

# "Informacija o Digitalnoj i Sajber akademiji - obrazovanje za digitalnu budućnost"

*Podgorica, decembar 2024.*

## Digitalna akademija

Iako proces digitalne transformacije mora pratiti tempo razvoja digitalnih tehnologija, za postizanje uspjeha u tom procesu potrebna je čvrsta osnova u nekoliko ključnih oblasti. Prije svega, to podrazumijeva unaprijeđenu infrastrukturu, jasno normativno i institucionalno uređenje, efikasno upravljanje i dostupnost podataka, kvalitetne obrazovne programe za sticanje digitalnih vještina, te saradnju sa privatnim sektorom. Takođe, potrebni su podsticaji kako bi se digitalna rješenja što efikasnije koristila.

Evropska komisija definiše digitalnu kompetenciju kao samopouzdanu, kritičku i odgovornu upotrebu digitalnih tehnologija u različitim kontekstima, kao što su učenje, rad i društveno angažovanje. To obuhvata digitalnu pismenost, sposobnost komunikacije i saradnje, kreiranje digitalnih sadržaja, sigurnost u digitalnom okruženju i rješavanje problema. Kako tehnologija napreduje, postaje očigledno da je neophodno kontinuirano usavršavanje ovih vještina.

Digitalne vještine postaju ključno sredstvo, ne samo za zaposlene, već i za nezaposlene osobe koje žele aktivno učestvovati na tržištu rada. Ove vještine su neophodne u gotovo svim oblastima, od osnovnih radnih pozicija do rukovodećih uloga. Kako radna okruženja postaju sve složenija i međusobno povezana, nivo i vrsta digitalnih vještina postaju odlučujući faktor za zapošljavanje i konkurentnost na tržištu rada. U savremenom dobu, digitalna transformacija djeluje kao pokretač inovacija, modernizacije i ekonomskog rasta. Ključni preduslovi za uspjeh ove transformacije uključuju poboljšanje IKT infrastrukture, razvoj i jačanje digitalnih vještina, podizanje svijesti građana i privrede o značaju digitalizacije, te poboljšanje kvaliteta i dostupnosti e-usluga.

Vlada Crne Gore je prepoznala digitalnu transformaciju kao jedan od pet glavnih prioriteta u Srednjoročnom programu rada 2022-2024. Ovaj plan, sa posebnim fokusom na 2023. godinu, naglašava razvoj digitalnog društva temeljenog na optimizovanim procesima i uslugama koje odgovaraju potrebama građana, privrede i javne administracije. U okviru ovih napora, poseban akcenat stavljen je na jačanje digitalnih vještina, što je od presudnog značaja za prevazilaženje digitalnog jaza u društvu.

Iako je omogućen pristup informaciono-komunikacionim tehnologijama važan korak ka stvaranju jednakih prilika za sve građane, sam pristup nije dovoljan. Potrebno je raditi na edukaciji i podizanju svijesti o mogućnostima koje digitalne tehnologije nude, kako bi se u potpunosti iskoristili njihovi benefiti u svakodnevnom životu.

Ministarstvo javne uprave pokrenulo je inicijativu uspostavljanja Digitalne akademije, online platforme namijenjene edukaciji i povezivanju svih ključnih aktera u procesu razvoja digitalnih i liderskih vještina. Digitalna akademija je usmjerena na javne službenike, studente i ranjive grupe, s ciljem brzog unapređenja njihovih kapaciteta za digitalnu transformaciju Crne Gore. Kroz ove programe, Akademija ima za cilj jačanje digitalne svijesti, kapaciteta i konkurentnosti crnogorskog društva, kao i razvoj ICT sektora.

## Vizija i misija

**Vizija:** Osnaživanje građana i građanki u domenu digitalnih kompetencija i vještina u cilju izgradnje naprednog društva naslonjenog na digitalne tehnologije.

**Misija:** Pružiti edukaciju i unaprijediti vještine državnih službenika i građana, podstičući efikasnu, profesionalnu i građanski orijentisanu javnu upravu.

## Ciljevi Digitalne akademije

Krajnji cilj je stvaranje sistemskog i kontinuiranog procesa stručnog osposobljavanja i usavršavanja ciljnih grupa u domenu digitalnih i njima komplementarnih vještina, radi održivosti i kontinuiranog unapređenja digitalizacije javne uprave i digitalne transformacije crnogorskog društva.

### Opšti ciljevi:

- Ojačati građane i građanke digitalnim vještinama za digitalno društvo
- Unaprijediti kapacitete transformacionog liderstva za pokretanje promjena
- Podsticati agilno upravljanje i principe usmjerene na čovjeka

### Specifični ciljevi:

- Razvijati prilagođene kurseve usklađene sa digitalnim potrebama
- Omogućiti praktičnu primjenu stečenog znanja
- Izgraditi zajednicu za saradnju učenja za kontinuirano unapređenje

## Dizajn programa obuka - kurikuluma

Na web portalu GOV.ME kreirana je posebna stranica za Digitalnu akademiju, koja pruža informacije o konceptu online platforme, dostupnim obukama i njihovim sadržajima. Prvi programi obuke, na koje su se ciljne grupe mogle prijaviti, obuhvatali su teme poput transformativnog liderstva i upravljanja promjenama, dizajna usmjerenog na čovjeka (Human-Centered Design) i sajber bezbjednosti sa fokusom na zaštitu podataka.

Stranica Akademije omogućava zainteresovanim budućim polaznicima da se prijave za dostupne module i izraze interesovanje za kurseve koji su im potrebni za prilagođavanje promjenama u digitalnom okruženju. Takođe, postoji obrazac za prijavu predavača koji žele da učestvuju u kreiranju novih programa i daju svoj doprinos zajednici.

U aprilu 2024. godine sprovedeno je anketno istraživanje među državnim službenicima, građanima i ranijim polaznicima Akademije kako bi se identifikovale potrebe za jačanjem kapaciteta. Nakon pregleda rezultata ankete, izdvojile su sljedeće teme:

1. Bezbjednosna kultura i sigurnosne prijetnje, uključujući upotrebu vještačke inteligencije
2. Obuke za korišćenje Excel-a i AutoCAD-a
3. Obrada podataka i način razmjene tih podataka

4. Interna i eksterna komunikacija, sa ciljem efikasnijeg prikupljanja podataka
5. Primjeri najbolje prakse u digitalnoj transformaciji poslovnih procesa unutar državne uprave i lokalne samouprave
6. Sertifikovani kursevi vezani za informacione tehnologije, kao što su Ethical Hacking, administracija Linux i Windows servera, te konfiguracija rutera
7. Obuke za digitalni marketing
8. Obuke o upravljanju stresom
9. Vještine javnog govora i komunikacije sa medijima
10. Edukacije tehničkih i praktičnih vještina, uključujući istraživanje, donošenje zaključaka i odluka

Zaključci ankete ističu potrebu za prilagođavanjem određenih tema za populaciju sa nižim nivoom digitalnih vještina, kao i važnost uključivanja stručnjaka izvan javnog sektora, kako bi se obuke obogatile konkretnim i korisnim primjerima iz prakse.

U toku 2024. godine uspješno su realizovane dvije edukacije i to jedna u obliku meetup događaja, a druga u obliku predavanja za učenike srednje škole. U pitanju su: ChatGPT - primjene, izazovi i etička pitanja i Budućnost digitalizacije: primjena vještačke inteligencije i mašinskog učenja.

Meetup "**ChatGPT - primjene, izazovi i etička pitanja**" održan je **18. juna 2024. godine** s ciljem edukacije državnih službenika i građana o osnovama korišćenja ChatGPT-a, izazovima i etici primjene ove tehnologije. Učesnici su se upoznali s generativnom vještačkom inteligencijom, načinima rada velikih jezičkih modela i značajem podataka u njihovom razvoju. Eksperti Nikola Bulatović i Goran Paštović su kroz predavanja predstavili praktične primjene ChatGPT-a u različitim industrijama i diskutovali o izazovima etičkog korišćenja. Fokus je bio na koristima koje generativna vještačka inteligencija može donijeti u poslovnim procesima, ali i na odgovornosti koja ide uz njen razvoj i primjenu. Meetup je okupio 43 učesnika i pružio im bolje razumijevanje potencijala ove tehnologije.

Trening "**Budućnost digitalizacije: Primjena vještačke inteligencije i mašinskog učenja**" održan je **3. oktobra 2024. godine** u Podgoričkoj Gimnaziji, s ciljem upoznavanja učenika sa osnovama vještačke inteligencije i mašinskog učenja. Predavanje je vodio Nikola Bulatović, stručnjak u ovoj oblasti, sa bogatim iskustvom u istraživanju i obrazovanju, koji je kroz primjere iz prakse objasnio ključne koncepte. Oko 160 učenika prisustvovalo je treningu, koji je bio interaktivan, sa prostorom za diskusiju i postavljanje pitanja. Ovaj događaj je pružio učenicima uvod u primjenu naprednih tehnologija u različitim sektorima.

U narednoj godini planirana je realizacija edukacija u skladu s identifikovanim potrebama iz ankete, čime će se nastaviti kontinuirani rad na jačanju kapaciteta i unapređenju znanja i vještina.

## Sajber akademija

Paralelno sa razvojem Digitalne akademije, razvijali smo i Sajber akademiju kako bismo ih početkom 2025. godine integrisali u jednu platformu pod nazivom: **eAkademija**. Sajber akademija je ključna za sve državne službenike i namještenike, kao i građane, jer omogućava podizanje svijesti o sajber higijeni i pruža neophodne alate za prepoznavanje i prevenciju sajber prijetnji. S obzirom na sve češće sajber napade i kompleksnost digitalnog okruženja Sajber akademija ima za cilj da osnaži korisnike u zaštiti svojih digitalnih resursa i podataka.

Pored edukacije Sajber akademija će podstaći razvoj sajber otpornosti na nivou pojedinca, institucija i društva u cjelini. Time doprinosimo ne samo unapređenju sajber bezbjednosti u javnom sektoru, već i stvaranju svjesnijeg i sigurnijeg digitalnog društva.

**eAkademija će biti centralna tačka za sticanje ključnih znanja i vještina koje su neophodne za suočavanje sa izazovima modernog digitalnog doba.**

## Vizija i misija

**Vizija:** Postizanje visokog nivoa svijesti o sajber higijeni i bezbjednosti među državnim službenicima, namještenicima i građanima, uz kontinuiranu edukaciju i osposobljavanje, s ciljem izgradnje otpornog i sigurnog digitalnog društva.

**Misija:** Pružiti sveobuhvatan pristup edukativnim sadržajima iz oblasti sajber bezbjednosti, sa posebnim naglaskom na praktičnu primjenu stečenih teorijskih znanja, kako bi se unaprijedile vještine i podigla svijest o značaju sajber higijene i bezbjednosti u savremenom digitalnom okruženju.

## Cilj Sajber akademije

U današnjem vremenu ubrzanog tehnološkog razvoja, digitalne tehnologije prožimaju gotovo sve aspekte našeg života i rada. Međutim, ovaj napredak prate i sve učestaliji pokušaji zloupotrebe, koji predstavljaju ozbiljnu prijetnju kako javnom, tako i privatnom sektoru. Zbog toga je kontinuirana edukacija ključna - ne samo za državne službenike i namještenike, već i za sve građane. Cilj je osnažiti ih znanjem i vještinama potrebnim za prepoznavanje i sprečavanje sajber prijetnji, čime se doprinosi bezbjednijem i otpornijem društvu koje može efikasno odgovoriti na izazove savremenog digitalnog doba.

### Opšti ciljevi:

- Ojačati ljudsku kariku u lancu sajber bezbjednosti kroz edukaciju i osposobljavanje državnih službenika, namještenika i građana.
- Osigurati kontinuirano podizanje svijesti o sajber higijeni i odgovornom ponašanju u digitalnom okruženju.
- Povećati otpornost pojedinaca i institucija na sajber prijetnje kroz praktičnu primjenu stečenih znanja i vještina.

### Specifični ciljevi:

- Razviti i implementirati kurseve iz oblasti sajber bezbjednosti na e-learning platformi, omogućavajući korisnicima sticanje znanja o zaštiti digitalnih resursa i podataka.
- Podizati svijest o sajber prijetnjama i higijeni kroz praktične savjete za prepoznavanje i izbjegavanje sajber rizika, čime se osigurava odgovorno ponašanje u digitalnom okruženju.
- Osigurati integraciju edukacije o sajber bezbjednosti sa zakonskim i podzakonskim aktima, omogućavajući korisnicima efikasnije razumijevanje pravnog okvira informacione bezbjednosti.
- Povezati edukatore sa polaznicima kurseva putem interaktivne platforme, čime se podstiče razmjena znanja i iskustava među stručnjacima, državnim službenicima i građanima.
- Jačati otpornost pojedinaca i institucija na sajber prijetnje kroz obuku koja kombinuje teorijska znanja i praktične primjere.
- Unaprijediti sajber bezbjednost u javnom sektoru kroz ciljanu edukaciju državnih službenika i namještenika, smanjujući rizik od sajber napada na ključne institucije.

## Osnovni kurs Sajber bezbjednosti - ključ za sigurnost u digitalnom okruženju

U savremenom digitalnom svijetu, sajber prijetnje postaju sve sofisticiranije, a korisnici interneta sve ranjiviji. U tom kontekstu, edukacija o sajber bezbjednosti dobija na značaju, posebno među državnim službenicima i namještenicima, ali i građanima, koji su svakodnevno izloženi potencijalnim napadima i prevarama. Osnovni kurs sajber bezbjednosti na ovoj platformi pruža temeljno razumijevanje ključnih koncepata i tehnika zaštite u digitalnom prostoru, s ciljem da polaznicima omogući prepoznavanje i reagovanje na sajber prijetnje, kao i implementaciju sigurnosnih praksi u svom svakodnevnom digitalnom ponašanju.

### • **Tematske jedinice kursa**

Kurs je dizajniran da obuhvati širok spektar tema koje su ključne za sajber zaštitu u svakodnevnom životu i radu. Počinje sa osnovama zaštite od phishing napada, gdje polaznici uče kako da prepoznaju pokušaje prevare putem elektronske pošte ili drugih komunikacijskih kanala. Zatim, kurs pokriva sigurnost prenosivih medija, kao što su USB uređaji, koji često služe kao vektori za sajber napade. Učenje o lozinkama i autentifikaciji je još jedna ključna tema, jer polaznici stiču znanje o tome kako da kreiraju i upravljaju snažnim lozinkama i koriste višefaktorsku autentifikaciju kao metod zaštite.

Fizička sigurnost je takođe, neizostavna tema, jer zaštita hardvera i kontrola fizičkog pristupa informacijama mogu biti ključni za sprečavanje potencijalnih napada. Bezbjednost mobilnih uređaja, kao i rad na daljinu, temeljno se obrađuju, jer rad sa pametnim telefonima i rad na daljinu postaju sve češći, a sa njima dolaze i novi rizici za sigurnost podataka i uređaja.

Jedna od ključnih tačaka kursa je i edukacija o sigurnosti javnih Wi-Fi mreža, kao i sigurnosti podataka u Cloud-u. Kurs takođe, obuhvata odgovorno ponašanje na društvenim mrežama, jer je dijeljenje ličnih informacija na ovim platformama potencijalni izvor za sajber napadače. Korišćenje

interneta i elektronske pošte, sigurnost kod kuće, kao i prepoznavanje socijalnog inženjeringa, takođe su obuhvaćeni temama, jer svi ovi faktori igraju značajnu ulogu u sveobuhvatnoj zaštiti.



- **Metodologija praćenja i motivacija**

Kurs je dizajniran tako da polaznici napreduju kroz module postepeno, s obavezom da uspješno završe prethodne lekcije i polože kriterijumske kvizove, prije nego što nastave dalje. Ovaj pristup omogućava temeljno usvajanje gradiva i testiranje znanja na svakom koraku. Kada završe kurs, polaznici dobijaju sertifikat, što predstavlja priznanje za uspješno savladan materijal, ali i medalju (bronzna, srebro, zlato) koja je nagrada za uspeh u savladavanju kursa. Ovaj sistem nagrađivanja dodatno podstiče motivaciju i takmičarski duh među praktikantima, čineći proces učenja dinamičnijim i angažovanijim.

- **Dugoročni značaj kursa**

Osnovni kurs sajber bezbjednosti nije samo kratkoročna edukacija, već ima dugoročni značaj u oblikovanju sigurnijeg i otpornijeg digitalnog društva. Kroz temeljnu obuku, polaznici stiču neophodne vještine i razvijaju svijest o značaju ljudskog faktora u sajber zaštiti, što predstavlja ključnu komponentu Strategije sajber bezbjednosti i izgradnju sigurnijeg digitalnog okruženja. Kurs obuhvata ključne oblasti poput zaštite od phishing napada, bezbjednosti mobilnih uređaja, rada na daljinu i odgovornog ponašanja na društvenim mrežama.

Posebno se ističe uvod u sajber higijenu kao esencijalan dio kursa, jer omogućava polaznicima razumijevanje uloge ljudskog faktora u lancu sajber zaštite. Kroz praktične module, polaznici uče kako prepoznati sajber prijetnje, primjenjivati najbolje internet prakse i bezbjedno postupati sa osjetljivim informacijama i uređajima. S obzirom na sve veći broj zaposlenih koji rade na daljinu, edukacija o zaštiti podataka i odgovornom ponašanju postaje sve važnija, posebno u kontekstu sprječavanja kompromitovanja poslovnih i ličnih informacija. Kurs takođe, obuhvata savjete o savjesnom korišćenju društvenih mreža, koje često predstavljaju potencijalni izvor informacija za napadače.

Kroz inovativne metode kao što su gamifikovani moduli i sertifikacije, kurs ne samo da motiviše polaznike da usvoje najsavremenije sigurnosne prakse, već i podstiče promjenu ponašanja koja doprinosi stvaranju zajednice otpornije na sajber prijetnje. Sajber akademija na ovaj način pruža savremen i strateški pristup edukaciji, omogućavajući korisnicima da se razviju u odgovorne i bezbjedne članove digitalnog društva, čime se dugoročno doprinosi jačanju kolektivne otpornosti na sve vrste digitalnih napada.