. Većina suvremenih procesora obrađuje odjednom 32 ili 64 bita. Sva su današnja novija računala (prijenosna, stolna) uglavnom 64-bitna, a različite tablete još uvijek nalazimo s 32-bitnim procesorima. Za prosječnog korisnika ta razlika nije toliko važna i on je neće osjetiti u svakodnevnom radu.

Kad govorimo o stabilnosti računala, bitno je reći da zbog građe središnje procesorske jedinice, gdje je riječ o više stotina milijuna tranzistora unutar pojedine središnje procesorske jedinice, dolazi do zagrijavanja.

Problemi nastaju u trenutku kada se procesor počne pregrijavati. Većina modernih računala ima zaštitu od pregrijavanja procesora, zahvaljujući kojoj se računalo jednostavno isključi kada temperatura procesora dostigne određenu vrijednost. Problemi nastaju kada su procesori na tzv. graničnim temperaturama. Pod graničnom temperaturom razumijevamo radnu temperaturu koja nije dovoljno visoka da se računalo isključi, ali je dovoljno velika da dođe do narušavanja performansi odnosno nestabilnosti sustava.

Kako bi procesori radili na optimalnoj temperaturi, opremljeni su hladnjakom. Hladnjaci mogu biti pasivni (hladi ih npr. dodatni ventilator koji se nalazi u kućištu ili ventilator napajanja) ili aktivni, odnosno posjeduju vlastiti ventilator koji se nalazi na njima.

No tijekom rada računala, neovisno o tome je li riječ o prijenosnom ili stolnom računalu, može doći do onečišćenja hladnjaka prašinom što će umanjiti njegovu učinkovitost. Posebno je to moguće u ljetnim mjesecima kada temperatura okoline prelazi uobičajene vrijednosti ili ako prijenosno računalo držimo na površini koja ne osigurava dovoljno hlađenje (npr. platnena podloga na stolu ili sl.).

Slika 2. Primjer procesora s onečišćenim ventilatorom (https://4bds6hergc-flywheel.netdna-ssl.com/wp-content/uploads/2015/06/dirty_laptop.jpg, 2.5.2018.)

Ako tijekom nastave računalo nepouzdano radi, primjerice iznenada se isključuje ili ponovno pokreće, vrlo je vjerojatan uzrok upravo nedovoljna efikasnost hlađenja na procesoru.

Često su onečišćena računala koja se nalaze na podu pokraj ili ispod stola. Napomenimo da i ovaj problem mora rješavati stručna osoba i da nikako ne pokušavate čistiti računalo od prašine **kada je pod naponom**.

Memorija

Memorija se često označuje kao „usko grlo“ svakog računala. Na njoj rijetko dolazi do kvarova, no nedovoljna količina ugrađene memorije može negativno utjecati na učinkovit rad računala.

Kada je riječ o radu računala odnosno operativnog sustava, valja napomenuti da se svi otvoreni programi odnosno sve ono što radimo uglavnom pohranjuje u memoriju sa slučajnim pristupom, tzv. RAM. Količina radne memorije u našim računalima uvijek je ograničena te toga moramo biti svjesni ako istodobno želimo pokrenuti određeni broj aplikacija.

Pri otvaranju aplikacija računalo podatke pohranjuje u radnu memoriju sve do iscrpljivanja slobodnog prostora. U tom trenutku, kada ponestane slobodnog prostora u radnoj memoriji, računalo privremene podatke počinje pohranjivati na čvrsti disk. U pravilu čvrsti disk ima manje brzine pristupa podacima od radne memorije te se nedostatak radne memorije očituje kroz intenzivan rad čvrstog diska i usporavanje.

Pri opisu matične ploče spomenuti su i utori za radnu memoriju. Prije nadogradnje računala potrebno je provjeriti koliko utora posjeduje matična ploča u stolnom ili prijenosnom računalu te kolika je maksimalna količina podržane radne memorije. Ugradnju i provjeru ispravnosti fizičkih modula radne memorije radi ovlaštena osoba.

Kapacitet memorije mjeri se brojem bajtova koje ona može pohraniti. Tipične vrijednosti radne memorije kreću se od 2 GB (2048 MB) kod tableta do 4, 8 ili 16 GB za prijenosna računala. Stolna računala i radne stanice mogu imati ugrađenu znatno veću količinu radne memorije.

Slika 3. Prikaz radne memorije za prijenosna računala (http://cdn6.bigcommerce.com/s-qlm4wa8b/products/337/images/879/2X4G3_S_DDR3_Laptop_RAM__62900.1447506768.1280.1280.jpg?c=2, 2.5.2 018.)

Nije lako procijeniti količinu radne memorije potrebnu bilo kome. Naime, ako rabimo računalo za rad u Wordu ili npr. Excelu, rijetko ćemo se susretati s navedenim problemima ako imamo ugrađeno. 8 GB RAM, međutim, ako se bavimo obradom videomaterijala, navedena količina radne memorije može izazvati opisane probleme.

Kada radna memorija postaje nedovoljna, operativni sustav počinje upotrebljavati virtualnu memoriju kojom se koristi kao sekundarnim skladištem podataka. Ta virtualna memorija nalazi se na čvrstom disku i naziva se (u slučaju Microsoft Windows operativnog sustava) „Windows Page File“. S obzirom na to da je čitanje podataka s čvrstog diska daleko sporije nego iz radne memorije, možemo zabilježiti znatniji pad performansi. Isto ćemo primijetiti i po užurbanom svjetlucanju lampice diska na našem računalu. Takvu situaciju često možemo iskusiti pri velikom broju web-stranica otvorenih u pregledniku (Car, 2015).

Čvrsti disk

Za razliku od radne memorije kojom se koristimo za privremenu pohranu podataka, čvrsti je disk memorija koja se rabi za trajnu pohranu podataka. Prezentacije, dokumenti i multimedija uglavnom su pohranjeni na čvrsti disk. Čvrsti disk poprilično je podložan kvarovima koji redovito rezultiraju gubitkom podataka zbog čega se preporučuje napraviti sigurnosnu pohranu digitalnog sadržaja (izrada sigurnosne kopije opisana je u nastavku priručnika).

Ako se operativni sustav na našem računalu ili tabletu ne može učitati i dobijemo poruku „**Operating system not found“,** moguća su dva razloga:

a. disk nije ispravan ili je zbog bilo kojeg razloga ostao bez napajanja
b. promijenjen je redoslijed pronalaska operativnog sustava (engl. *Boot order*) u BIOS-u.

Slika 4. Poruka o nemogućnosti učitavanja operativnog sustava

Najsigurnija opcija koja će spasiti podatke u slučaju bilo kakvog kvara jest sigurnosna pohrana. Jedan od pouzdanih načina sigurnosne pohrane je aplikacija OneDrive, o kojoj će više biti govora u narednim poglavljima, te upotreba mogućnosti povijesti datoteka (engl. *File History*).

Problemi s čvrstim diskovima uglavnom se očituju na dva načina. Prvi je fizički kvar čvrstog diska koji uglavnom dovodi do trajnoga gubitka podataka (vidljivo kroz npr.

nemogućnost pokretanja operativnog sustava ili čitanja datoteka), a drugi je fragmentacija podataka, koja se detaljno opisuje u nastavku.

Kada se tijekom vremena na disk upisuju novi podatci te brišu i modificiraju postojeći, datotekama se mijenjaju veličina i lokacija na disku. Ako se mijenja, odnosno povećava veličina datoteke (npr. otvorili smo dokument u Wordu i u njega nešto nadopisali ili ga uredili), a ne postoji slobodan prostor odmah pokraj iste lokacije na disku, datotečni će sustav njezin „novi dio“ pohraniti ondje gdje nađe slobodnog mjesta. Na taj će način dokument u Wordu biti pohranjen na dva ili više različitih fizičkih lokacija na disku. Da bi se taj isti dokument u Wordu ponovno otvorio, disk će morati napraviti nekoliko koraka više kako bi se podaci „prikupili“ u slučaju da su lokacije udaljene.

Navedeno nazivamo fragmentacijom podataka i ta vrsta usporenja računala često može biti zamijenjena s pomanjkanjem radne memorije, pogotovo jer se u oba slučaja očituje u intenzivnom čitanju i zapisivanju po čvrstom disku. Ako na računalu imamo više od 4 GB, pažnju bi trebalo usmjeriti na čvrsti disk. Problem možemo riješiti defragmentacijom. Na računalima s operativnim sustavima Microsoft Windows 10 defragmentacija je prema zadanim vrijednostima prilagođena da se pokreće jednom tjedno (Car, 2015). Mehaničke diskove polako zamjenjuju tzv. SSD (engl. *Solid state drive*) diskovi i kod njih također dolazi do pojave fragmentacije podataka, no zbog načina konstrukcije (nema pokretnih mehaničkih komponenti) ne opažamo navedenu vrstu problema.

Za one koji žele znati više

Više o defragmentaciji možete naći na https://support.microsoft.com/hr-hr/help/4026701/windows-defragment-your-windows-10-pc

Ulazno-izlazne jedinice

Ulazno-izlazne naprave rijetko se kvare. Većinu današnjih ulazno-izlaznih jedinica spajamo preko USB priključka. Stolna i prijenosna računala na sebi imaju standardne USB priključke, a na različitim vrstama tableta nalazimo tzv. mini/mikro USB te USB-C priključke. Za spajanje miša ili tipkovnice na tablet, zbog toga što je na tipkovnici standardni USB priključak, a na tabletu mini/mikro USB priključak, potreban je tzv. OTG kabel. Češće se tipkovnica i miš, ako za time ima potrebe, s tabletom spajaju bežičnim putem.

Slika 5. Standardni USB priključak i standardni USB kabel (https://xpert-ict.weebly.com/port--serial-usb-and-parallel.html, 2.5.2018.)

Slika 6. Mikro USB priključak (https://images-na.ssl-images-amazon.com/images/I/51djySNYPcL._SX522_.jpg, 2.5.2018.)

Slika 7. OTG kabel (https://www.amazon.in/OTG-BZ-OTG-BL-Micro-USB-Cable/dp/B00G5AI1RS, 2.5.2018.)

Ako bežična tipkovnica i miš imaju problema sa spajanjem na bilo koju vrstu računala, valja provjeriti imaju li ispravnu bateriju te ju po potrebi zamijeniti.

Spajanje računala na projektore

Često je u učionici, na predavanjima ili različitim usavršavanjima računalo potrebno povezati na različite vrste projektora. Tada računalo treba povezati s pomoću odgovarajućeg kabla, a najčešće je to VGA ili HDMI kabel. Dodatne opcije povezivanja moguće su pomoću DVI priključka ili putem lokalne mreže.

Slika 8. VGA i HDMI priključci (https://sites.google.com/a/bps-ok.org/website/home/staff/technology/chromebooks/staff-chromebook-faqs/howcanidisplayachromebookscreenonaprojectorormonitor, 2.5.2018.)

Nakon povezivanja računala s projektorom treba pritisnuti tipku Windows ( ) + P i odabrati jednu od sljedeće četiri mogućnosti:

- samo ekran računala – slika se prikazuje samo na ekranu računala
- dupliciraj – identična će slika odnosno prikaz biti i na računalu, i na projektoru
- proširi – prikaz s računala proširit će se i na prikaz na projektoru kao da imamo dva monitora, pri čemu npr. prezentaciju možemo premještati s jednog ekrana na drugi odnosno odabrati što želimo vidjeti samo mi, a što želimo podijeliti sa sudionicima sastanka, konferencije ili predavanja
- samo drugi ekran – slika će se prikazati samo na projektoru.

Problemi koji se mogu javiti prilikom povezivanja računala s projektorom, a očituju se u nemogućnosti prikaza slike, mogu se riješiti u većini slučajeva na dva načina. Prvi je klasično ponovno pokretanje računala, a drugi provjera je li dobro izabran izvor signala na projektoru. Ako niti nakon tih koraka ne uspijevamo prikazati željeni sadržaj pomoću projektora, najbolje je pozvati lokalnog administratora.

1.2 Hardverska nestabilnost računala izazvana upravljačkim programima

Do sada su opisani najčešći problemi koji se odnose na probleme s računalnim komponentama. Daleko su češći problemi koji se odnose na probleme sa softverom, bez obzira na to je li riječ o cjelokupnom operativnom sustavu, upravljačkim programima ili određenoj aplikaciji.

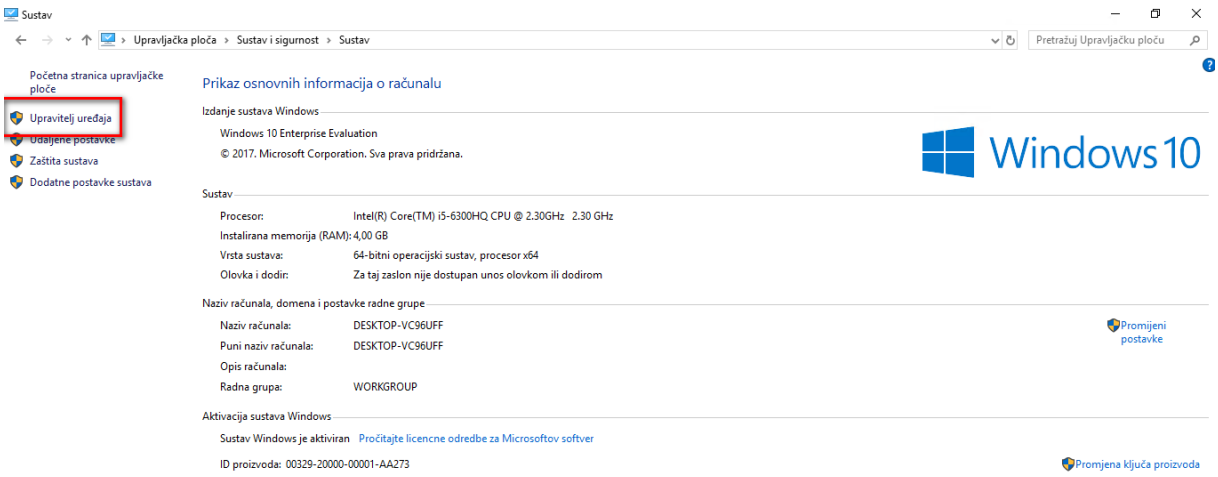
Mnogo je vjerojatnije da pri puštanju multimedijalne prezentacije zvuk izostane zbog problema s upravljačkim programima, a ne zbog problema s fizičkim kvarom sastavnice.

Za upravljačke programe možemo reći da definiraju sučelje za komunikaciju, vremenski slijed naredbi i sl. Ukratko možemo reći da oni definiraju „komunikacijski kanal“ sastavnice, npr. grafičke kartice s operativnim sustavom.

Specifični su za svaki uređaj odnosno sastavnicu kao i za operativni sustav, a stvaraju ih proizvođači uređaja.

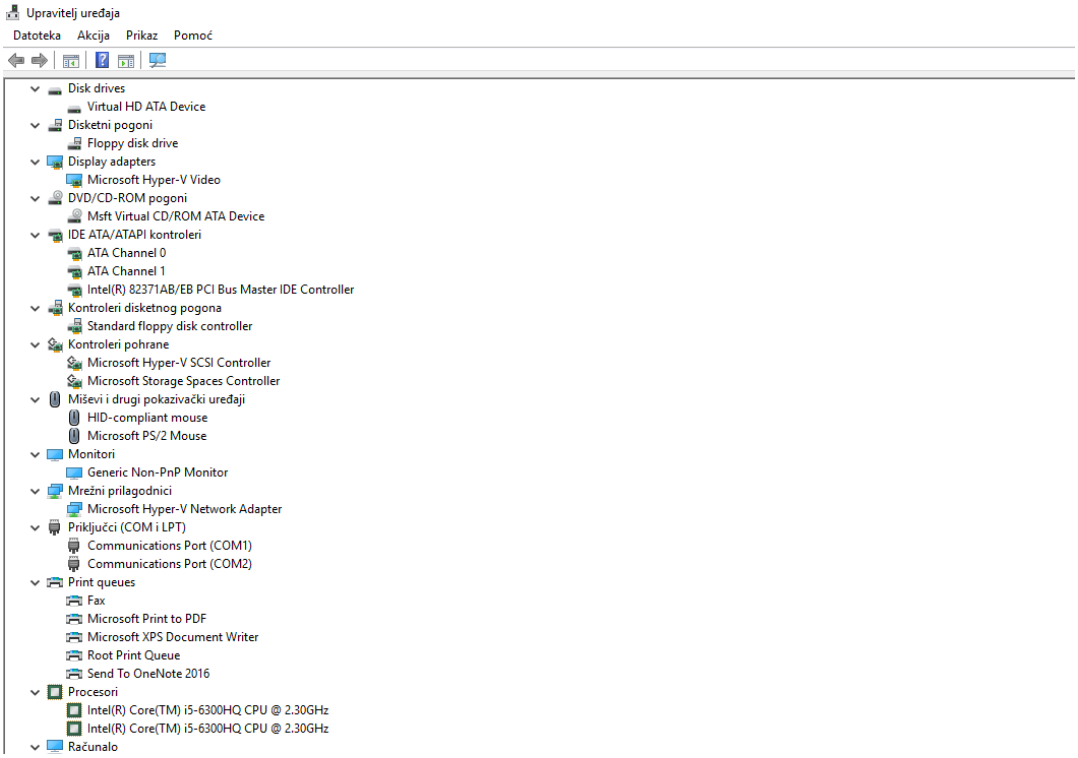
S pomoću Upravitelja uređaja (engl. *Device manager*) možemo provjeriti je li uređaj odnosno upravljački program pravilno instaliran, no isprekidani zvuk, nemogućnost promjene rezolucije ekrana ili npr. nemogućnost ispisa određenog dokumenta već pokazuju da nešto nije u redu. U takvim slučajevima svakako valja provjeriti i upravljačke programe.

Za pristup Upravitelju uređaja potrebno je otvoriti: **Upravljačka ploča → Sustav i sigurnost → Sustav** (slika 9.).



Slika 9. Prikaz Sistemske ploče

U lijevom dijelu prozora odaberite **Upravitelj uređaja**. U njemu se može otvoriti prozor u kojem je moguće ukloniti upravljačke programe, nadograditi ih, onemogućiti njihov rad.



Slika 10. Prikaz upravitelja uređaja

Ako *upravljački programi* nisu instalirani nakon instalacije ili nadogradnje računala, ili pak postoji problem s komponentom, Upravitelj uređaja će to prikazati, označujući ih žutim uskličnikom ili upitnikom. U tom će slučaju trebati instalirati upravljačke programe koje ste dobili s uređajem ili pronaći njihovu najnoviju inačicu na internetu. Bitno je naglasiti da su ažurirani upravljački programi nužni za ispravan rad računala i znatno utječu na cjelokupnu stabilnost sustava (Car, Medić, 2017).

Za one koji žele znati više

Više o instalaciji upravljačkih programa te njihovu ažuriranju možete pronaći na: https://support.microsoft.com/hr-hr/help/4028443/windows-update-drivers-in-windows-10

BIOS

U dijelu o građi računala operativni je sustav opisan kao jedan vid sučelja, poveznice između čovjeka i računala. Na sličan se način može opisati i BIOS, kao skup računalnih programa koji omogućava osnovnu komunikaciju sa sastavnicama pri pokretanju.

BIOS-u se pristupa kod pokretanja računala, i to **kombinacijom tipki koja je obično ispisana na ekranu pri pokretanju**.

Ako tablet, stolno ili prijenosno računalo s Microsoft Windows operativnim sustavom javi poruku **Operating sistem not found** (vidi sliku 4.), prije nego što posumnjamo na

kvar diska možda je potrebno promijenit redoslijed pogona s kojih će se operativni sustav podizati.

Za one koji žele znati više

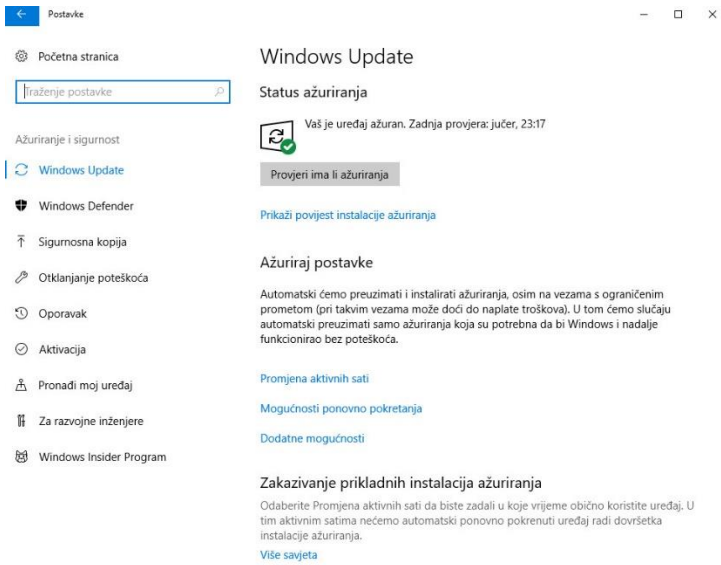
Više o promjeni redoslijeda pokretanja u BIOS-u može se naći na https://www.lifewire.com/change-the-boot-order-in-bios-2624528 (sadržaj je na engleskom jeziku).

1.3 Softverski uzrokovana nestabilnost u radu

Za siguran je i pouzdan rad bilo kojeg računala, tableta ili pametnog telefona od iznimne važnosti imati instalirana zadnja ažuriranja operativnog sustava jer ona otklanjaju uočene nedostatke i sigurnosne propuste u operativnom sustavu. Navedeno je od posebne važnosti za uređaje koji se rabe u nastavnom procesu jer je na njima nužno zaštititi osobne podatke te općenito sav digitalni sadržaj.

Kada govorimo o računalima s operativnim sustavom Microsoft Windows, zadnja ažuriranja skidaju se s Microsoftova web-mjesta koje se zove *Windows Update.* Bez obzira na to o kojoj je inačici operativnog sustava riječ, ažuriranje Windowsa nalazi se na istome mjestu u sklopu upravljačke ploče.

Pristupa se slijedom **Start → Postavke → Ažuriranje i sigurnost → Windows Update.** Posumnjate li da računalo nije ažurirano, treba odabrati opciju **Provjeri ima li ažuriranja.**



Slika 11. Windows Update

Slično i kod operativnog sustava iOS, koji se nalazi na svim Appleovim uređajima (tableti, pametni telefoni), možemo provjeriti je li uređaj ažuriran u **Postavke → Općenito → Ažuriranje softvera.** Kod Android operativnog sustava slijed je **Postavke → O uređaju → Nadogradnja softvera → Nadogradi.**

Slika 12. iOS nadogradnja

Kada je riječ o „nadopuni“ operativnog sustava Windows, vrlo je bitno razlikovati ažuriranje i nadogradnju. Prije pojave Windowsa 10, ako smo željeli nadogradnju na višu inačicu operativnog sustava, npr. s Windowsa XP na Windowse 7 ili s Windowsa 7 na Windowse 8, morali smo proći složeniji put nadogradnje koji je uključivao posjedovanje instalacijskog medija s novijom verzijom sustava te specifična tehnička znanja.

S pojavom Windowsa 10 odustalo se od takvog načina nadogradnje i prema sadašnjem stavu Microsofta više to nikada nećemo morati niti raditi jer će se novija inačica operativnog sustava automatski preuzimati s Microsoftova servisa za nadogradnju. Preuzimat će se u pozadini, bez potrebe za bilo kakvom interakcijom krajnjeg korisnika.

Kada računalo ispunjava uvjete za nadogradnju, ona će se automatski preuzeti s Microsoftova servisa Windows Update i računalo će se nadograditi na najnoviju inačicu operativnog sustava.

2. poglavlje: **Rješavanje tehničkih problema**

U ovom poglavlju naučit ćete:

- ☑ što su Windows vatrozid i Windows Defender
- ☑ o korisničkim računima
- ☑ o oporavku sustava.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

2.1 Prijetnje na internetu

Jedna od većih opasnosti pri radu na internetu zasigurno su razni oblici štetnog softvera. Korištenje vatrozidom i antivirusnim programima te već spomenuto ažuriranje operativnog sustava osnovni su preduvjeti za sprečavanje štetnih događaja (Gollman, 2011).

Zaštita podataka, posebice na razini škola, podrazumijeva sljedeće:

- definiranje i provođenje politike lozinki
- ovlašten pristup povjerljivim podacima samo određenim osobama
- čuvanje integriteta podataka (nitko ne može mijenjati podatke bez dopuštenja vlasnika podataka)
- dostupnost i raspoloživost podataka ovlaštenim osobama kada su im potrebni
- sigurnosnu pohranu podataka.

Iako zvuče složeno, neke od ovih aspekata možemo osigurati sami. Bitno je kod kolega, suradnika i učenika podizati svijest o važnosti brige o tome kada se, gdje i pod kojim uvjetima ostavljaju podaci kao i o tome da otvaranju sumnjivih poruka ili poruka nepoznatih pošiljatelja valja postupati s krajnjim oprezom. Kod postavljanja lozinki na svim uslugama (elektronička pošta i sl.), pa čak i na računu za prijavu u vlastito računalo, valja se koristiti kompleksnijom lozinkom. Preporučeno je rabiti kombinaciju velikih i malih slova te brojeva. Jednako tako treba paziti da lozinka sadržava duži niz znakova jer se time smanjuje mogućnost otkrivanja i krađe lozinke.

Da je štetni program zarazio računalo utvrđuje se u ovakvim situacijama:

- računalo iznenada postane sporo (a isključili smo npr. nedostatnu radnu memoriju)
- pojavi se mnogo skočnih prozora koji sadržavaju reklame ili neprimjereni sadržaj
- povezivanje na mrežu je neuspješno ili je veza vrlo spora
- pojavljuju se nepoznate datoteke odnosno digitalni sadržaji
- nestanu digitalni sadržaj, sistemske datoteke ili se postojeće datoteke odjednom više ne mogu otvoriti.

Primijetite li jedan ili više navedenih simptoma, preporučuje se sljedeće:

- odspojiti računalo s mreže – ako je riječ o stolnom računalu, izvucite mrežni kabel ili pokušate odspojiti tablet ili prijenosno računalo s bežične mreže, time smanjujete mogućnost širenja zaraze i ukidate neovlašteni mrežni pristup računalu
- obavijestiti vašega sistemskoga i mrežnog administratora – iznimno je važno čim prije obavijestiti stručnu osobu koja može prevenirati dodatnu te pokušati sanirati nastalu štetu
- pogledati postavke vatrozida (imate li ovlasti) pa ga uključiti ako već nije uključen – neovisno o prvom koraku, ovaj korak može pomoći pri spajanju na bežične mreže
- pokrenuti antivirusni program – promptno pokretanje antivirusnog programa može zlonamjerni program staviti u karantenu i zaustaviti njegovo izvršavanje.

Nikako ne pozivajte telefonske brojeve koji se mogu pojaviti na skočnim prozorima niti ne slijedite moguće upute da putem unosa podataka s kreditnih kartica plaćate ponude za „čišćenje virusa“. Ako to napravite, ne samo da ćete ostati bez vaših datoteka nego postoji i opasnost od krađe broja kreditne kartice te gubitka određenog iznosa. Pogledajmo detaljniji pregled štetnog softvera.

Virusi

Virusi pri svom izvršavanju pokušavaju kopirati sami sebe unutar druge aplikacije odnosno programa kojima se koristimo. Virus se širi i umnožava unutar jednog računala te pokušava širenje na druga računala u mreži. Naravno, ne smijemo zaboraviti da je idealan put širenja virusa bilo koji oblik digitalnog sadržaja, pa čak i slike. Osim putem mreže, širenje zaraženoga digitalnog sadržaja moguće je putem različitih medija poput USB štapića, prijenosnih diskova, CD/DVD medija i sl.

Čest slučaj širenja virusa jest putem elektroničke pošte, pri čemu treba imati na umu da se virus sa zaređenog računala može proširiti tako da svim kontaktima u adresaru pošalje elektroničku poruku koja će, naravno, sadržavati i zlonamjerni kod. Također su mogući virusi koji inficiraju sektore za pokretanje operativnog sustava te virusi koji inficiraju izvršne datoteke i makroviruse.

Korisnicima operativnog sustava Windows odnosno korisnicima Microsoft Office paketa savjetuje se paziti na tzv. makroviruse koji inficiraju samo dokumente izrađene u programima koji podržavaju makronaredbe poput Microsoftova Worda, Excela i sl. Takvi se virusi šire u trenutku otvaranja dokumenta.

Ako putem elektroničke pošte zaprimite dokument u Wordu ili Excelu, a niste sigurni smije li se otvoriti, najbolje ga je zadržati u zaštićenom načinu prikaza (engl. *Protected view*). Samo ako postoji sigurnost u ispravnost takvog dokumenta u redu je omogućiti uređivanje te pohranu na računalo (Bobovec, Car, 2017).

Slika 13. Zaštićeni način prikaza kod Microsoft Office aplikacija

Ovoliko oblika zaraze i širenja virusa pri svakodnevnoj uporabi računala može djelovati zastrašujuće. No u praksi malo opreznosti kod npr. otvaranja privitaka u elektroničkoj pošti te korištenje ažuriranim antivirusnim programom znatno smanjuju mogućnost zaraze. Posumnjate li na zarazu, jednostavno slijedite osnovne upute s početka poglavlja.

Crvi

Za razliku od virusa, crvi su sposobni samostalno tražiti sustave domaćine i inficirati ih preko mreže. Iako će mnogi poistovjetiti viruse s crvima, bitno je naglasiti da se virusi šire inficirajući druge programe, a crvi imaju sposobnost samostalne migracije s računala na računalo odnosno operativnog sustava preko mreže, bez pomoći drugih

aplikacija (Bobovec, Car, 2017). Za zaštitu od crva slijedite isti savjet koji je naveden kod virusa.

Špijunski kod

Posebna vrsta štetnog softvera naziva se špijunski kod. On sakuplja podatke o korisniku pa tako nakon inficiranja računala može:

- pratiti naše aktivnosti
- pratiti koje smo programe otvorili i koliko ih upotrebljavali te
- mijenjati postavke internetskog preglednika te tako dodatno ugroziti sigurnost računala.

S obzirom na to da može bilježiti npr. unos s tipkovnice, osim krađe identiteta i/ili osobnih podataka špijunski kod može doprijeti i do PIN-ova, lozinki, bankovnih podataka i sl. (Bobovec, Car, 2017). Osnovna je zaštita protiv špijunskog koda ista kao kod virusa i crva.

Ucjenjivački softver

Ucjenjivački softver (engl. *ransomware*) posebna je vrsta štetnog programa koji kriptira korisnikove podatke na disku i traži otkupninu za pristup njima. Ovaj je softver prepoznatljiv po jasno naznačenoj uputi za plaćanje otkupnine i nemogućnosti pristupa podacima na disku. Jedini je siguran način zaštite redovita sigurnosna pohrana podataka i pridržavanje dosada navedenih sigurnosnih savjeta. Plaćanje otkupnine nikako ne jamči povrat podataka te ne sprečava njihovo objavljivanje.

Reklamni kod

Reklamni kod odnosno reklamne programe (engl. *adware*) nalazimo, uglavnom, kod „besplatnih“ programa koji zahtijevaju da se složimo s uvjetima korištenja koji dopuštaju prikaz različitih reklama. Reklamni programi u pravilu nisu štetni softver, no treba pažljivo prolaziti kroz proces instalacije, čitati uvjete korištenja programom s kojima se slažemo te posebno pažljivo gledati što sve dopuštamo reklamnom programu da prilagodi na računalu.

Nakon što smo ga instalirali takav program može (ali i ne mora):

- sakupljati informacije o korisniku, njegovim pretraživanjima i sl. te na temelju tako prikupljenih informacija korisniku prikazivati oglase koji bi ga mogli zanimati
- mijenjati postavke web-preglednika: preglednik se preusmjerava na određena web-mjesta s ciljem potencijalne prodaje ili sl.
- modificirati određene postavke operativnog sustava koje se odnose na rad na mreži i znatno narušiti performanse računala.

Stoga se još jednom skreće pozornost na važnost provjere svih navedenih koraka pri instalaciji programa.

2.2 Pravodobna zaštita računala

Sigurnosna zaštita računala uglavnom je dio politike institucija. Kako smo spomenuli ranije, dobar dio koraka prema boljoj zaštiti možemo napraviti sami:

- obvezna je upotreba lozinke za prijavu na računalo, odnosno upotreba korisničkog računa
- nemojte se prijavljivati na računalo s administratorskim ovlastima
- na računalo instalirajte samo nužan softver za rad u učionici
- programe preuzimajte samo sa službenih web-mjesta
- konfigurirajte odnosno uključite vatrozid na računalu
- redovito primjenjujte sigurnosna ažuriranja
- koristite se antivirusnim programima: oni moraju biti instalirani i konfigurirani na računalima
- uključite sigurnosne funkcije internetskog preglednika te isključite sve nepotrebne dodatke i ekstenzije
- pretražujući internet koristite se sigurnim vezama, odnosno onima koje rabe https protokol s obzirom na to da je u takvim slučajevima riječ o kriptiranome komunikacijskom kanalu
- budite oprezni kod otvaranja elektroničkih poruka
- izbjegavajte spajanje na nezaštićene WiFi mreže (Žižek, 2014).[1]

Promotrimo u nastavku dvije važne sastavnice zaštite operativnog sustava Windows: vatrozid i antivirusni program.

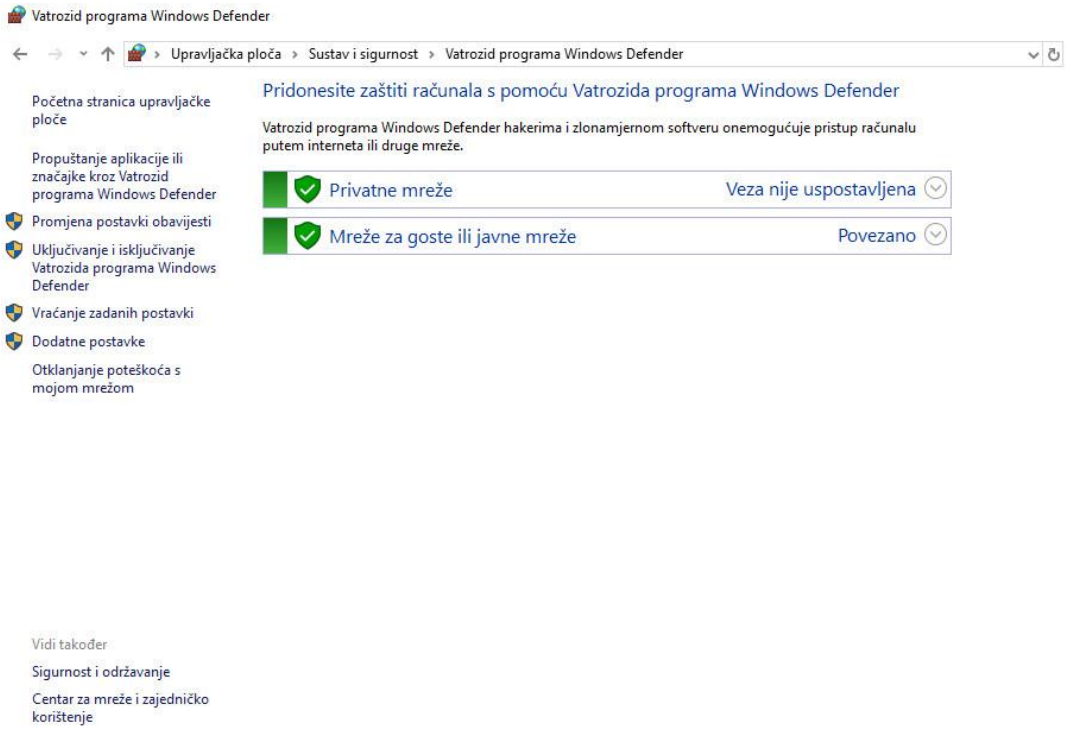
Vatrozid

Vatrozid (engl. *firewall*) može biti softversko rješenje, kao na primjeru Windows vatrozida, ili hardverska komponenta na mreži (posjeduje ga usmjernik). Namjena mu je sprečavanje zaštita od raznih vrsta štetnih napada i prodiranja *zlonamjernih aplikacija* na računala. Funkcionira tako da provjerava mrežni promet te ga blokira ili propušta prema definiranom skupu pravila.

Windows Vatrozid ugrađena je funkcija unutar sustava Windows i zadano je uključen. Preporučuje se da bude uključen za sve tipove mrežnih veza (*Private, Public, Domain*), kao i za sve vrste mrežnih veza (posebno za WiFi). Preporučeno je također prilagoditi ga tako da blokira sav promet osim onoga koji eksplicitno dopustimo.

Prilagođavanja za vatrozid nalaze se u **Upravljačka ploča → Mreža i Internet → Centar za mreže i zajedničko korištenje** te zatim s lijeve strane odaberemo **Vatrozid programa Windows Defender**.

[1] https://sysportal.carnet.hr/node/1386



Slika 14. Vatrozid programa Windows Defender

Ispravno uključen vatrozid bitna je komponenta zaštite i ako nismo sigurni jesmo li nakon mijenjanja zadanih postavki zadovoljili sve uvjete zaštite našeg računala, najbolje je koristiti se mogućnošću s lijeve strane: **Vraćanje zadanih postavki** (Car, Medić, 2017).

Antivirusni programi

Danas na tržištu postoji više zaštitnih alata čija je namjena zaštita računala od zlonamjernih programa. Operativni sustavi Windows već imaju instaliran **Windows Defender.** Pri pronalasku virusa odnosno zaražene aplikacije program takvu datoteku premješta u karantenu – područje za dezinfekciju i uklanjanje, čime se sprečava da štetni kod uspostavi kontakt s drugim programima ili da zarazi druge datoteke.

Nijedan zaštitni program nije uvijek u potpunosti učinkovit. Moguće je da nekad neće moći otkriti ili otkloniti neki specifični zlonamjerni program i potrebno se stoga poslužiti drugim sredstvima. No zaštita je pouzdana dok su god zaštitni programi ažurirani najnovijim funkcionalnostima (Pipkin, 2000).

Danas je na tržištu dostupno nekoliko desetaka antivirusnih programa. Neki od njih su:

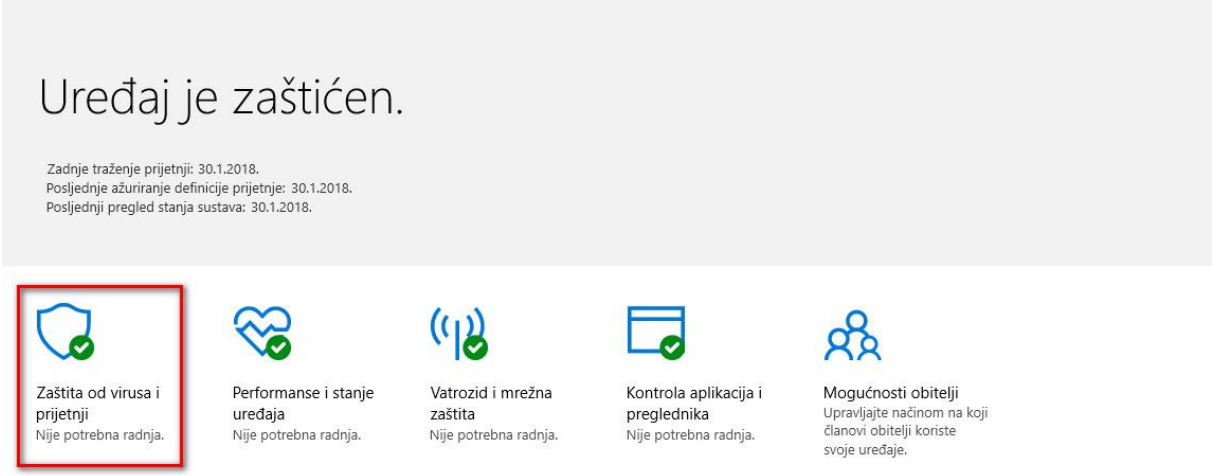
- Bitdefender
- Norton
- Kaspersky
- Avira
- Avast

- ESET
- Trend Micro
- F-Secure
- McAfee.

No navedene je programe potrebno je potražiti na internetu, instalirati na računalo te vjerojatno platiti licenciju za korištenje. Na računalu ne smiju istodobno biti konfigurirana dva antivirusna programa, a operativni sustav Windows, kako smo naveli, već ima učinkovit alat **Windows Defender**.

Riječ je o programu koji se automatski pokreće pri pokretanju našeg računala te može pridonijeti zaštiti od štetnih programa.

S operativnim sustavom Windows 10 došla su i određena poboljšanja Windows Defendera, a novina je **Windows Defender Security Center** koji pokrećemo preko izbornika Start.



Slika 15. Prikaz Windows Defender centra za sigurnost

Novina sigurnosnog centra odnosno ove funkcionalnosti jest u potpunom pregledu sigurnosnih postavki našeg računala.

Ako sumnjamo na neku zarazu bilo kojom vrstom štetnog koda, potrebno je kliknuti na **Zaštita od virusa i prijetnje** te kliknuti na **Brzi pregled**.

2.3 Upotreba kontrole korisničkih računa

Pri prijavi u operativni sustav Windows 10 potrebno je rabiti korisnički račun. Bitno je to zbog zaštite računala i njegova sadržaja, ali i kao dio zaštite od štetnih programa. Operativni sustavi Windows razlikuju nekoliko vrsta korisničkih računa:

- Microsoftov račun (kreiran pri otvaranju servisa Outlook.com ili sličnih servisa)
- korisnički račun Active Directory
- lokalni korisnički račun
- korisnički račun Microsoft Azure.

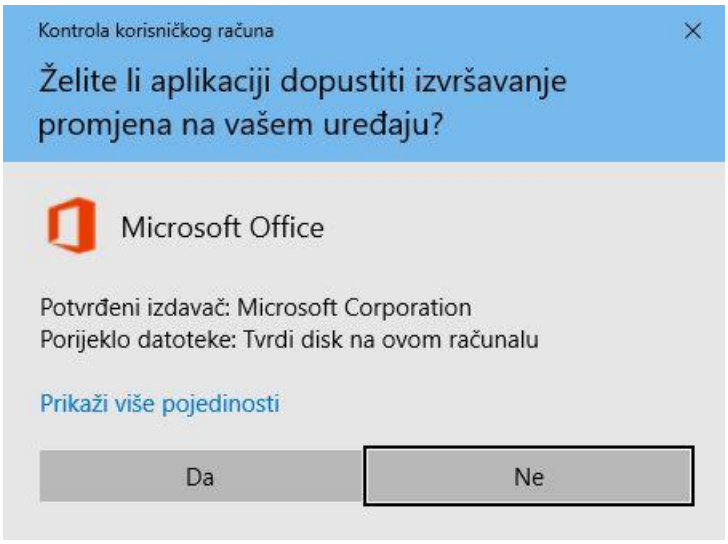
Uz pomoć korisničkog računa obavljamo autentikaciju odnosno identifikaciju s kojom dokazujemo da smo točno određeni korisnik. Svaki bi korisnički račun trebao imati pripadajuću lozinku. Kako smo prije naveli, lozinke bi trebale biti složene. To u praksi znači da se moraju sastojati od najmanje jednoga velikog slova, najmanje jednoga malog slova, najmanje jednoga posebnog znaka i ne smiju biti kraće od 8 znakova, a poželjno je i više. Primjeri loše odabranih lozinki jesu:

- zaporke s očitim asocijacijama kao što su prezime ili datum rođenja
- zaporke kraće od 8 znakova (zaporke veće duljine teže je pogoditi, a najveća je moguća duljina zaporki 127 znakova).

Kontrola korisničkog računa

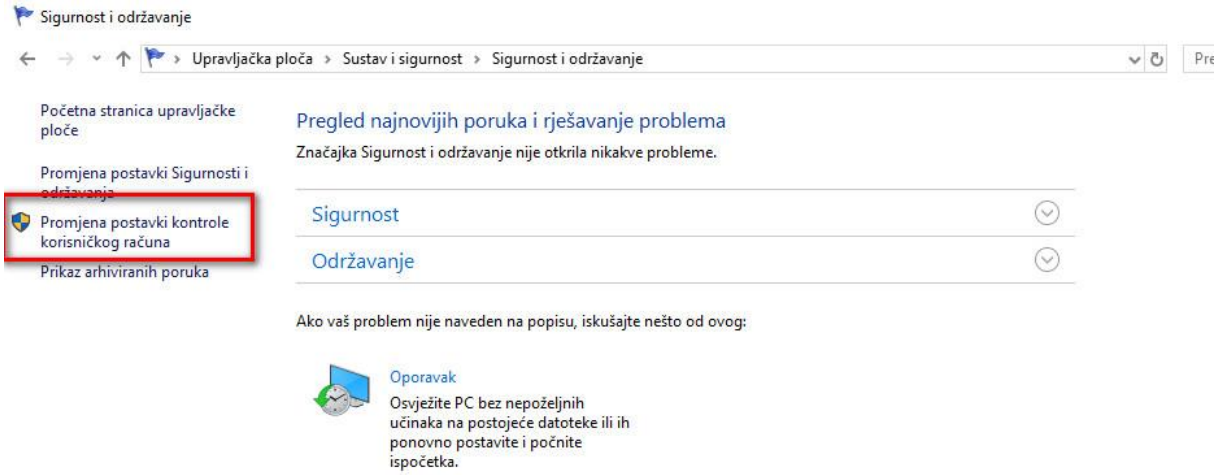
Kontrola korisničkog računa još je jedan od slojeva zaštite našega digitalnog identiteta i digitalnog sadržaja. Riječ je o ugrađenoj funkcionalnosti u operativnim sustavima Windows 8.1 i novijima kojom se sprečavaju neovlaštene promjene na računalu, a koje bi mogle prouzročiti nestabilnost samog sustava. Prije izvršenja bilo koje radnje koja bi mogla utjecati na rad računala ili kojom bi se mogle izmijeniti postavke koje utječu i na druge korisnike, UAC (engl. *User Account Control* = kontrola korisničkog računa) će zatražiti dopuštenje ili administratorsku zaporku. Kada se pojavi poruka UAC-a, trebate je pažljivo pročitati i provjeriti je li radnja ili program koji se pokreće uistinu onaj koji želite pokrenuti.

Potvrđivanjem tih radnji prije njihova izvršenja UAC može spriječiti instaliranje zlonamjernih programa (engl. *malware*) i špijunskih programa (engl. *spyware*), odnosno spriječiti nedopuštene promjene na računalu.



Slika 16. Poruka kontrole korisničkog računa koja se javila pri pokušaju instalacije Microsoft Office paketa

Postavke kontrole korisničkog računa možemo promijeniti, odnosno provjeriti tako da otvorimo **Upravljačka ploča → Sustav i sigurnost → Sigurnost i održavanje.**



Slika 17. Promjena postavki kontrole korisničkog računa

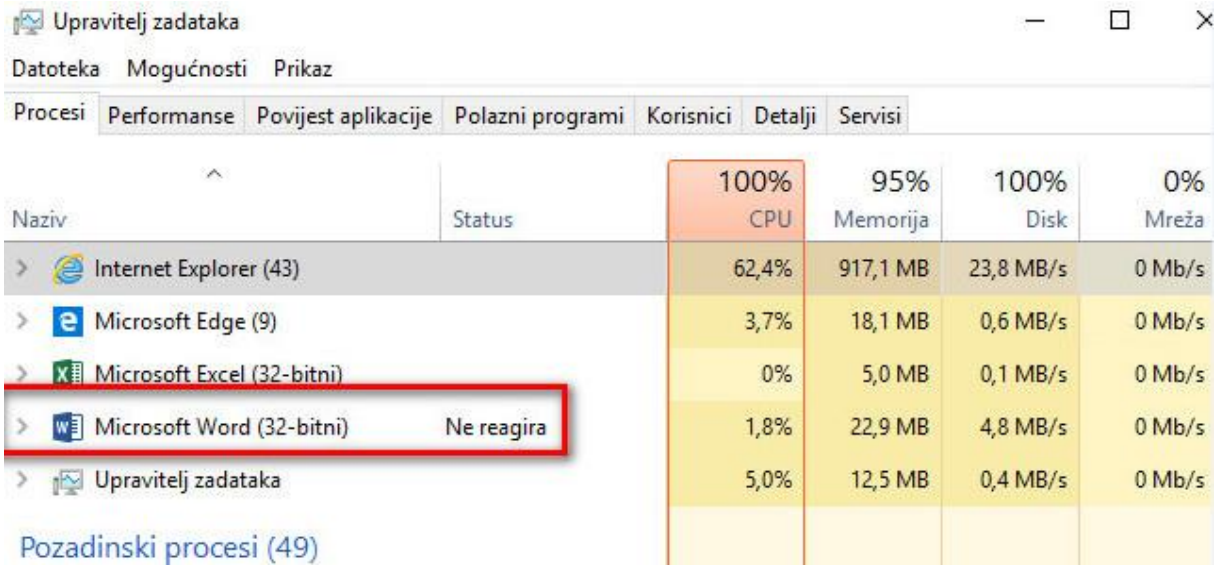
Nakon što se sučelje otvorilo, potrebno je s lijeve strane odabrati **Promjena postavki kontrole korisničkog računa**.

Preporučljivo je rabiti opciju **Uvijek me obavještavaj** pri čemu će se tražiti dodatna potvrda svaki put kada pokušamo promijeniti postavke sustava Windows i kada se neka od aplikacija pokuša instalirati na naše računalo (Car, Medić, 2017).

Europska unija
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

2.4 Rješavanje problema s nepouzdanim radom računala uz pomoć sistemskih alata

Katkad instalacija nekog programa, iako nije donijela i zarazu s virusom, može računalo učiniti nepouzdanim. Primjerice to se može očitovati „smrzavanjem“ aplikacije ili aplikacija koje su do sada pouzdano radile. Rad aplikacije moguće je prekinuti s pomoću kombinacije tipki **Ctrl+Alt+Delete → Upravitelj zadataka** (engl. *Task Manager*). Desnim klikom miša na aplikaciju odabiremo opciju **Završi zadatak**. No to je kratkoročno rješenje i možda će novu aplikaciju trebati ukloniti s računala.



Slika 18. Prikaz aplikacije u upravitelju zadataka koja je ne reagira

Deinstalacija programa

Programi potrebni za rad na računalu trebaju se najprije postaviti na sustav (*instalirati*). Proces instalacije uglavnom je automatski i zahtijeva minimalnu intervenciju korisnika.

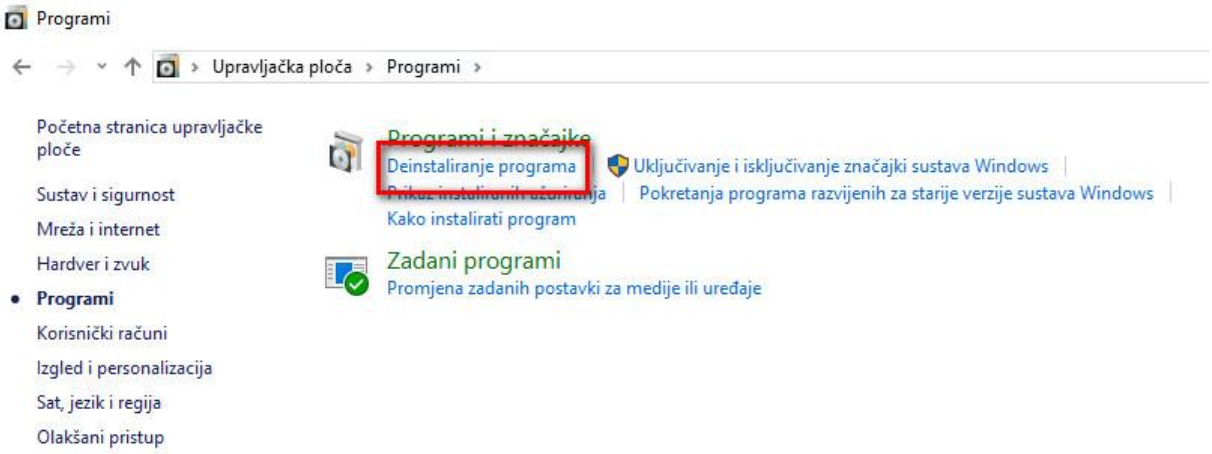
Pri pokretanju programa operativni sustav mora u spremnik istodobno smjestiti i instrukcije i podatke programa te započeti s njegovim izvođenjem. Od tog trenutka zapravo govorimo o *procesu* koji se izvodi, a koji pritom zauzima određena sredstva računalnog sustava: spremnik, procesorsko vrijeme, radnu memoriju…

Operativni sustav mora osigurati da se svi procesi nesmetano izvode (da jedan ne utječe na performanse drugog). Problemi koji se mogu pojaviti vezani su za pristup sredstvima sustava, nama se to očituje u obliku nestabilnosti sustava, nemogućnosti pokretanja upravo instaliranoga ili nekoga drugog programa i sl.

Ako se pojavi takav problem, prva je pomoć uklanjanje instaliranog programa. Osim toga, trebalo bi ukloniti i posljednje ažuriranje Windows Updatea primijeti li se slična situacija.

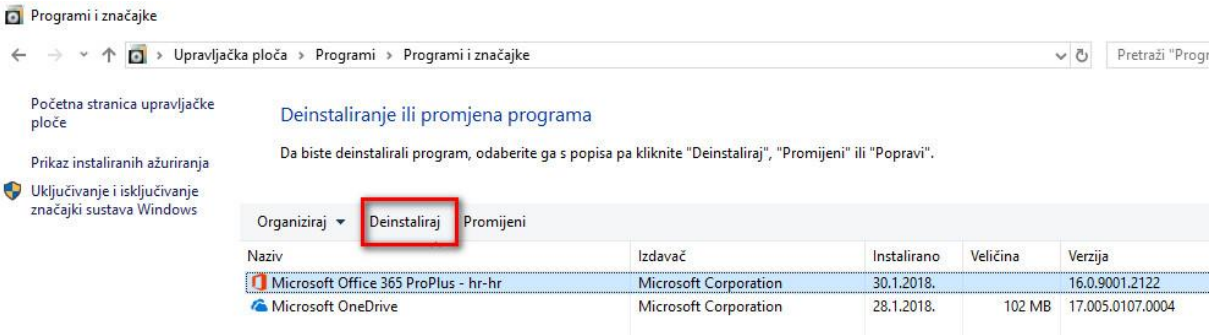
Europska unija Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Programi se deinstaliraju ovako: **Upravljačka ploča → Programi.**



Slika 19. Deinstaliranje programa

Nakon što smo kliknuli na **Deinstaliranje programa**, otvara se sučelje u kojem je potrebno odabrati posljednji instalirani program te odabrati opciju **Deinstaliraj**.

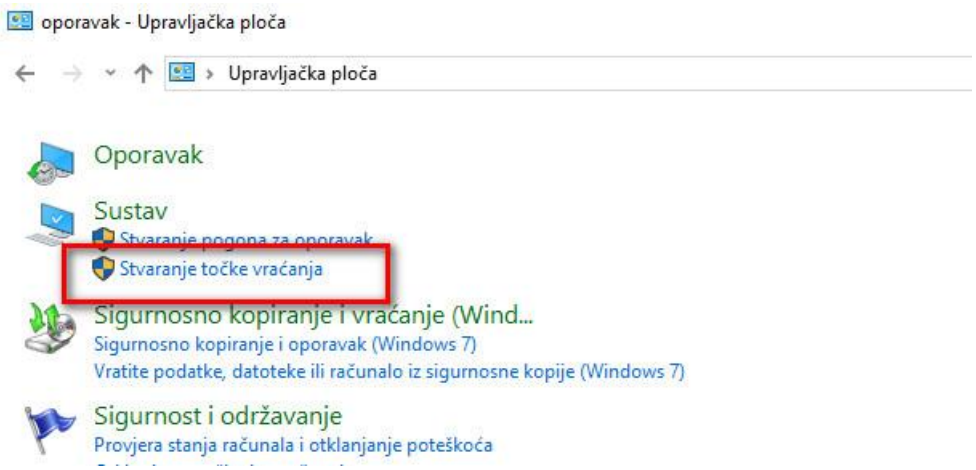


Slika 20. Odabir programa koji želimo deinstalirati

Oporavak Windowsa 10

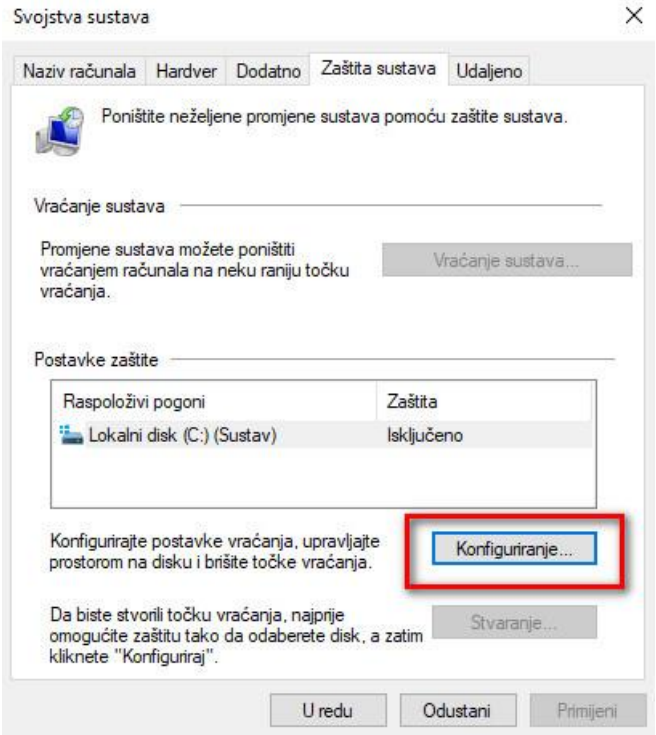
Ako ni nakon deinstalacije programa računalo nije vraćeno u stabilno stanje, potrebno je napraviti oporavak sustava Microsoft Windows 10. Stoga računalo treba konfigurirati tako da dopušta tu mogućnost, odnosno treba otvoriti **Upravljačku ploču** te odabrati **Stvaranje točke vraćanja.**

Europska unija
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr



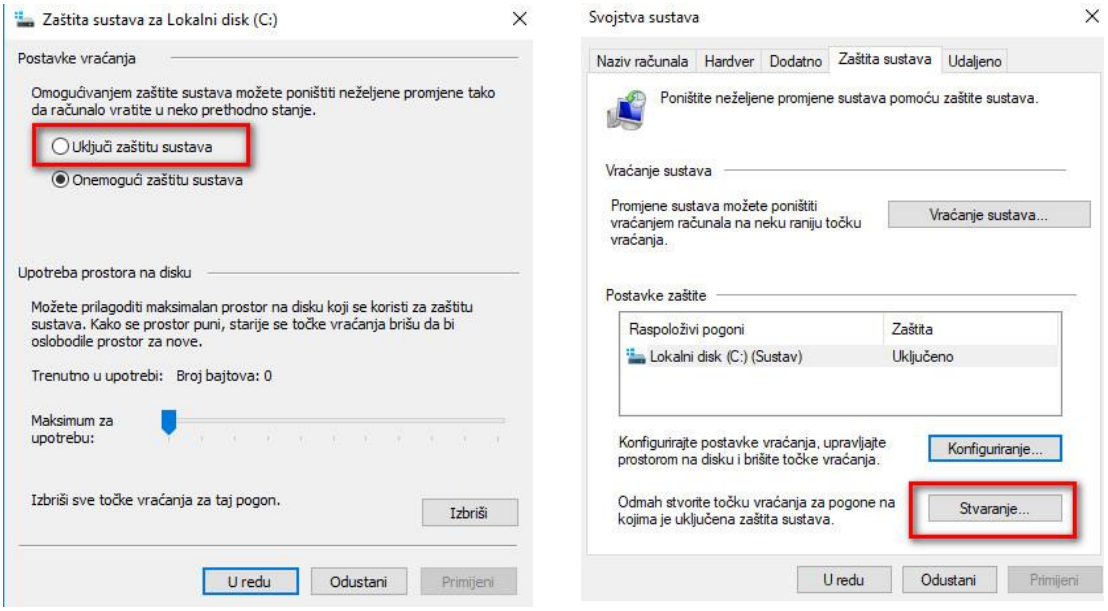
Slika 21. Stvaranje točke vraćanja

Nakon što smo odabrali **Stvaranje točke vraćanja** otvara se sljedeće dijaloško sučelje prikazano na slici u nastavku.



Slika 22. Konfiguriranje točke vraćanja

Nakon što smo kliknuli na **Konfiguriranje…** potrebno je kliknuti na **Uključi zaštitu sustava** te ju potom stvoriti odabirom opcije **Stvaranje…**.



Slika 23. Stvaranje točke oporavka

Nakon tih koraka možemo pristupiti oporavku sustava Microsoft Windows 10 odnosno našeg računala. Potrebno je odabrati **Vraćanje sustava…**.

Ovime smo računalo vratili u prethodno stanje. Navedenim postupkom **neće** se izgubiti datoteke (prezentacije, učenički seminari, osobni dokumenti…) koje smo u međuvremenu pohranili na disk. Oporavak ne utječe na korisničke, nego samo na sistemske datoteke, tj. na datoteke važne za rad operativnog sustava.

Europska unija
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

3. poglavlje: **Stvaranje baze znanja i unapređenje procesa**

U ovom poglavlju naučit ćete:

- ☑ koja je važnost baze znanja
- ☑ što je SharePoint Wikipedija
- ☑ što je OneDrive.

Važnost baze znanja

Kvalitetne informacije i znanje prikupljeno u profesionalnom razvoju često želimo podijeliti. Prikupljene informacije najprije treba strukturirano organizirati te podijeliti sa suradnicima u timu, čime se povećava znanje i unapređuje suradnja.

Korisno je stoga kreiranje baze znanja koja školama pomaže u prikupljanju znanje na jednome mjestu. Baze znanja možemo dijeliti ili s kolegama ili s generacijama učenika te ih iz godine u godinu nadopunjavati i širiti.

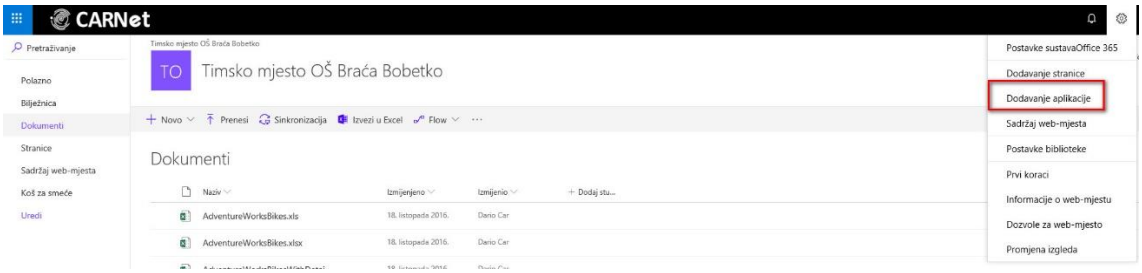
Danas na raspolaganju imamo različite sustave, aplikacije, metodologije i tehnike za upravljanje znanjem. Neke aplikacije koje pomažu ubrzati razmjenu znanja i poboljšati komunikaciju dostupne su u sklopu sustava Office 365 za škole. Riječ je o aplikacijama u oblaku za koje nije potrebno rezervirati dodatne resurse vezane za održavanje ili upravljanje.

Za one koji žele znati više

Više o Office 365 paketu za škole možete naći u priručniku „Office 365“ na: http://bit.ly/2FsUC26

Osim velikog spektra alata za suradnju i razmjene znanja pokrivenih u okviru drugih webinara, korisno je spomenuti još jednu mogućnost. Microsoft je u sklopu sustava **SharePoint Online** dodao mogućnost kreiranja **Wikipedije**. S načelom korištenja upoznati smo putem istoimene *online* kolaborativne enciklopedije. U SharePointu Wikipediju kreiramo na sljedeći način:

Prijavimo se na SharePoint i odaberemo **Postavke ( ) → Dodavanje aplikacije**



Slika 24. Dodavanje aplikacije

Iz ponuđenog popisa aplikacija odaberemo **Biblioteka wiki stranica** te definiramo naziv**.** Potvrdimo sa **Stvori.** Nakon toga je Wikipedija koju smo kreirali spremna za korištenje i kreiranje baze znanja koju možemo podijeliti s učenicima odnosno suradnicima.

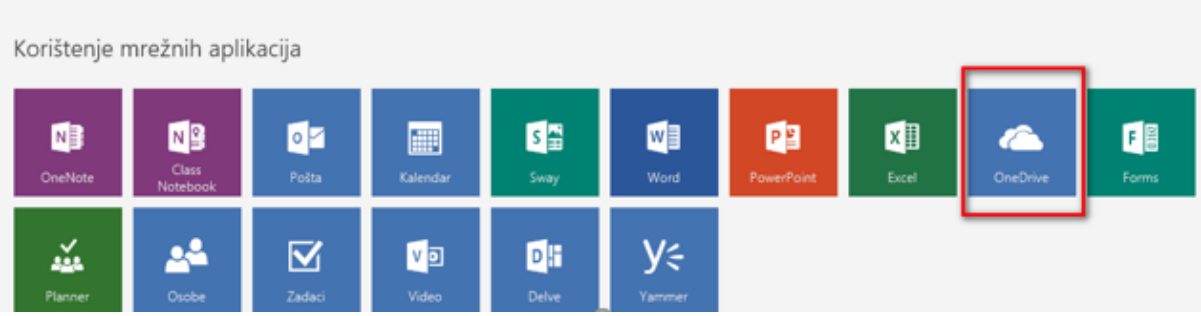
Korištenje aplikacijom OneDrive

OneDrive je aplikacija u oblaku koju nalazimo u sklopu sustava Office 365. Sama aplikacija ima nekoliko namjena, a jedna od njih jest pohrana i dijeljenje dokumenata sa suradnicima. S obzirom na to da je u priručniku nekoliko puta spomenuta važnost izrade sigurnosne kopije, aplikaciju OneDrive sagledat ćemo upravo s tog aspekta.

OneDrive je jednostavan za administraciju i korištenje, a iznimno je pogodan kao oblik sigurnosne pohrane dokumenata koji se nalaze na računalu – sve datoteke iz mape OneDrive koja se nalazi na našem računalu pohranit će se u oblaku.

S obzirom na spomenute mogućnosti gubitka podataka zbog kvara čvrstog diska, gubitka/krađe računala ili štetnog softvera, treba istaknuti da se pri upotrebi aplikacije OneDrive gube podaci na računalu, međutim oni i dalje ostaju u oblačnom spremištu podataka. Nakon zamjene diska i/ili računala te ponovnog postavljanja OneDrivea na računalu, podaci će se sinkronizirati na naše računalo.

Aplikacija je korisna kao zamjena za USB štapiće ili kada nam je datoteka prevelika za slanje putem elektroničke pošte.



Slika 25. Prijava na OneDrive

Upotreba OneDrivea moguća je na nekoliko načina, primjerice može poslužiti kao mjesto za pohranu podataka, zatim kao način pristupa dokumentima s bilo kojeg uređaja, uključivo i pametne telefone ili kao alat za suradnju i dijeljenje dokumenata.

Pristup datotekama moguće je ostvariti:

- kroz web-preglednik
- iz Microsoft Office 2013/2016 aplikacija poput Worda, Excela, PowerPointa
- kroz Windowsov preglednik (engl. *Windows Explorer*)
- iz Microsoft Office aplikacija napravljenih za pametne telefone (iPhone, Windows Phone, Androidovi uređaji i telefoni) (Car, Kralj 2015).

Za one koji žele znati više

Više o aplikaciji OneDrive možete naći u priručniku „Office 365“ na: http://bit.ly/2FsUC26

4. poglavlje: **Spajanje na mrežu**

U ovom poglavlju naučit ćete:

- ☑ koje su vrste računalnih mreža
- ☑ o zaštiti mreža
- ☑ o spajanju na mrežu.

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Računalne mreže

Računalna mreža nastaje kada međusobno povezana dva ili više računala mogu razmjenjivati informacije. Računalne se mreže mogu podijeliti na:

- **LAN (**engl. ***Local Area Network*****)** – lokalna mreža, npr. računalna mreža unutar škole ili ona koju posjedujemo kod kuće nazivamo lokalnom mrežom.
    - LAN mreže mogu biti žičane i bežične.
- **WAN (**engl. ***Wide Area Network*****)** – mreža širokog područja (engl. *Wide Area Network*) je mreža koja spaja različite lokalne mreže.
    - Sinonim za WAN mrežu je internet.

Razmjena informacija računalnom mrežom osim svih prednosti nosi i potencijalne opasnosti, kao što su krađa digitalnog sadržaja i osobnih informacija te mogućnost zaraze računala različitim štetnim programima.

Bežične mreže

Bežične mreže za prijenos informacija rabe radiovalove malih valnih duljina. Sastavnice bežičnih računalnih mreža jesu računala (tableti, stolna računala, pametni telefoni) te pristupni uređaji. Pristupni uređaj (engl. *access point*) logički povezuje više računala međusobno i osigurava im pristup internetu (Bobovec, Car, 2017). Bežične su mreže zbog svoje praktičnosti našle široku primjenu u obrazovnim ustanovama. Kako se informacije prenose radiovalovima, spajanje na njih te njihova upotreba nose daleko više opasnosti od povezivanja putem žičanih mreža te valja na umu imati potencijalne rizike. O prepoznavanju i smanjivanju rizika više će riječi biti u nastavku teksta.

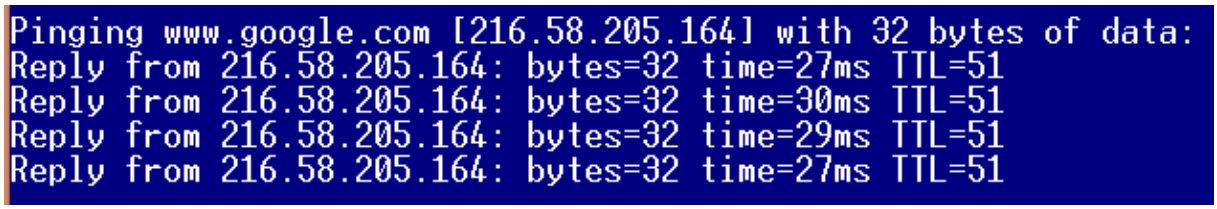
Osnove internetske sigurnosti

Za razumijevanje osnova sigurnosti u računalnim mrežama razmotrit ćemo najprije osnove funkcioniranja računalnih mreža odnosno interneta.

Kada govorimo o prometu koji se odvija na internetu, bitno je reći da se on zasniva na strogo definiranim protokolima. Svaki uređaj spojen ma računalnu mrežu ima svoju adresu, koju zovemo IP adresom i ona je predstavljena nizom brojeva. S obzirom na to da je ljudima nešto teže pamtiti brojeve, poslužitelji uz IP adresu imaju i svoje „ime“, npr. www.carnet.hr, www.srce.hr itd. Sustav koji, ljudima prihvatljivija, imena pretvara u, serverima razumljive, IP adrese naziva se DNS (engl. *Domain Name System*).

Dakle, kada u internetski preglednik upišemo https://www.google.com, DNS sustav napraviti će tzv. imensku rezoluciju i računalu vratiti IP adresu željenog poslužitelja, u ovome slučaju Googlea.

Tek u tome trenutku kreće naš zahtjev za otvaranjem web-stranice (engl. *request*) prema poslužitelju, nakon čega slijedi njegov odgovor (engl. *response*) u obliku tražene web-stranice. Primjer provjere dostupnosti IP adrese poslužitelja Google dan je na slici u nastavku.



Slika 26. Provjera mrežne dostupnosti IP adrese poslužitelja Google

Ako IP adresu poslužitelja upišemo u internetski preglednik, u obliku https://216.58.205.164, otvorit će se Googleova stranica.

Ovaj smo kratki uvod u način kako „radi“ internet odnosno bilo koja mreža napravili kako bismo mogli povući paralelu s primjerom iz svakodnevnog života. Protokol kojim šaljemo podatke sličan je procedurama koje se rabe kod slanja (klasične) pošte. Recimo da želite poslati knjigu poštom, uz jedan uvjet: možete se koristiti samo poštanskim omotnicama. Najprije morate rastaviti knjigu na stranice, staviti određeni broj stranica u svaku kuvertu i poslati na adresu primatelja. Primatelj odrađuje suprotan proces, otvara omotnice i koristeći se brojevima na stranicama sastavlja knjigu koja bi u konačnici trebala biti čitljiva. Jednako tako, slanje nezaštićene poruke možemo povezati i sa slanjem razglednice, pri čemu bilo tko može pročitati što je na njoj napisano.

Upravo zbog toga moramo paziti na koji način šaljemo naše informacije odnosno osobne i druge povjerljive podatke. Kako većinu podataka šaljemo ili putem elektroničke pošte, ili kroz web-obrasce, takvu bi komunikaciju trebalo šifrirati odnosno kriptirati. Trebalo bi je, drugim riječima, učiniti nečitljivim u prijenosu od našeg računala do ciljanog primatelja i obratno.

Zaštita bežičnih mreža

Kod bežičnih je računalnih mreža osnovno uvođenje autentikacije isključivo zato da bi se onemogućio neovlašteni pristup. Potrebno je i koristiti se protokolima s većom razinom šifriranja podataka. Za sve navedeno odgovorna je osoba zadužena za održavanje mreže. Danas razlikujemo nekoliko vrsta autentikacije, i to: **otvorenu autentikaciju** te **autentikaciju dijeljenim ključem.** Autentikaciju prepoznajemo po unosu „ključa“ pri spajanju na mrežu.

Povezivanje na zaštićenu/nezaštićenu bežičnu mrežu

Ako posjedujemo prijenosno računalo ili računalo s ugrađenom karticom za bežično povezivanje, treba kliknuti na odjeljak **Povezivanje** u dijelu područja obavijesti, pri čemu je na popisu dostupnih mreža potrebno odabrati onu na koju se želimo spojiti, a zatim kliknuti na „**Poveži“**. Kod povezivanja na bežične mreže uglavnom je potrebno unijeti mrežni sigurnosni ključ ili pristupni izraz.

Često se kod spajanja na bežične računalne mreže može vidjeti obavijest o tome da se spajamo na nezaštićenu bežičnu mrežu, što često može biti na različitim javnim mjestima (zračne luke, internetski kafići i sl.). Kod takvog spajanja moramo biti svjesni činjenice da je sva naša komunikacija „vidljiva“ i ostalim sudionicima na mreži, uključujući i lozinke kojima se koristimo. **Zbog toga je vrlo bitno, pogotovo na takvim**

mrežama, provjeriti rabimo li u internetskom pregledniku šifriranu vezu (onu koja se koristi https protokolom).

Kod spajanja na nezaštićenu mrežu, osim preferirane komunikacije preko https (zaštićenih) veza, potrebno je provjeriti i postavke vatrozida. Vatrozid mora biti uključen (vidi poglavlje 2., dio Vatrozid).

Uz opisano spajanje na bežičnu mrežu, spajanje na lokalnu mrežu moguće je i žičanim putem, rabeći UTP kabel koji na sebi ima RJ-45 konektore. Na prijenosnom odnosno stolnom računalu potrebno je potražiti mrežni priključak koji se obično nalazi na stražnjoj strani ili postrance.

Slika 27. Mrežni priključak i mrežni kabel, RJ45 (https://noisegate.com.au/wp-content/uploads/2017/03/ethernet-cable-and-laptop-300x194.jpg, 1.7.2018.)

Ovakav način spajanja smatramo pouzdanijim jer je manja opasnost da će neautorizirani korisnici odnosno napadači presretati promet.

Zaključak

Uporaba računala postala je neizostavni dio nastavnog procesa. Poput drugih tehnologija, računala traže potreban skup vještina koje moramo savladati, a podrazumijevaju i probleme koje za uspješnu uporabu moramo naučiti riješiti.

Ovaj priručnik daje pregled osnovnih hardverskih problema te naputke o tome kako ih riješiti. Naglasimo još jednom važnost kontaktiranja stručnih osoba pri rješavanju hardverskih problema. Kako je računalo uređaj koji se za svoj rad koristi električnom energijom, valja ponajprije slijediti sve općenite smjernice za korištenje uređajima pod naponom. Hardverski problemi koje možemo sami rješavati uglavnom su vezani za periferiju (tipkovnica, miš, monitor i projektor) te instalaciju odgovarajućih upravljačkih programa.

Budući da nema potpune zaštite od štetnih programa ili zlonamjernih osoba, bitno je naglasiti da se moguća šteta u većini slučajeva može spriječiti. Podizanje svijesti o opasnostima na internetu uz preventivnu će zaštitu korištenje internetom učiniti mnogo sigurnijim. Korištenje antivirusnim programima, redovito ažuriranje operativnog sustava, kao i uporaba vatrozida neki su od osnovnih postupaka kojih se valja pridržavati.

Govoreći o poboljšanju procesa i razmjene informacija dotakli smo se sustava Office 365 te SharePoint Wikipedije, kao i OneDrivea u kontekstu zaštite podataka odnosno digitalnog sadržaja. Napomenimo da je redovita sigurnosna pohrana podataka najbolji način čuvanja digitalnog sadržaja od gubitka zbog kvara sastavnica računala te od gubitka podataka uzrokovanoga štetnim softverom.

Pri povezivanju računala na mrežu moramo biti svjesni rizika koje donosi razmjena podataka. Kod prijenosa podataka valja se, kad god je to moguće, koristiti kriptiranim vezama te uvijek pratiti osnovne smjernice povezane sa sigurnom uporabom interneta. Kod većine je računalnih problema upravo sprečavanje najbolji lijek. Razumijevanje rizika koji su predstavljeni u priručniku doprinosi njihovom minimiziranju i sigurnom korištenju tehnologije koja nam je na raspolaganju u suvremenom svijetu.

Europska unija
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
UČINKOVITI LJUDSKI POTENCIJALI
Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.
Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Popis literature

Car, D. (2015). *Građa računala*. Zagreb: Algebra d.o.o.

Car, D. (2018). *Office 365 poslovno korištenje*. Zagreb: Algebra d.o.o.

Car, D. i Kralj, L. (2016). *Office 365*. Hrvatska akademska i istraživačka mreža – CARNET.

Car, D. i Medić, G. (2017). *Administracija klijentskog operacijskog sustava Windows*. Zagreb: Algebra d.o.o.

Car, D. i Medić, G. (2017). *Administracija Windows servera i mrežne infrastrukture*. Zagreb: Algebra d.o.o.

Gollman, D. (2011). *Computer Security* (3. izd.). John Wiley & Sons.

Pipkin, D. L. (2000). *Information Security.* Prentice Hall PTR.

Ribarić, S. (2011). *Građa računala*. Zagreb: Visoko učilište Algebra.

Impressum

Nakladnik: Hrvatska akademska i istraživačka mreža – CARNET

Projekt: „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot-projekt)“

Urednik: izv. prof. dr. sc. Davor Horvatić

Autor: izv. prof. dr. sc. Davor Horvatić, Dario Car, prof.

Lektorica: Dijana Stilinović, prof.

Recenzent: prof. dr. sc. Dragan Peraković

Priprema, prijelom: Algebra

Zagreb, srpanj 2018.

Kontakt

Hrvatska akademska i istraživačka mreža – CARNET

Josipa Marohnića 5, 10000 Zagreb

tel.: +385 1 6661 555

www.carnet.hr

Više informacija o EU fondovima možete pronaći na mrežnim stranicama Ministarstva regionalnoga razvoja i fondova Europske unije: www.strukturnifondovi.hr

Ovaj priručnik izrađen je s ciljem podizanja digitalne kompetencije korisnika u sklopu projekta e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot-projekt), koji sufinancira Europska unija iz europskih strukturnih i investicijskih fondova. Nositelj projekta je Hrvatska akademska i istraživačka mreža – CARNET.