ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

ΘΕΜΑΤΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΔΙΠΛΩΜΑΤΙΚΩΝ ΕΡΓΑΣΙΩΝ

Ακαδημαϊκό έτος 2025-2026

Επιβλέπων: Καθηγητής Στέφανος Γκρίτζαλης

Α/Α	**Θέμα Μεταπτυχιακής Διπλωματικής Εργασίας**	**Σύντομη Περιγραφή**
1.	Ασφάλεια και Ιδιωτικότητα σε Μεγάλα Γλωσσικά Μοντέλα (Security and Privacy in Large Language Models)	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
2.	Ασφάλεια και Ιδιωτικότητα στην Ομοσπονδιακή Μάθηση (Security and Privacy in Federated Learning)	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
3.	Ασφάλεια και Ιδιωτικότητα στην Αυτενεργούσα Τεχνητή Νοημοσύνη: Κίνδυνοι και Μέτρα Μετριασμού Κινδύνων (Security and Privacy in Agentic Artificial Intelligence: Risks and Mitigation Controls)	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
4.	Ασφάλεια και Ιδιωτικότητα στις Επιφυείς Υπηρεσίες (Security and Privacy in Over-The-Top Services)	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
5.	Ασφάλεια και Ιδιωτικότητα και Ηχητικοί Βοηθοί (Voice Assistants): Τεχνικά, Ηθικά και Νομικά Ζητήματα	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
6.	Τεχνολογίες Κατασκοπευτικού Λογισμικού (Spyware Technologies)	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)

7.	Ιδιωτικότητα και Νεφοϋπολογιστική (Privacy and Cloud Computing): Συγκριτική Ανάλυση Amazon Web Services, Microsoft Azure, Google Cloud Platform	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
8.	Ιδιωτικότητα και Πλατφόρμες Τηλεδιασκέψεων (Privacy and Teleconference Platforms): Συγκριτική Ανάλυση Cisco WebEx, Zoom, Microsoft Teams, Google Meet	Τεχνολογική επισκόπηση και ερευνητικά ζητήματα (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
9.	Διοίκηση Κινδύνων Ασφάλειας στην Εφοδιαστική Αλυσίδα την Εποχή της Τεχνητής Νοημοσύνης (Supply Chain Security Risk Management in the Artificial Intelligence Era)	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
10.	Διοίκηση Επιχειρησιακής Συνέχειας (Business Continuity Management) Επιχειρήσεων και Οργανισμών	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
11.	Πλαίσιο Εφαρμογής, Ελέγχων (Auditing) και Συμμόρφωσης (Compliance) του Κανονισμού DORA 2022/2554	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
12.	Πλαίσιο Εφαρμογής, Ελέγχων (Auditing) και Συμμόρφωσης (Compliance) της Directive NIS2 2022/2555 και του Ν. 5160/2024	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
13.	Μεθοδολογίες Εκτίμησης Αντικτύπου για την Προστασία Δεδομένων κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων (Data Protection Impact Assessment – GDPR) και Εκτίμησης Αντικτύπου στα Θεμελιώδη Δικαιώματα κατά την Πράξη για την Τεχνητή Νοημοσύνη (Fundamental Rights Impact Assessment – AI Act)	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)
14.	Κανονιστικό Πλαίσιο Κυβερνοασφάλειας (Cybersecurity Regulation Framework): Ευρωπαϊκή Ένωση, ΗΠΑ, Κίνα	Τεχνολογική επισκόπηση και μεθοδολογικό και οργανωτικό πλαίσιο εφαρμογής (προς περαιτέρω εξειδίκευση μετά από συνεργασία)