

Livrabil 02 – Agenda instruirii

Răzvan Rughiniș

Universitatea Națională de Știință și Tehnologie

POLITEHNICA București

razvan.rughinis@upb.ro

În urma analizei competențelor ce necesită aprofundarea în cele două planuri de învățământ, pentru Știința Datelor și Securitate Informațională, următoarele teme sunt propuse ca agendă a instruirii.

Figura 1. Structura curriculumului propus

Argumente bazate pe dovezi: analiza datelor în societate

- Coincidențe, corelații și cauzalitate
- Măsurarea fenomenelor și erori de măsurare
- Eșantionarea și modelarea; erori specifice
- Extragerea informației prin tehnici de analiză a datelor

Datele masive în societate

- Dimensiunea economică: datele și piața liberă, modele de afaceri
- Dimensiunea psihologică și sociologică

Confidențialitatea și securitatea datelor

- Decidenți: Modele de reglementare în EU, SUA și China
- Experți și utilizatori: Strategii de asigurare a confidențialității

AI și securitatea cibernetică

- Provocările AI pentru securitatea cibernetică
- Atacurile specifice modelelor ML / AI

Opțional - Teme aprofundate

- Blockchain și aplicațiile sale
- Securizarea Internetului Lucrurilor (IoT)

Argumente bazate pe dovezi: analiza datelor în societate

Subiecte:

- Coincidențe, corelații și cauzalitate
- Măsurarea fenomenelor și erori de măsurare
- Eșantionarea și modelarea; erori specifice
- Extragerea informației prin tehnici de analiză a datelor

Aceste subiecte vor consolida înțelegerea de către studenți a analizei bazate pe dovezi, acoperind aspecte cruciale precum cauzalitatea, erorile de măsurare și eșantionarea. Ele abordează în mod direct competențele parțial acoperite din Analiza exploratorie a datelor (EDA) și Înțelegerea datelor, oferind o perspectivă mai profundă asupra tehnicilor de analiză a datelor și a gestionării erorilor.

Date masive în societate

Subiecte:

- Dimensiunea economică a datelor masive; datele și piața liberă; modele de afaceri
- Dimensiunea psihologică și sociologică a datelor masive

Acoperirea dimensiunilor economice, psihologice și sociologice ale datelor masive va îmbunătăți competențele analitice și specifice domeniului ale studenților, în special în ceea ce privește înțelegerea datelor și aplicarea științei datelor. Aceasta oferă un context mai larg asupra modului în care datele au un impact asupra diferitelor aspecte ale societății, pregătind studenții să ia în considerare aceste efecte în activitatea lor.

Confidențialitate și securitate în fluxurile informaționale

Subiecte:

- Modele de reglementare a confidențialității datelor masive: UE, SUA și China
- Strategii de asigurare a confidențialității datelor ca expert și utilizator

Acest curs va acoperi lacunele în competențele privind confidențialitatea și securitatea cibernetică, oferind o înțelegere cuprinzătoare a reglementărilor privind confidențialitatea datelor și strategii practice pentru confidențialitatea datelor. Acesta susține în mod direct competențele din domeniul Etică și confidențialitate, punând accentul pe modelele de reglementare și tehnicile de asigurare a confidențialității.

IA și securitatea cibernetică

Subiecte:

- Provocările AI pentru securitatea cibernetică
- Atacuri specifice modelelor de AI

Abordarea provocărilor pe care AI le ridică pentru securitatea cibernetică va spori competențele studenților atât în ceea ce privește provocările AI, cât și în ceea ce privește confidențialitatea și securitatea cibernetică. Acest subiect asigură faptul că studenții sunt conștienți și pregătiți să abordeze riscurile de securitate asociate cu tehnologiile IA, completând cunoștințele lor existente în domeniul învățării automate și al IA.

Opțional – Teme aprofundate

Subiecte:

- Blockchain și aplicațiile sale
- Securizarea Internetului Lucrurilor (IoT)

Cursul de blockchain le permite studenților să înțeleagă și să implementeze tehnologii de registre distribuite, care sunt fundamentale pentru securitatea și integritatea tranzacțiilor digitale, contribuind astfel la dezvoltarea de soluții sigure pentru diverse aplicații, inclusiv criptomonede și contracte inteligente. Cursul de securizare a IoT pregătește studenții să abordeze provocările unice ale securității dispozitivelor conectate, asigurând protecția datelor și a infrastructurilor critice într-un mediu în continuă expansiune, caracterizat printr-o multitudine de dispozitive interconectate și vulnerabilități specifice. Aceste cursuri echipează studenții cu competențe avansate necesare pentru a proteja și inova în sectoarele emergente ale tehnologiei.

Tabelul 1. Repartizarea pe grupuri și ore a tematicilor propuse

Tematică	Subiecte	Număr ore Grupul 1	Număr ore Grupul 2
Argumente bazate pe dovezi: analiza datelor în societate	Coincidențe, corelații și cauzalitate		
	Măsurarea fenomenelor și erori de măsurare		
	Eșantionarea și modelarea; erori specifice		
	Extragerea informației prin tehnici de analiză a datelor		
Datele masive în societate	Dimensiunea economică a datelor masive; datele și piața liberă; modele de afaceri;		
	Dimensiunea psihologică și sociologică a datelor masive		
Confidențialitatea și securitatea datelor	Rolul de decident: Modele de reglementare a confidențialității datelor masive: EU, SUA și China		
	Rolul de expert și utilizator: Strategii de asigurare a confidențialității datelor		
AI și securitatea cibernetică	Provocările AI pentru securitatea cibernetică Atacuri specifice modelelor ML / AI		
Opțional – Teme aprofundate	Blockchain și aplicațiile sale		
	Securizarea Internetului Lucrurilor (IoT)		