

**Πανεπιστήμιο
Πειραιώς**



**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ
ΣΠΟΥΔΩΝ «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ
ΚΑΙ ΕΠΙΣΤΗΜΗ ΔΕΔΟΜΕΝΩΝ»**



ΣΧΟΛΗ

**ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ**

<https://cybersecdatasci.cs.unipi.gr/>

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



ΟΔΗΓΟΣ ΣΠΟΥΔΩΝ 2025 – 2026





Πειραιάς, Οκτώβριος, 2025

Περιεχόμενα

1.	ΚΑΛΩΣΟΡΙΣΜΑ ΤΟΥ ΔΙΕΥΘΥΝΤΗ.....	5
2.	ΟΡΓΑΝΑ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ.....	6
3.	ΟΡΓΑΝΑ ΤΗΣ ΣΧΟΛΗΣ.....	6
4.	ΟΡΓΑΝΑ ΤΟΥ ΤΜΗΜΑΤΟΣ.....	6
5.	ΟΡΓΑΝΑ ΤΟΥ ΠΜΣ.....	6
6.	ΔΙΔΑΚΤΙΚΟ ΠΡΟΣΩΠΙΚΟ ΤΟΥ Π.Μ.Σ.....	6
7.	ΕΡΕΥΝΗΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ.....	10
8.	ΥΛΙΚΟΤΕΧΝΙΚΗ ΥΠΟΔΟΜΗ.....	11
9.	ΠΑΡΟΧΕΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΙΔΡΥΜΑΤΙΚΟΣ ΛΟΓΑΡΙΑΣΜΟΣ.....	13
1)	ΙΔΡΥΜΑΤΙΚΟΣ ΛΟΓΑΡΙΑΣΜΟΣ.....	13
2)	ΑΚΑΔΗΜΑΪΚΗ ΤΑΥΤΟΤΗΤΑ, ΦΟΙΤΗΤΙΚΟ ΕΙΣΙΤΗΡΙΟ.....	13
3)	ΗΛΕΚΤΡΟΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ.....	13
4)	ΕΦΑΡΜΟΓΗ ΦΟΙΤΗΤΙΚΗΣ ΜΕΡΙΜΝΑΣ.....	14
5)	ΥΠΗΡΕΣΙΑ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ – VPN.....	14
6)	ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ – WIFI.....	14
7)	ΔΙΑΘΕΣΗ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΗ ΧΡΗΣΗ.....	15
8)	ΗΛΕΚΤΡΟΝΙΚΗ, ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΕΚΠΑΙΔΕΥΣΗ (E-LEARNING).....	15
9)	ΒΙΒΛΙΟΘΗΚΗ.....	15
10.	ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΠΜΣ.....	16
1)	ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΚΟΠΟΣ ΤΟΥ ΠΜΣ.....	17
2)	ΓΙΑΤΙ ΝΑ ΑΚΟΛΟΥΘΗΣΕΤΕ ΑΥΤΟ ΤΟ ΠΡΟΓΡΑΜΜΑ – ΕΥΚΑΙΡΙΕΣ ΕΡΓΑΣΙΑΣ.....	17
3)	ΚΑΤΗΓΟΡΙΕΣ ΕΙΣΑΚΤΕΩΝ.....	19
4)	ΚΡΙΤΗΡΙΑ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΛΟΓΗΣ ΥΠΟΨΗΦΙΩΝ ΓΙΑ ΤΟ ΠΜΣ.....	19
5)	ΔΙΑΡΚΕΙΑ ΣΠΟΥΔΩΝ – ΟΡΟΙ ΦΟΙΤΗΣΗΣ.....	21
6)	ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΠΟΥΔΩΝ.....	21
7)	ΕΠΙΣΤΗΜΟΝΙΚΟΙ ΣΤΟΧΟΙ.....	26
11.	ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΩΝ ΑΝΑ ΕΙΔΙΚΕΥΣΗ ΚΑΙ ΕΞΑΜΗΝΟ.....	27
1)	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΑΠΕΣ).....	27
2)	ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΕΝΣΩΜΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΑΑΕΣ).....	33

3)	ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΑΝΑΛΥΤΙΚΗ ΚΑΙ ΑΝΑΛΥΤΙΚΗ ΔΕΔΟΜΕΝΩΝ (ΕΑΑΔ).....	36
12.	ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ.....	40
1)	ΓΕΝΙΚΕΣ ΙΚΑΝΟΤΗΤΕΣ.....	40
2)	ΓΝΩΣΕΙΣ.....	40
3)	ΔΕΞΙΟΤΗΤΕΣ.....	42
4)	ΙΚΑΝΟΤΗΤΕΣ.....	44

1. ΚΑΛΩΣΟΡΙΣΜΑ ΤΟΥ ΔΙΕΥΘΥΝΤΗ

Το Πρόγραμμα Μεταπτυχιακών Σπουδών του Πανεπιστημίου Πειραιώς στην **Κυβερνοασφάλεια και Επιστήμη Δεδομένων** διανύει το πέμπτο ακαδημαϊκό έτος. Μετά από μια επιτυχημένη εκκίνηση κατά το ακαδημαϊκό έτος 2021-2022, είμαστε υπερήφανοι για την εγγραφή φοιτητών υψηλής ποιότητας και στόχευσης, καθώς και για την παροχή ενός υπερσύγχρονου ακαδημαϊκού προγράμματος, που βασίζεται στη συγχώνευση δύο τομέων αιχμής της επιστήμης της πληροφορικής.

Ως Διευθυντής του ΠΜΣ για το ακαδημαϊκό έτος 2025-2026, το όραμά μου είναι να διασφαλίσω τη συνεχή βελτίωση του προγράμματός μας, τόσο σε ακαδημαϊκό όσο και σε οργανωτικό επίπεδο. Μαζί με τη Συντονιστική Επιτροπή του ΠΜΣ, είμαστε αφοσιωμένοι στο να διασφαλίσουμε ότι οι εγγεγραμμένοι φοιτητές θα λάβουν επικαιροποιημένη εκπαίδευση, προηγμένες γνώσεις, πρακτικές δεξιότητες και ερευνητική εμπειρία αιχμής στις θεωρητικές γνώσεις, τις τεχνολογίες και τις εφαρμογές της κυβερνοασφάλειας και της επιστήμης των δεδομένων. Λαμβάνοντας υπόψη τις διαρκώς εξελισσόμενες τεχνολογικές και ακαδημαϊκές μεταβολές, καθώς και την ανατροφοδότηση από τους φοιτητές μας, φέτος εφαρμόσαμε μικρής κλίμακας αλλά πολύ στοχευμένες αλλαγές στο πρόγραμμά μας. Στόχος μας ήταν να καλύψουμε πρόσθετες πτυχές της κυβερνοασφάλειας και της επιστήμης των δεδομένων, καθώς και να προσφέρουμε στους φοιτητές μας περισσότερες εναλλακτικές για τα μαθήματα επιλογής. Η ομάδα των διδασκόντων του ΠΜΣ αποτελείται από εξαιρετικά έμπειρους καθηγητές, διεθνώς αναγνωρισμένους στους τομείς της κυβερνοασφάλειας και της επιστήμης των δεδομένων, δημιουργώντας ένα μοναδικό πρόγραμμα.

Κατά το τρέχον ακαδημαϊκό έτος, θα συνεχίσουμε να βελτιώνουμε το πρόγραμμά μας όσον αφορά τη διδασκαλία, την έρευνα, το εργαστήριο και άλλες δραστηριότητες με:

1. Υποστήριξη των μαθημάτων μας (σε επίπεδο εργαστηριακών συνεργατών, υποδομών κ.λπ.) από τα συνεργαζόμενα ερευνητικά εργαστήρια του Πανεπιστημίου Πειραιώς, δηλαδή το Εργαστήριο Κυβερνοασφάλειας, το Εργαστήριο Επιστήμης Δεδομένων, το Εργαστήριο Συστημάτων Υποστήριξης Αποφάσεων, το Εργαστήριο Ενσωματωμένων Συστημάτων και το Εργαστήριο Έρευνας Δικτύων.
2. Επέκταση των ήδη καθιερωμένων συνεργασιών μας με επιτυχημένους παρόχους εκπαιδευτικών πλατφορμών, τόσο στον τομέα της κυβερνοασφάλειας όσο και της επιστήμης των δεδομένων.
3. Επέκταση των ήδη καθιερωμένων συνεργασιών μας με φορείς πιστοποίησης, προκειμένου να παρέχουμε ευκαιρίες στους σπουδαστές μας για συνεχή κατάρτιση και πιστοποίηση.

4. Παροχή ενημέρωσης σε φοιτητές και ερευνητές σε διάφορα στάδια σταδιοδρομίας, επεκτείνοντας τις αλληλεπιδράσεις μας με τις επιχειρήσεις και τη βιομηχανία.

Εξερευνήστε τον οδηγό σπουδών αλλά και των ιστότοπο του ΠΜΣ για να ενημερωθείτε για τα μαθήματα, την έρευνα, τους συνεργαζόμενους εταίρους, τις εκδηλώσεις και άλλα. Είτε είστε υποψήφιος φοιτητής, μέλος της κοινότητας του Πανεπιστημίου Πειραιώς, είτε πιθανός συνεργάτης από τη δημόσια διοίκηση ή τη βιομηχανία, μπορείτε να επικοινωνήσετε μαζί μας με ερωτήσεις ή ιδέες. Ειδικά για τους υποψήφιους φοιτητές: ελπίζουμε ότι το Πρόγραμμα Μεταπτυχιακών Σπουδών στην Κυβερνοασφάλεια και την Επιστήμη Δεδομένων θα αποτελέσει ιδανική επιλογή για τα μελλοντικά σας επαγγελματικά ή ακαδημαϊκά σχέδια. Ανυπομονούμε να συνεργαστούμε μαζί σας για την επίτευξη των στόχων σας!

Καθ. Παναγιώτης Κοτζανικολάου, Διευθυντής ΠΜΣ

2. ΟΡΓΑΝΑ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ

1. Σύγκλητος
2. Πρυτανικό Συμβούλιο
3. Πρύτανης
4. Αντιπρυτάνεις

3. ΟΡΓΑΝΑ ΤΗΣ ΣΧΟΛΗΣ

1. Γενική Συνέλευση Σχολής
2. Κοσμητεία
3. Κοσμήτορας

4. ΟΡΓΑΝΑ ΤΟΥ ΤΜΗΜΑΤΟΣ

1. Συνέλευση του Τμήματος
2. Πρόεδρος Τμήματος

5. ΟΡΓΑΝΑ ΤΟΥ ΠΜΣ

Αρμόδια όργανα για την ίδρυση, οργάνωση και λειτουργία των Π.Μ.Σ. σύμφωνα με το νόμο ν. 4957/2022 είναι:

1. η Σύγκλητος του Ιδρύματος
2. η Συνέλευση του Τμήματος
3. η Συντονιστική Επιτροπή (Σ.Ε.) του Π.Μ.Σ.
4. ο Διευθυντής του Π.Μ.Σ.

Γραμματεία ΠΜΣ Κυβερνοασφάλεια και Επιστήμη Δεδομένων

Διεύθυνση: Γραφείο 503, Κεντρ. κτίριο, Καραολή & Δημητρίου 80, Πειραιάς 18534

Τηλέφωνο: 210 4142105, 210 4142263

E-mail: msc-cds-info@unipi.gr, infodept@unipi.gr

6. ΔΙΔΑΚΤΙΚΟ ΠΡΟΣΩΠΙΚΟ ΤΟΥ Π.Μ.Σ.

Στο ΠΜΣ διδάσκουν κατά κύριο λόγο τα μέλη ΔΕΠ του Τμήματος Πληροφορικής, με αναγνωρισμένη υψηλή γνωστική και ακαδημαϊκή επάρκεια, και συνάφεια με το αντικείμενο του προγράμματος. Τα μέλη ΔΕΠ του Τμήματος που συμμετέχουν στο ΠΜΣ είναι (με αλφαβητική σειρά):

• **Καθηγητής Δημήτρης Αποστόλου** (παραθέσεις: 6394, h-index: 38, i10-index: 111, βάσει του Google Scholar: <https://scholar.google.com/citations?user=8aHcmTsAAAAJ&hl=el&oi=ao>). Ο Δημήτρης Αποστόλου είναι Καθηγητής του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιώς και μέλος του Εργαστηρίου Συστημάτων Υποστήριξης Αποφάσεων. Είναι Διδάκτωρ του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Η/Υ του ΕΜΠ, και κάτοχος MSc στην Τεχνολογία Πληροφοριών (Information Technology) από το University College London και MS σε Chemical Engineering & Environmental Science από το New Jersey Institute of Technology. Τα ερευνητικά του ενδιαφέροντα εστιάζονται σε Ευφυή Συστήματα Υποστήριξης Αποφάσεων, Συστήματα Υποστήριξης Ομάδων και Συστήματα Διαχείρισης Επιχειρησιακών Διαδικασιών και Γνώσης. Έχει συμμετάσχει σε μεγάλο αριθμό ερευνητικών έργων πληροφορικής επιδοτούμενων από την Ευρωπαϊκή Επιτροπή και Εθνικούς φορείς, με ρόλο υπεύθυνου έργου σε τρία από αυτά. Έχει διατελέσει σύμβουλος πληροφορικής και έχει συμμετάσχει σε έργα σχεδιασμού και ανάπτυξης πληροφοριακών συστημάτων για το δημόσιο τομέα και ιδιωτικούς φορείς. Έχει περισσότερες από 40 δημοσιεύσεις σε περιοδικά όπως Information Systems, IEEE Intelligent Systems, IEEE Computational Intelligence, International Journal of Information Management και πάνω από 90 δημοσιεύσεις σε πρακτικά συνεδρίων καθώς και ένα βιβλίο από τον εκδοτικό οίκο Springer-Verlag. Συμμετέχει σε επιτροπές συνεδρίων όπως το Business Information Management και είναι κριτής σε περιοδικά όπως το Decision Support Systems, Management Decision, Knowledge Management Research & Practice.

• **Καθηγητής Χρήστος Δουληγέρης** (παραθέσεις: 10138, h-index: 47, i10-index: 192, βάσει του Google Scholar: <https://scholar.google.com/citations?user=f7-JRJUAAAAJ&hl=el&oi=ao>). Ο Δρ. Χρήστος Δουληγέρης έλαβε το Δίπλωμα Ηλεκτρολόγου Μηχανικού από το ΕΜΠ και MSc, MPhil και PhD από το Πανεπιστήμιο Columbia της Νέας Υόρκης. Είναι καθηγητής στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς. Κατείχε τη θέση του Αναπληρωτή Καθηγητή στο University of Miami, ΗΠΑ. Διετέλεσε Πρόεδρος και Διευθύνων Σύμβουλος της Ηλεκτρονικής Διακυβέρνησης Α.Ε. (Η.ΔΙ.Κ.Α. Α.Ε.), μέλος της Εκτελεστικής Γραμματείας του Εθνικού Συμβουλίου του Ηλεκτρονικώς Επιχειρείν και είναι μέλος του Διοικητικού Συμβουλίου της Ελληνικής Εταιρείας Επιστημόνων και Επαγγελματιών Πληροφορικής και Επικοινωνιών. Διετέλεσε αναπληρωματικό μέλος της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Ο Καθ. Κ. Δουληγέρης έχει λάβει υποτροφία από το Ίδρυμα Κρατικών Υποτροφιών (ΙΚΥ) για μεταφορά τεχνογνωσίας από Έλληνες του εξωτερικού στην Ελλάδα (1987) και από το Ίδρυμα Fulbright για συνεργασία με το Εθνικό Ίδρυμα

Αγροτικών Ερευνών (1988). Έχει διατελέσει επιστημονικός υπεύθυνος των έργων σε πολλά έργα εθνικά και ευρωπαϊκά με αντικείμενο την ασφάλεια πληροφοριακών συστημάτων και επικοινωνιών. Ο Δρ. Δουληγέρης έχει εκτεταμένο δημοσιευμένο έργο σε διεθνή περιοδικά και πρακτικά συνεδρίων του χώρου των τηλεπικοινωνιών και έχει συμμετάσχει σε πληθώρα ερευνητικών και αναπτυξιακών προγραμμάτων. Επιμελήθηκε την ειδική έκδοση του περιοδικού IEEE Communications Magazine στην "Security for Telecommunication Networks" και έχει συνεπιμεληθεί το βιβλίο "Network Security: Current Status and Future Directions", IEEE Press/ John Wiley. Μετέχει στους επιμελητές έκδοσης πολλών περιοδικών όπως IEEE Communications Letters, IEEE Network, Computer Networks (Elsevier), International Journal of Wireless and Mobile Computing (IJWMC).

• **Καθηγητής Ιωάννης Θεοδωρίδης** (παραθέσεις: 15791, h-index: 56, i10-index: 156, βάσει του Google Scholar: <https://scholar.google.com/citations?user=1f5twhoAAAAJ&hl=el&oi=ao>). Ο Καθηγητής Γιάννης Θεοδωρίδης (γνωστικό αντικείμενο: Βάσεις Δεδομένων) είναι μέλος ΔΕΠ του Τμήματος Πληροφορικής, Διευθυντής του Εργαστηρίου Επιστήμης Δεδομένων. Τα ερευνητικά του ενδιαφέροντα κινούνται στο χώρο της Επιστήμης Δεδομένων (Data Science) και ειδικότερα περιλαμβάνουν διαχείριση και αναλυτική δεδομένων μεγάλου όγκου. Διατελεί μέλος της επιτροπής επιμελητών (editorial board) του περιοδικού ACM Computing Surveys (από το 2016). Επίσης έχει συνεισφέρει ως κριτής σε διεθνή περιοδικά και πρόεδρος ή μέλος επιτροπών συνεδρίων του χώρου της διαχείρισης δεδομένων, εξόρυξης γνώσης από δεδομένα, γεωπληροφορικής κλπ. Από το 2001 μέχρι σήμερα, έχει απασχοληθεί ως συντονιστής έργου ή επικεφαλής ερευνητικής ομάδας σε πλήθος ερευνητικών έργων του προγράμματος Horizon 2020 κ.α. Είναι συν-συγγραφέας τριών μονογραφιών και άνω των 100 άρθρων σε διεθνή επιστημονικά περιοδικά και συνέδρια με κρίση, με περισσότερες από 10.000 αναφορές στο έργο του (σύμφωνα με την πηγή Google Scholar). Γεννημένος το 1967, κατέχει Δίπλωμα (1990) and Διδακτορικό (1996) Ηλεκτρολόγου Μηχανικού και Μηχανικού Υπολογιστών από το Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ).

• **Καθηγητής Παναγιώτης Κοτζανικολάου** (παραθέσεις: 4233, h-index: 32, i10-index: 67, βάσει του Google Scholar: <https://scholar.google.com/citations?user=BOpUZOGAAAAJ&hl=el&oi=ao>). Ο Παναγιώτης Κοτζανικολάου είναι Καθηγητής (γνωστικό αντικείμενο: "Ασφάλεια και Ιδιωτικότητα Δικτύων Νέας Γενιάς") στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς και διευθυντής του Εργαστηρίου Ασφάλειας του Τμήματος. Κατέχει πτυχίο Πληροφορικής του Πανεπιστημίου Πειραιώς και διδακτορικό δίπλωμα στην ασφάλεια πληροφοριακών συστημάτων. Έχει εργαστεί ως Ειδικός Επιστήμονας στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

(Α.Δ.Α.Ε.) και ως σύμβουλος ασφάλειας συστημάτων στον ιδιωτικό τομέα. Έχει συμμετάσχει σε έργα έρευνας και ανάπτυξης και σε μελέτες στη θεματική περιοχή της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων, για φορείς του δημόσιου και του ιδιωτικού τομέα. Έχει συμμετάσχει σε οργανωτικές επιτροπές διεθνών συνεδρίων και είναι κριτής σε διεθνή επιστημονικά περιοδικά στο χώρο της ασφάλειας. Έχει δημοσιεύσει περισσότερες από 60 ερευνητικές δημοσιεύσεις σε επιστημονικά περιοδικά, συνέδρια και βιβλία στο χώρο της ασφάλειας και ιδιωτικότητας, έχοντας λάβει έως τώρα περισσότερες από 1250 ετεροαναφορές (h-index=19, Πηγή: Google Scholar). Είναι μέλος της Ελληνικής Εταιρείας Επιστημόνων Η/Υ και Πληροφορικής (ΕΠΥ). Έχει λάβει διάφορες πιστοποιήσεις ασφάλειας πληροφοριακών συστημάτων (CISSP, ISO 27001 Lead Auditor).

• **Καθηγητής Κωνσταντίνος Πατσάκης** (παραθέσεις: 10838, h-index: 43, i10-index: 105, βάσει του Google Scholar: <https://scholar.google.com/citations?user=wkHmlyAAAAJ&hl=el&oi=ao>). Ο Κωνσταντίνος Πατσάκης είναι Καθηγητής (Ερευνητικό Αντικείμενο: Ιομορφικό Λογισμικό και Κρυπτογραφία) στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς. Κατέχει πτυχίο Μαθηματικών από το Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών, μεταπτυχιακό στην ασφάλεια πληροφοριών από το Royal Holloway, University of London και διδακτορικό δίπλωμα στην ασφάλεια πληροφοριών από το Πανεπιστήμιο Πειραιώς. Έχει εργαστεί ως ερευνητής στην έδρα της UNESCO για ιδιωτικότητα στην Καταλονία και στο Trinity College της Ιρλανδίας. Έχει εργαστεί σε πλήθος Ευρωπαϊκών έργων (FP7, H2020) ως ερευνητής, τεχνικός διευθυντής και συντονιστής. Μέχρι σήμερα έχει δημοσιεύσει περισσότερα από 70 άρθρα σε διεθνή περιοδικά και συνέδρια και αποτελεί μέλος της οργανωτικής επιτροπής διεθνών συνεδρίων και είναι κριτής διεθνών περιοδικών του χώρου της ασφάλειας, κρυπτογραφίας και ιδιωτικότητας.

• **Καθηγήτρια Δέσποινα Πολέμη** (παραθέσεις: 898, h-index: 14, i10-index: 23, βάσει του Google Scholar: <https://scholar.google.com/citations?user=WuDuv4kAAAAJ&hl=el&oi=ao>). Η Δέσποινα Πολέμη (γνωστικό αντικείμενο: ασφάλεια και ηλεκτρονικό επιχειρείν) έχει λάβει πτυχία στα εφαρμοσμένα μαθηματικά (Applied Mathematics) από το Portland State University, και Ph.D. στη Θεωρία Πληροφοριών από το City University of New York. Στο παρελθόν κατείχε θέσεις στο Queens College, Baruch College of City University of New York και στο State University of New York at Farmingdale. Τα ερευνητικά της ενδιαφέροντα περιλαμβάνουν την ασφάλεια συστημάτων, την ασφάλεια στα ναυτιλιακά συστήματα και τις συνεργατικές υπηρεσίες. Έχει περισσότερες από 100 δημοσιεύσεις στις παραπάνω περιοχές. Έχει συμμετάσχει στην διοργάνωση πλήθους συνεδρίων και έχει λάβει χρηματοδοτήσεις από οργανισμούς

όπως οι Danish Research Foundation, MSI Army Research Office/Cornell University, IEEE, State University of New York (SUNY), και Graduate School of City University of New York (CUNY). Έχει διατελέσει Επιστημονικός Υπεύθυνος και Τεχνικός Υπεύθυνος πολλών ερευνητικών έργων από προγράμματα οργανισμών όπως είναι οι National Security Agency (NSA), Dr. Nuala McGann Drescher Foundation, Υπ. Άμυνας. Έχει διατελέσει μέλος της ομάδας ειδικών και κριτής προγραμμάτων του European Network and Information Security Agency (ENISA).

• **Καθηγητής Μιχάλης Ψαράκης** (παραθέσεις: 3277, h-index: 28, i10-index: 52, βάσει του Google Scholar: <https://scholar.google.com/citations?user=zX2KSXEAAAAJ&hl=el&oi=ao>). Ο Μιχάλης Ψαράκης είναι Καθηγητής με γνωστικό αντικείμενο «Αρχιτεκτονική Ενσωματωμένων Συστημάτων με έμφαση στο Υλικό» στο τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς, όπου διευθύνει το Εργαστήριο Ενσωματωμένων Συστημάτων. Κατέχει δίπλωμα Μηχανικού Ηλεκτρονικών Υπολογιστών από το τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών και Πληροφορικής του Πανεπιστημίου Πατρών και διδακτορικό δίπλωμα από το Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών. Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν: σχεδίαση, δοκιμή και επαλήθευση ενσωματωμένων συστημάτων, μικροεπεξεργαστών και συστημάτων-σε-τσιπ (SoC), σχεδίαση ενσωματωμένων συστημάτων ανεκτικών στα ελαττώματα, και σχεδίαση επιταχυντών με χρήση FPGA. Έχει δημοσιεύσει περισσότερες από 60 εργασίες σε έγκριτα περιοδικά και πρακτικά διεθνών συνεδρίων. Έχει διατελέσει μέλος της οργανωτικής επιτροπής και της επιτροπής προγράμματος πολλών διεθνών συνεδρίων (IEEE/ACM DATE, IEEE IOLTS, IEEE DFT, IEEE ISVLSI, ARC). Έχει εργαστεί στον ιδιωτικό τομέα για έξι χρόνια και έχει συμμετάσχει σε πολλά Ευρωπαϊκά και Εθνικά προγράμματα Έρευνας και Ανάπτυξης στον τομέα των ενσωματωμένων συστημάτων. Είναι μέλος της IEEE, της IEEE Computer Society και της ACM.

• **Αν. Καθηγητής Άγγελος Πικράκης** (παραθέσεις: 2878, h-index: 23, i10-index: 47, βάσει του Google Scholar: <https://scholar.google.com/citations?user=hPZSYsgAAAAJ&hl=el&oi=ao>). Ο Αναπληρωτής Καθηγητής Άγγελος Πικράκης (γνωστικό αντικείμενο: Επεξεργασία Σήματος με έμφαση σε ήχο-φωνή) είναι μέλος ΔΕΠ του Τμήματος Πληροφορικής, μέλος του Εργαστηρίου Επιστήμης Δεδομένων και συνεργαζόμενο μέλος του Ινστιτούτου Επεξεργασίας Λόγου (ΙΕΛ). Τα ερευνητικά του ενδιαφέροντα εντάσσονται στην περιοχή της ανάλυσης ήχων, με έμφαση σε αλγορίθμους μηχανικής μάθησης, Hidden Markov μοντέλα, Bayesian αρχιτεκτονικές και μεθόδους αντιστοίχισης ακολουθιών και επιβλέπει διδακτορικές διατριβές σε σχετικά γνωστικά αντικείμενα. Έχει συγγράψει στην αγγλική γλώσσα δύο βιβλία διεθνούς αναγνώρισης και περισσότερα από 50 άρθρα σε διεθνή επιστημονικά περιοδικά και συνέδρια με κριτές,

έχοντας λάβει έως τώρα περισσότερες από 1150 ετεροαναφορές (h-index=16, Google Scholar), ένα βραβείο καλύτερης εργασίας και μία πρώτη θέση σε διαγωνισμό αλγορίθμων. Έχει συμμετάσχει, σε ερευνητικά προγράμματα, χρηματοδοτούμενα από την ΓΓΕΤ και την ΕΕ, ως μέλος ερευνητικών ομάδων. Επίσης, διατελεί μέλος της επιτροπής επιμελητών (editorial board) του περιοδικού EURASIP Journal on Advances in Signal Processing (από το 2008 – σήμερα) και έχει συνεισφέρει για περισσότερο από δέκα έτη ως συνδιοργανωτής, μέλος της οργανωτικής επιτροπής και κριτής σε διεθνή περιοδικά και συνέδρια. Γεννήθηκε το 1970 και κατέχει Δίπλωμα Μηχανικού Η/Υ και Πληροφορικής από το Πανεπιστήμιο Πατρών (1993) και Διδακτορικό στην Επιστήμη της Πληροφορικής από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (2002).

• **Αν. Καθηγητής Διονύσιος Σωτηρόπουλος** (παραθέσεις: 1182, h-index: 17, i10-index: 30, βάσει του Google Scholar: <https://scholar.google.com/citations?user=cIdrKTOAAAAJ&hl=el&oi=ao>). Ο Δρ. Διονύσιος Σωτηρόπουλος έλαβε το διδακτορικό τίτλο του στην Πληροφορική από το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιά, στην Ελλάδα το έτος 2011. Το βασικό του πτυχίο του στην Πληροφορική το έλαβε από το ίδιο τμήμα το έτος 2003. Το ερευνητικό αντικείμενο της διδακτορικής του διατριβής εστιάζει σε θέματα βιο-εμπνευσμένου υπολογισμού με ιδιαίτερη έμφαση σε μεθοδολογίες μηχανικής μάθησης που βασίζονται σε Τεχνητά Ανοσοποιητικά Συστήματα. Αυτή τη στιγμή εργάζεται ως Αναπληρωτής Καθηγητής στο Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς με γνωστικό αντικείμενο «Βιο-εμπνευσμένοι Αλγόριθμοι με έμφαση στην Ανάλυση Κοινωνικών Μέσων». Έχει διατελέσει, επίσης, μετα-διδακτορικός ερευνητής στο Οικονομικό Πανεπιστήμιο Αθηνών στο τμήμα Διοικητικής Επιστήμης και Τεχνολογίας και είναι μέλος της ερευνητικής ομάδας SocioMine. Επιπλέον, κατείχε τη θέση του επισκέπτη ερευνητή στο Norwich Business School στο University of East Anglia. Τα κύρια ερευνητικά του ενδιαφέροντα αφορούν στους τομείς της Μηχανικής Μάθησης, της Εξόρυξης Δεδομένων, του Εξελικτικού Υπολογισμού, της Επεξεργασίας Σήματος, των Εφαρμογών Μοντελοποίησης Χρηστών για την δημιουργία Εξατομικευμένων Συστημάτων Σύστασης και των Ευφύων Συστημάτων Λογισμικού. Το ενδιαφέρον του σχετικά με τα Ψηφιακά Κοινωνικά Δίκτυα εστιάζεται στην ανάπτυξη αλγορίθμων μηχανικής μάθησης και αναγνώρισης προτύπων για την εξόρυξη δεδομένων από τα συγκεκριμένα δίκτυα. Η ερευνητική του δραστηριότητα σε αυτόν τον τομέα τα τελευταία χρόνια αριθμεί πλήθος δημοσιεύσεων σε θέματα που άπτονται της ανίχνευσης κοινοτήτων σε ψηφιακά κοινωνικά δίκτυα όπως το Twitter, της πρόγνωσης μελλοντικών δεσμών, της θεματικής μοντελοποίησης των αναρτήσεων

των χρηστών, της ανάλυσης συναισθήματος καθώς και της υπολογιστικής θεώρησης Μοντέλων Διαμόρφωσης Γνώμης.

7. ΕΡΕΥΝΗΤΙΚΑ ΕΡΓΑΣΤΗΡΙΑ

Οι διδάσκοντες του Προγράμματος Μεταπτυχιακών Σπουδών είναι συνδεδεμένοι με ερευνητικά εργαστήρια που λειτουργούν στο Πανεπιστήμιο Πειραιά. Τα εργαστήρια που αναφέρονται παρακάτω προσφέρουν τους ανθρώπινους και άλλους πόρους τους (h/w, s/w, κ.λπ.) στους φοιτητές του ΠΜΣ. Ειδικότερα:

- Το [Εργαστήριο Ασφάλειας](#) παρέχει υποστήριξη στα μαθήματα: “Ασφάλεια Δικτύων και Επικοινωνιών (Network and Communications Security)”, “Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων (Information Security Governance)”, “Εφαρμοσμένη Κρυπτογραφία (Applied Cryptography)”, “Έλεγχος Εισβολών Δικτύων και Συστημάτων (Penetration Testing)”, “Ανάλυση Ψηφιακών Πειστηρίων (Digital Forensics)”, “Ανάλυση Κακόβουλου Λογισμικού (Malware Analysis)”, “Ασφάλεια Λογισμικού (Software Security)”, “Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας (Advanced Cryptographic and Security Technologies)”, “Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων (Legal and Ethical Issues in Cybersecurity and Data Science)”.
- Το [Εργαστήριο Επιστήμης Δεδομένων](#) παρέχει υποστήριξη στα μαθήματα: “Αναλυτική Δεδομένων και Μηχανική Μάθηση (Data Analytics and Machine Learning)”, “Διαχείριση Μεγάλων Δεδομένων (Big Data Management)”, “Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων (Deep Learning with Applications in Cybersecurity and Analytics)”, “Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας (Geospatial Data Management and Analytics)”, “Οπτική Ανάλυση Δεδομένων (Visual Analytics)”, “Αναλυτική Γράφων και Δικτύων (Graph and Network Analytics)”, “Αναλυτική Χρονοσειρών και Πρόβλεψη (Time-Series Analytics and Forecasting)”, “Βαθιά Μηχανική Μάθηση (Deep Learning)”.
- Το [Εργαστήριο Συστημάτων Υποστήριξης Αποφάσεων](#) παρέχει υποστήριξη στα μαθήματα: “Τεχνικές Βελτιστοποίησης (Optimization Techniques)”, “Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής (Computational Tools for Business Analytics)”, “Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής (Mathematical Methods for Business Analytics)”.

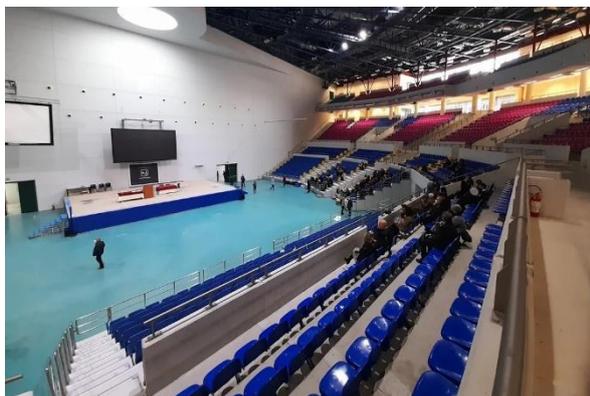
- Το [Εργαστήριο Διακριτών Μαθηματικών και Θεωρητικής Επιστήμης Υπολογιστών](#) παρέχει υποστήριξη στο μάθημα “Αλγόριθμοι και Πολυπλοκότητα (Algorithms and Complexity)”.
- Το [Εργαστήριο Ενσωματωμένων Συστημάτων](#) παρέχει υποστήριξη στα μαθήματα: “Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων (Secure Internet of Things Applications)”, “Σχεδίαση Ενσωματωμένων Συστημάτων (Embedded Systems Design)”, “Αξιόπιστα Υπολογιστικά Συστήματα (Dependable Computing Systems)”, “Προστασία Κρίσιμων Υποδομών (Critical Infrastructure Protection)”, “Ασφάλεια Υλικού (Hardware Security)”, “Αξιοπιστία Ενσωματωμένων Συστημάτων (Embedded Systems Reliability)”.
- Το [Εργαστήριο Δικτύων](#) παρέχει υποστήριξη στα μαθήματα “Σχεδίαση Αρχιτεκτονικών Ασφάλειας (Security Architecture Design)”, “(Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας (Special Topics in Security and Privacy))”.

8. ΥΛΙΚΟΤΕΧΝΙΚΗ ΥΠΟΔΟΜΗ

Για την εύρυθμη λειτουργία του ΠΜΣ διατίθενται αίθουσες διδασκαλίας και σεμιναρίων, αμφιθέατρα εξοπλισμένα με οπτικοακουστικά μέσα και εργαστήρια του Ιδρύματος. Τα μαθήματα πραγματοποιούνται στις υποδομές του Κτιριακού Συγκροτήματος της Νίκαιας. Επιπλέον, κατά τη διεξαγωγή των μαθημάτων αξιοποιούνται περιβάλλοντα προσομοίωσης και εικονικά εργαστήρια μέσω της συνεργασίας με οργανισμούς παρόχους «Υποδομής ως Υπηρεσίας» (Infrastructure as a Service). Ειδικότερα, κατά τα εργαστηριακά μαθήματα καλύπτονται οι εκπαιδευτικές ανάγκες που σχετίζονται με τη δημιουργία περιβάλλοντος μελέτης και δοκιμής ασφαλείας σε εικονικά περιβάλλοντα σε θέματα κυβερνοασφάλειας, συμπεριλαμβανομένης της διακυβέρνησης ασφαλείας, του σχεδιασμού αρχιτεκτονικής ασφαλείας, της ασφαλείας δικτύου, της ασφαλείας λογισμικού, ανάλυσης κακόβουλου λογισμικού, καθώς και με το σχεδιασμό ενσωματωμένου συστήματος, τις εφαρμογές ασφαλών IoT, τα αξιόπιστα συστήματα και τις κρίσιμες υποδομές, όπως επίσης με την επιχειρηματική αναλυτική και αναλυτική δεδομένων.

Επιπλέον, αξιοποιούνται υποδομές όπως η βιβλιοθήκη και η δυνατότητα πρόσβασης σε ηλεκτρονικές βάσεις δεδομένων, αίθουσα μελέτης, ο επιστημονικός και

εκπαιδευτικός εξοπλισμός, υπηρεσίες πληροφορικής και επικοινωνιών, καθώς και υποστηρικτικές ή συμβουλευτικές υπηρεσίες. Τέλος, για τη διάθεση και κατανομή των πόρων λαμβάνονται υπ' όψη οι ανάγκες των φοιτητών. Για παράδειγμα, τα μαθήματα διεξάγονται κατά τις ώρες 18:00 – 21:00 για την εξυπηρέτηση των εργαζομένων, ή επίσης έχουν δημιουργηθεί ράμπες για την διευκόλυνση της πρόσβασης φοιτητών με αναπηρίες. Επιπλέον, βάσει των ανωτέρω υποδομών ενισχύεται η φοιτητο-κεντρική μάθηση καθώς και η υιοθέτηση ευέλικτων τρόπων μάθησης και διδασκαλίας. Τέλος, αξίζει να σημειωθεί ότι όλες οι υποστηρικτικές δραστηριότητες και οι χώροι μπορούν να οργανωθούν με διάφορους τρόπους, ανάλογα με το εσωτερικό θεσμικό πλαίσιο.





9. ΠΑΡΟΧΕΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΗΡΕΣΙΕΣ ΙΔΡΥΜΑΤΙΚΟΣ ΛΟΓΑΡΙΑΣΜΟΣ

1) ΙΔΡΥΜΑΤΙΚΟΣ ΛΟΓΑΡΙΑΣΜΟΣ

Με την ολοκλήρωση της εγγραφής σας στο Πανεπιστήμιο, είναι απαραίτητη η ενεργοποίηση του λογαριασμού σας στην εφαρμογή <https://uregister.unipi.gr>. Με την ενεργοποίηση του λογαριασμού σας θα αποκτήσετε πρόσβαση τόσο στον προσωπικό σας φοιτητικό λογαριασμό, όσο και στις ηλεκτρονικές υπηρεσίες που παρέχει το Πανεπιστήμιο και το Υπουργείο Παιδείας. Μετά την εγγραφή στο σύστημα uRegister, κάθε χρήστης αποκτά πρόσβαση στην υπηρεσία mypassword, από όπου μπορεί α) να επαναφέρει τον κωδικό του, εάν τον έχει ξεχάσει, ή β) να διαχειρίζεται τον κωδικό του, το email και το κινητό τηλέφωνο που έχει δηλώσει. Η υπηρεσία διαχείρισης κωδικού χρήστη βρίσκεται στη διεύθυνση <https://mypassword.unipi.gr/>.

2) ΑΚΑΔΗΜΑΪΚΗ ΤΑΥΤΟΤΗΤΑ, ΦΟΙΤΗΤΙΚΟ ΕΙΣΙΤΗΡΙΟ

Η ακαδημαϊκή ταυτότητα είναι υποχρεωτική για όλους τους εγγεγραμμένους φοιτητές. Εκδίδεται μετά από αίτηση που υποβάλλεται ηλεκτρονικά στη διεύθυνση academicid.minedu.gov.gr. Η ακαδημαϊκή ταυτότητα λειτουργεί και ως φοιτητικό εισιτήριο (πάσο) που διευκολύνει τις μετακινήσεις με τα μέσα μαζικής μεταφοράς.



3) ΗΛΕΚΤΡΟΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ

Στη διεύθυνση <https://sso.unipi.gr/> λειτουργεί η διαδικτυακή εφαρμογή της Ηλεκτρονικής Γραμματείας. Από την εφαρμογή αυτή έχετε τη δυνατότητα:

- να ενημερώνετε για τα μαθήματα του προγράμματος σπουδών, τους διδάσκοντες, τα προτεινόμενα συγγράμματα, κλπ.,
- να υποβάλλετε δηλώσεις εγγραφής και δηλώσεις μαθημάτων κάθε εξαμήνου,
- να ενημερώνετε για τη βαθμολογία στα μαθήματα που έχετε εξεταστεί,
- να λαμβάνετε άμεσα και σε ηλεκτρονική μορφή βεβαιώσεις φοίτησης.

Η πρόσβαση στην εφαρμογή αυτή γίνεται μέσω των προσωπικών κωδικών.

4) ΕΦΑΡΜΟΓΗ ΦΟΙΤΗΤΙΚΗΣ ΜΕΡΙΜΝΑΣ

Στη διεύθυνση sitis.unipi.gr λειτουργεί η ηλεκτρονική πλατφόρμα υποβολής αιτήσεων της Φοιτητικής Μέριμνας. Από την εφαρμογή αυτή έχετε τη δυνατότητα να

υποβάλετε την αίτησή σας και να ανεβάσετε τα απαραίτητα δικαιολογητικά για σίτιση ή στέγαση.

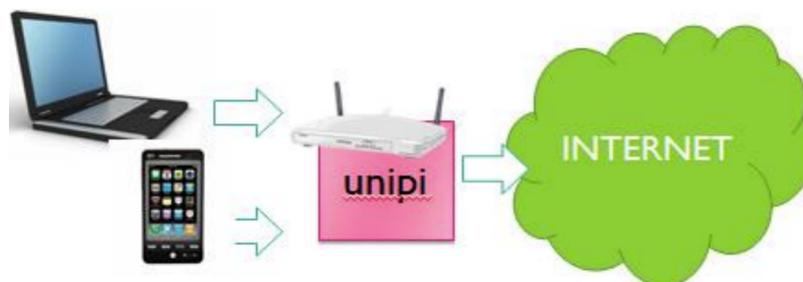
Επιπλέον μπορείτε να ελέγχετε το στάδιο στο οποίο βρίσκεται η αίτησή σας, μέχρι την τελική της αξιολόγηση.

5) ΥΠΗΡΕΣΙΑ ΑΠΟΜΑΚΡΥΣΜΕΝΗΣ ΠΡΟΣΒΑΣΗΣ – VPN

Η υπηρεσία πρόσβασης στο εσωτερικό δίκτυο του Πανεπιστημίου (υπηρεσία VPN) παρέχει δυνατότητα χρήσης των ηλεκτρονικών υπηρεσιών του Πανεπιστημίου από απομακρυσμένες θέσεις ή δίκτυα, όπως π.χ. από οικιακές συνδέσεις Internet. Μέσω της υπηρεσίας αυτής είναι, για παράδειγμα, εφικτή η πρόσβαση στο περιεχόμενο ηλεκτρονικών επιστημονικών βιβλίων, περιοδικών και βάσεων δεδομένων που διαθέτει η βιβλιοθήκη, από θέσεις εργασίας εκτός Πανεπιστημίου. Περισσότερα στοιχεία για την υπηρεσία αυτή δίνονται στην ηλεκτρονική διεύθυνση www.unipi.gr/unipi/el/hu-sundesh-vpn.html

6) ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ – WIFI

Όλοι οι χώροι διδασκαλίας του Πανεπιστημίου καλύπτονται από ελεύθερο ασύρματο δίκτυο wi-fi που ονομάζεται unipi. Σε αυτό μπορείτε να συνδεθείτε είτε με φορητό υπολογιστή είτε από το κινητό σας, χωρίς τη χρήση κάποιου κωδικού. Επίσης, όλοι οι φοιτητές που έχουν λάβει προσωπικό κωδικό, μπορούν να κάνουν χρήση του πανευρωπαϊκού ασύρματου δικτύου eduroam. Για τους εξουσιοδοτημένους χρήστες, είναι επιπλέον δυνατή η πρόσβαση στο διεθνές ακαδημαϊκό δίκτυο EDUROAM (www.eduroam.org), μέσω του οποίου χρήστες από όλη την Ευρώπη έχουν τη δυνατότητα να χρησιμοποιήσουν απομακρυσμένα και με ασφάλεια τις υπηρεσίες που παρέχει το ακαδημαϊκό τους ίδρυμα. Η χρήση του δικτύου eduroam προϋποθέτει την έκδοση προσωπικού κωδικού.



7) ΔΙΑΘΕΣΗ ΛΟΓΙΣΜΙΚΟΥ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΗ ΧΡΗΣΗ

Στους φοιτητές του Πανεπιστημίου παρέχεται δωρεάν πρόσβαση σε λογισμικό της εταιρείας Microsoft μέσω της υπηρεσίας Imagine (πρώην Dreamspark). Η πρόσβαση στην υπηρεσία Imagine γίνεται μέσω των προσωπικών κωδικών στη διεύθυνση dreamspark.unipi.gr Επίσης, σε όλους τους φοιτητές, ανεξαρτήτως βαθμίδας, και με τη χρήση του προσωπικού κωδικού διατίθεται το λογισμικό Microsoft Office 365 Education Plus, μέσω της διεύθυνσης <https://delos365.grnet.gr>. Αναλυτικές οδηγίες για την ενεργοποίηση της υπηρεσίας μπορείτε να βρείτε στη διεύθυνση <http://www.unipi.gr/unipi/images/various/noc/office365instructions.pdf>

Εκτός του λογισμικού που διατίθεται κεντρικά, ορισμένα ακαδημαϊκά τμήματα διαθέτουν επιπλέον συνδρομές για τις οποίες μπορείτε να ενημερωθείτε απευθείας από τους διδάσκοντες και τη Γραμματεία σας.



8) ΗΛΕΚΤΡΟΝΙΚΗ, ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΕΚΠΑΙΔΕΥΣΗ (E-LEARNING)

Στο Πανεπιστήμιο λειτουργούν, υπό την εποπτεία και με την επιμέλεια των Ακαδημαϊκών Τμημάτων συστήματα εξ αποστάσεως ηλεκτρονικής μάθησης τα οποία υποστηρίζουν το εκπαιδευτικό έργο. Σε αυτά αναρτώνται σημειώσεις, ανακοινώσεις και λοιπό εκπαιδευτικό υλικό. Ενημέρωση για τη χρήση τους παρέχεται από τους διδάσκοντες. Το σύστημα που εξυπηρετεί τους φοιτητές του τμήματος Πληροφορικής βρίσκεται στη διεύθυνση <http://gunet2.cs.unipi.gr>

9) ΒΙΒΛΙΟΘΗΚΗ

Website: www.lib.unipi.gr

Η Βιβλιοθήκη του Πανεπιστημίου Πειραιώς απευθύνεται στους καθηγητές, ερευνητές και φοιτητές, και αποστολή της είναι η υποστήριξη της εκπαίδευσης και της έρευνας. Στεγάζεται στο κεντρικό κτίριο του Πανεπιστημίου, στο δεύτερο υπόγειο. Η είσοδος της είναι στην κεντρική κυκλική σκάλα στο μέσο του ισογείου. Επίσης, για τα ΑΜΕΑ

χρησιμοποιείται και ο ανελκυστήρας στην αριστερή πλευρά του κτιρίου. Η βιβλιοθήκη αποτελείται από τρεις βασικούς χώρους:

- Το Χώρο Υποδοχής, όπου βρίσκεται ο χώρος κίνησης του υλικού, η κλειστή συλλογή, σπάνιες συλλογές και οι υπολογιστές για την αναζήτηση στον κατάλογο και τις πηγές πληροφόρησης,
- Το Βιβλιοστάσιο, όπου στεγάζεται το σύνολο της έντυπης συλλογής της βιβλιοθήκης, το φωτοτυπικό μηχάνημα και υπολογιστές για τους αναγνώστες, και
- Το Αναγνωστήριο, όπου βρίσκονται τα λεξικά, τα εκθετήρια με τα τελευταία τεύχη των έντυπων περιοδικών και άλλο πληροφοριακό υλικό.

Το ωράριο λειτουργίας της έχει επεκταθεί για να εξυπηρετεί τις ανάγκες των μελών του Πανεπιστημίου, από τις 8.00 το πρωί έως τις 20.00 το βράδυ, καθημερινά, όλες τις εργάσιμες ημέρες.

Υπηρεσίες βιβλιοθήκης Πανεπιστημίου Πειραιώς:

- Γενική πληροφόρηση: Στην υποδοχή δίνεται πληροφόρηση σχετικά με τη βιβλιοθήκη και το υλικό της, όπως κανόνες δανεισμού, φωτοτυπίες, χρήση οπτικοακουστικού υλικού, τοποθεσία τεκμηρίων κλπ. Για τον ίδιο λόγο έχουν εκδοθεί 9 ενημερωτικά φυλλάδια.
- Εξειδικευμένη πληροφόρηση: Η βιβλιοθήκη παρέχει online θεματικές συνδρομητικές και ανοικτής πρόσβασης βάσεις δεδομένων. Με ηλεκτρονικό ταχυδρομείο, τηλεφωνικά, ή προσωπικά, υποβάλλονται εξειδικευμένα ερωτήματα έρευνας που διεκπεραιώνονται από βιβλιοθηκονόμους του σχετικού τμήματος.
- Δανεισμός: κάθε μέλος του Πανεπιστημίου εγγράφεται ως μέλος στη βιβλιοθήκη, ώστε να δανείζεται το υλικό της. Λειτουργεί επίσης υπηρεσία ανανεώσεων και κρατήσεων για δανεισμένο υλικό και τήρηση προτεραιότητας δανεισμού κατά την επιστροφή.
- Απόκτηση υλικού που δεν υπάρχει στη βιβλιοθήκη, είτε με προτάσεις για τον εμπλουτισμό της ή με διαδανεισμό από τις ελληνικές βιβλιοθήκες, ή συνεργαζόμενες του εξωτερικού.
- Εκπαίδευση χρηστών: το προσωπικό της βιβλιοθήκης προσφέρει στους νεοεισερχόμενους φοιτητές, αλλά και σε κάθε ενδιαφερόμενο, υποστήριξη και ενημέρωση στη χρήση της βιβλιοθήκης, του καταλόγου της, των υπηρεσιών και των ηλεκτρονικών πηγών πληροφόρησης που παρέχει.

10. ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΠΜΣ

Το πρόγραμμα Κυβερνοασφάλειας & Επιστήμης Δεδομένων απευθύνεται σε επιστήμονες πληροφορικής και επαγγελματίες της πληροφορικής που επιθυμούν να εγγραφούν σε μεταπτυχιακές σπουδές πληροφορικής και να γνωρίσουν τις πρόσφατες εξελίξεις στους τομείς της ασφάλειας υπολογιστών και υποδομών και της ανάλυσης δεδομένων και επιχειρήσεων. Οι τομείς αυτοί παρουσιάζουν ταχεία επιστημονική ανάπτυξη, υψηλή δυναμική και συνεχώς αυξανόμενη ζήτηση στην ευρωπαϊκή και παγκόσμια αγορά. Το πρόγραμμα απονέμει Μεταπτυχιακό Δίπλωμα Ειδίκευσης (MSc) στην “Κυβερνοασφάλεια και Επιστήμη Δεδομένων” με τις ακόλουθες τρεις κατευθύνσεις:

- [Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων \(ΑΠΕΣ - ICSS\)](#)
- [Αξιοπιστία και ασφάλεια ενσωματωμένων συστημάτων \(ΑΑΕΣ - ESSR\)](#)
- [Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων \(ΕΑΑΔ - BDA\)](#)

Βασικές πληροφορίες:

Διάρκεια: 3 εξάμηνα πλήρους απασχόλησης

Ημερομηνία έναρξης: μέσα Οκτωβρίου

Τέλη: 4500€

ECTS: 90 μονάδες

Μερική απαλλαγή από τα δίδακτρα παρέχεται στους φοιτητές με τον υψηλότερο μέσο όρο βαθμολογίας, σε κάθε μία από τις τρεις προσφερόμενες κατευθύνσεις.

1) ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΚΟΠΟΣ ΤΟΥ ΠΜΣ

Το Πρόγραμμα Μεταπτυχιακών Σπουδών (ΠΜΣ) «Κυβερνοασφάλεια και Επιστήμη Δεδομένων», έχει ως αντικείμενο την εκπαίδευση νέων επιστημόνων στις επιστημονικές περιοχές της Ασφάλειας Εφαρμογών, Συστημάτων και Δικτύων, της Επιχειρησιακής Αναλυτικής και Αναλυτικής Δεδομένων καθώς και στις νέες επιστημονικές περιοχές που δημιουργούνται από τη σύγκλιση των παραπάνω περιοχών, όπως είναι η ασφάλεια και η ιδιωτικότητα μεγάλων δεδομένων και η εφαρμογή της επιστήμης δεδομένων στην ανάπτυξη προηγμένων τεχνολογιών ασφάλειας.

Σκοπός του ΠΜΣ είναι: η επιστημονική και τεχνολογική κατάρτιση σε πεδία της Πληροφορικής που εμφανίζουν ραγδαία επιστημονική ανάπτυξη, υψηλή δυναμική και

διαρκώς αυξανόμενη ζήτηση στην Ευρωπαϊκή και την παγκόσμια αγορά εργασίας όπως είναι τα πεδία που αναφέρθηκαν παραπάνω, με σκοπό την εκπαίδευση καταρτισμένων και ικανών επιστημόνων και ερευνητών που θα προωθήσουν την ανάπτυξη της χώρας και των Ελληνικών επιχειρήσεων στο πλαίσιο της Κοινωνίας της Πληροφορίας.

2) ΓΙΑΤΙ ΝΑ ΑΚΟΛΟΥΘΗΣΕΤΕ ΑΥΤΟ ΤΟ ΠΡΟΓΡΑΜΜΑ – ΕΥΚΑΙΡΙΕΣ ΕΡΓΑΣΙΑΣ

Οι τρέχουσες και μελλοντικές τάσεις της αγοράς δείχνουν μια συνεχώς αυξανόμενη ζήτηση για εμπειρογνώμονες σε διάφορους τομείς της Πληροφορικής, έναν από τους τομείς με τη μεγαλύτερη απορρόφηση στην αγορά εργασίας. Οι τρεις κατευθύνσεις που συνθέτουν το μεταπτυχιακό μας πρόγραμμα παρέχουν τόσο θεωρητικές όσο και πρακτικές δεξιότητες σε τεχνολογίες αιχμής της Πληροφορικής, συμπεριλαμβανομένης της Μηχανικής Μάθησης, της Κυβερνοασφάλειας, της Αναλυτικής Μεγάλων Δεδομένων, κτλ. Οι δεξιότητες αυτές θεωρούνται ότι βρίσκονται στις 10 κορυφαίες τάσεις της τεχνολογίας και της αγοράς για το 2021 και μετά, σύμφωνα με διάφορες έρευνες των [Forbes](#), [Gartner](#) και άλλων (ενδεικτικά παραδείγματα μπορείτε να βρείτε [εδώ](#) και [εδώ](#)).

Προοπτικές απασχόλησης για την ειδικευση Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΑΠΕΣ): Καθώς οι απειλές στον κυβερνοχώρο εξελίσσονται συνεχώς και τα δεδομένα γίνονται προσβάσιμα μέσω του διαδικτύου, η κυβερνοασφάλεια θα παραμείνει ένας κλάδος της πληροφορικής και διαρκώς ανερχόμενη ζήτηση. Οι μέσες απολαβές των ειδικών σε θέματα κυβερνοασφάλειας είναι υψηλότερες από τις αναμενόμενες μέσες απολαβές όλων των ειδικοτήτων της πληροφορικής. Η ανάγκη για ασφάλεια στον κυβερνοχώρο είναι τέτοια ώστε το 2021, οι επιθέσεις στον κυβερνοχώρο εκτιμάται ότι κόστισαν 6 τρισεκατομμύρια δολάρια παγκοσμίως. Η ζήτηση για εξειδικευμένους επιστήμονες στον τομέα της κυβερνοασφάλειας δεν αφορά μόνο άμεσα τον τομέα της πληροφορικής, αλλά εντοπίζεται επίσης σε όλους τους τομείς της οικονομίας, συμπεριλαμβανομένων των οικονομικών, της υγείας, της βιομηχανίας, των δημόσιων υπηρεσιών, της άμυνας και του ηλεκτρονικού εμπορίου, μεταξύ άλλων. Οι ευκαιρίες σταδιοδρομίας για τους αποφοίτους της κατεύθυνσης ΑΠΕΣ, περιλαμβάνουν, μεταξύ άλλων τις ειδικότητες: Μηχανικοί/σύμβουλοι κυβερνοασφάλειας, υπεύθυνοι προστασίας προσωπικών δεδομένων, αναλυτές κινδύνων ασφάλειας πληροφοριών, ελεγκτές ασφάλειας δικτύων και συστημάτων, ελεγκτές κώδικα κτλ.

Προοπτικές απασχόλησης για την ειδίκευση Ασφάλεια και Αξιοπιστία Ενσωματωμένων Συστημάτων (AAΕΣ): Ο πολλαπλασιασμός των συσκευών Διαδικτύου των Πραγμάτων (Internet of Things – IoT) στις εφαρμογές των επιχειρήσεων και της καθημερινής ζωής έχει ανοίξει μια σειρά από νέες θέσεις εργασίας ως σχεδιαστές και προγραμματιστές ενσωματωμένων συστημάτων στη σημερινή αγορά. Επιπλέον, δεδομένου ότι η ενσωμάτωση των συσκευών IoT σε βιομηχανίες με κρίσιμη σημασία για την ασφάλεια, όπως η αυτοκινητοβιομηχανία, η υγειονομική περίθαλψη, η αεροναυπηγική κ.λπ., είναι διαρκώς αυξανόμενη, η αξιοπιστία γίνεται ολοένα και πιο σημαντική, ωθώντας τις εταιρείες να προσλαμβάνουν εξειδικευμένους επιστήμονες στο σχεδιασμό ασφαλών και αξιόπιστων συστημάτων, καθιστώντας έτσι την κυβερνοασφάλεια ενσωματωμένων συστημάτων μια από τις πιο ανερχόμενες και καλά αμειβόμενες αγορές εργασίας για τους επιστήμονες πληροφορικής. Σύμφωνα με πρόσφατη έκθεση της Markets and Markets, το μέγεθος της παγκόσμιας αγοράς ασφάλειας IoT αναμένεται να αυξηθεί από 12,5 δισεκατομμύρια δολάρια το 2020 σε 36,6 δισεκατομμύρια δολάρια έως το 2025, ενώ βασικοί παράγοντες που οδηγούν σε αυτή την ανάπτυξη είναι οι αυξανόμενες ανησυχίες για την ασφάλεια των κρίσιμων υποδομών. Οι ευκαιρίες σταδιοδρομίας για τους αποφοίτους της κατεύθυνσης AAΕΣ, περιλαμβάνουν, μεταξύ άλλων τις ειδικότητες: Μηχανικοί υλικού και ενσωματωμένου λογισμικού IoT, Μηχανικοί ασφάλειας ενσωματωμένων συστημάτων, Μηχανικοί δοκιμών ενσωματωμένων συστημάτων/υλικού, Αναλυτές ασφάλειας IoT / κρίσιμων υποδομών κτλ.

Προοπτικές απασχόλησης για την ειδίκευση Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων (AAΕΔ): Το 2010 η ειδικότητα του αναλυτή δεδομένων εκτιμήθηκε ως η πλέον ανερχόμενη ειδίκευση πληροφορικής. Σήμερα, υπάρχουν ακόμη πολλοί περισσότεροι λόγοι για να σταδιοδρομήσει κανείς στην Επιστήμη Δεδομένων. Οι ανάγκες για επεξεργασία και ανάλυση μεγάλων ή πολύ μεγάλων δεδομένων θα συνεχίσουν να αυξάνονται. Σύμφωνα με μια πρόσφατη Έκθεση, η παγκόσμια αγορά μεγάλων δεδομένων προβλέπεται να αυξηθεί από 138,9 δισεκατομμύρια δολάρια το 2022 σε 229,4 δισεκατομμύρια δολάρια έως το 2025, με τον κλάδο της επιστήμης δεδομένων να αυξάνεται κατά 30% έως το 2024. Επιπλέον, η εκθετική ανάπτυξη της μηχανικής μάθησης και της τεχνητής νοημοσύνης θα αυξήσουν περαιτέρω τις ευκαιρίες απασχόλησης στην καινοτομία για τους αναλυτές δεδομένων. Οι ευκαιρίες σταδιοδρομίας για τους αποφοίτους της κατεύθυνσης AAΕΔ, περιλαμβάνουν, μεταξύ άλλων τις ειδικότητες: αναλυτές μηχανικής μάθησης/βαθιάς μάθησης, μηχανικοί μεγάλων δεδομένων, προγραμματιστές επιχειρηματικής αναλυτικής, αναλυτές δεδομένων κτλ.

Πέραν της διαρκώς αναπτυσσόμενης τάσης της αγοράς, οι μεταπτυχιακοί φοιτητές μας έχουν την ευκαιρία να συνεχίσουν τις σπουδές τους σε διδακτορικό επίπεδο. Επί του παρόντος, αρκετοί απόφοιτοι του Προγράμματος Μεταπτυχιακών Σπουδών μας υπηρετούν ως μεταδιδακτορικοί ερευνητές ή υποψήφιοι διδάκτορες σε όλους τους παραπάνω τομείς, συμμετέχοντας σε ερευνητικά προγράμματα που χρηματοδοτούνται από την ΕΕ και σε εθνικό επίπεδο.

3) ΚΑΤΗΓΟΡΙΕΣ ΕΙΣΑΚΤΕΩΝ

Στο ΠΜΣ γίνονται δεκτοί κάτοχοι τίτλου πρώτου κύκλου σπουδών Α.Ε.Ι. της ημεδαπής ή ομοταγών ιδρυμάτων της αλλοδαπής σύμφωνα με τις διατάξεις του άρθρου 34 του Ν.4485/2017, κατά προτεραιότητα πτυχιούχοι Τμημάτων Πληροφορικής, Σχολών Τεχνολογιών Πληροφορικής και Επικοινωνιών, Πολυτεχνείων ή Πολυτεχνικών Σχολών, Τμημάτων Θετικών Επιστημών Πανεπιστημίων, Μηχανικών Πληροφορικής Τ.Ε., Μηχανικών Τ.Ε., Σχολών Θετικών ή Τεχνολογικών Επιστημών ή/και άλλων συναφών με τις κατευθύνσεις ειδικοτήτων.

Τα μέλη των κατηγοριών Ε.Ε.Π., Ε.ΔΙ.Π. και Ε.Τ.Ε.Π. και διοικητικών υπαλλήλων του ιδρύματος, που πληρούν τις προϋποθέσεις της προηγούμενης παραγράφου, μπορούν μετά από αίτησή τους να γίνουν δεκτοί ως υπεράριθμοι, και μόνο ένας κατ' έτος, σύμφωνα με τις διατάξεις του Ν.4485/2017 (άρθρο 34, παρ.8), και σύμφωνα με τον Εσωτερικό Κανονισμό του ιδρύματος.

4) ΚΡΙΤΗΡΙΑ ΚΑΙ ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΛΟΓΗΣ ΥΠΟΨΗΦΙΩΝ ΓΙΑ ΤΟ ΠΜΣ

Η επιλογή των εισακτέων στο ΠΜΣ γίνεται σύμφωνα με τις διατάξεις και τις ρυθμίσεις του παρόντος Κανονισμού Μεταπτυχιακών Σπουδών.

Με απόφαση της Συνέλευσης, δημοσιεύεται και αναρτάται στην ιστοσελίδα του Τμήματος και του Ιδρύματος προκήρυξη για την εισαγωγή μεταπτυχιακών φοιτητών στο ΠΜΣ. Στην προκήρυξη αναγράφονται όλες τις σχετικές λεπτομέρειες (ημερομηνίες και τόπος κατάθεσης της αίτησης, απαραίτητα δικαιολογητικά που πρέπει να τη συνοδεύουν, κ.ά.). Οι σχετικές αιτήσεις μαζί με τα απαραίτητα δικαιολογητικά υποβάλλονται ηλεκτρονικά ή κατατίθενται στην Γραμματεία του Τμήματος, σε προθεσμία που ορίζεται κατά την προκήρυξη και δύναται να παραταθεί με απόφαση της Συνέλευσης του Τμήματος.

Τα απαιτούμενα δικαιολογητικά που υποβάλλονται από κάθε υποψήφιο είναι τα εξής:

1. Αίτηση εγγραφής.

2. Βιογραφικό σημείωμα.
3. Επικυρωμένο Αντίγραφο πτυχίου ή βεβαίωση περάτωσης σπουδών, εφόσον υπάρχει κατά τη στιγμή υποβολής της αίτησης. Η προσκόμιση του συγκεκριμένου δικαιολογητικού είναι απαραίτητη προϋπόθεση για την εγγραφή υποψηφίου στο ΠΜΣ.
4. Πιστοποιητικό αναλυτικής βαθμολογίας.
5. Δύο συστατικές επιστολές.
6. Αντίγραφο Πτυχιακής ή Διπλωματικής εργασίας (εάν εκπονήθηκε).
7. Επιστημονικές δημοσιεύσεις (εάν υπάρχουν).
8. Αποδεικτικά επαγγελματικής ή ερευνητικής δραστηριότητας (εάν υπάρχουν).
9. Πιστοποιητικό καλής γνώσης Αγγλικής γλώσσας και εφόσον υπάρχουν πιστοποιητικά γνώσης και άλλων γλωσσών.
10. Φωτοτυπία της αστυνομικής ταυτότητας ή του διαβατηρίου.
11. Μία πρόσφατη φωτογραφία, η οποία επισυνάπτεται στην αίτηση του υποψηφίου.

Η Συνέλευση του Τμήματος με απόφασή της δύναται να ορίσει πρόσθετο/α δικαιολογητικό/α. Η ακριβής διαδικασία περιγράφεται στην προκήρυξη.

Οι υποψήφιοι που είναι κάτοχοι τίτλου σπουδών πρώτου κύκλου από ιδρύματα της αλλοδαπής πρέπει να προσκομίσουν τον τίτλο σπουδών ώστε να γίνει έλεγχος εάν το ίδρυμα της αλλοδαπής περιλαμβάνεται στο Εθνικό Μητρώο αναγνωρισμένων ιδρυμάτων της αλλοδαπής, καθώς και το Εθνικό Μητρώο τύπων τίτλων σπουδών αναγνωρισμένων ιδρυμάτων της αλλοδαπής. Τίτλοι σπουδών της αλλοδαπής υποβάλλονται και γίνονται αποδεκτοί σύμφωνα με τις κείμενες διατάξεις.

Η επιλογή των εισακτέων πραγματοποιείται από επιτροπή μελών ΔΕΠ (Επιτροπή Επιλογής), που συγκροτείται με απόφαση της Συνέλευσης. Η έγκριση της εγγραφής των φοιτητών ορίζεται από τη Συνέλευση του Τμήματος.

Τα κριτήρια επιλογής καθώς και οι λεπτομέρειες εφαρμογής των κριτηρίων αυτών (μόρια, συντελεστές κ.λπ.) γίνονται γνωστά στους υποψηφίους με την προκήρυξη του ΠΜΣ και είναι τα ακόλουθα:

1. Βαθμός πτυχίου.
2. Συνάφεια του Τμήματος προέλευσης με το ΠΜΣ.
3. Είδος και εύρος εργασιακής ή/και ερευνητικής εμπειρίας.
4. Συστατικές επιστολές από μέλη ΔΕΠ ΑΕΙ ή / και από εργοδότη.
5. Γνώση Αγγλικής γλώσσας.
6. Συνέντευξη.

Η Συνέλευση του Τμήματος με απόφαση της δύναται να ορίσει πρόσθετο/α δικαιολογητικό/α. Η Συνέλευση δύναται να συγκροτεί Επιτροπή (Πρόσθετων Εσωτερικών) Εξετάσεων, κατόπιν πρότασης της Επιτροπής Επιλογής για όλους ή για μερικούς υποψηφίους. Την ύλη και το χρόνο των εξετάσεων αυτών καθορίζει η Επιτροπή Επιλογής.

Η διαδικασία επιλογής διενεργείται από την Επιτροπή Επιλογής, η οποία:

- 1) Καταρτίζει πλήρη κατάλογο όσων έχουν υποβάλει αίτηση.
- 2) Απορρίπτει τους υποψηφίους που δεν πληρούν τα ελάχιστα κριτήρια σε περίπτωση που έχουν τεθεί τέτοια από τη Συνέλευση και περιλαμβάνονται στον Κανονισμό Λειτουργίας του ΠΜΣ ή ο φάκελος τους είναι ελλιπής ως προς κάποιο δικαιολογητικό/έγγραφο.
- 3) Καλεί σε συνέντευξη όσους υποψηφίους αποφασισθεί να κληθούν. Η συνέντευξη γίνεται από τα μέλη της Επιτροπής Επιλογής.
- 4) Οργανώνει τυχόν εσωτερικές εξετάσεις για τους υποψηφίους που θα κριθεί απαραίτητο.
- 5) Ιεραρχεί βαθμολογικά τους υποψηφίους και υποβάλλει την πρότασή της για την τελική έγκριση στη Συνέλευση.

Οι επιτυχόντες θα πρέπει να εγγραφούν στη Γραμματεία του Τμήματος σε προθεσμία που θα οριστεί από την Συνέλευση του Τμήματος. Σε περίπτωση ισοβαθμίας, στην τελευταία θέση της κατάταξης του πίνακα επιτυχόντων, έχουν δυνατότητα εγγραφής όλοι οι ισοβαθμίσαντες.

Σε περίπτωση μη εγγραφής ενός ή περισσότερων φοιτητών, θα κληθούν αν υπάρχουν, οι επιλαχόντες, με βάση τη σειρά τους στον εγκεκριμένο αξιολογικό πίνακα, να εγγραφούν στο Πρόγραμμα.

5) ΔΙΑΡΚΕΙΑ ΣΠΟΥΔΩΝ – ΟΡΟΙ ΦΟΙΤΗΣΗΣ

Η χρονική διάρκεια σπουδών για την απονομή του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) ορίζεται σε τρία (3) ακαδημαϊκά εξάμηνα, στα οποία περιλαμβάνεται και ο χρόνος εκπόνησης μεταπτυχιακής διατριβής.

Ο ανώτατος επιτρεπόμενος χρόνος ολοκλήρωσης των σπουδών, ορίζεται στα έξι (6) ακαδημαϊκά εξάμηνα. Ο μεταπτυχιακός φοιτητής με αίτησή του μπορεί να ζητήσει αιτιολογημένα προσωρινή αναστολή φοίτησης η οποία δεν υπερβαίνει τα δύο

εξάμηνα. Τα εξάμηνα αναστολής της φοιτητικής ιδιότητας δεν προσμετρώνται στην προβλεπόμενη ανώτατη διάρκεια κανονικής φοίτησης.

6) ΣΥΝΟΠΤΙΚΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΠΟΥΔΩΝ

Τα μαθήματα, η κατανομή τους ανά εξάμηνο και ανά ειδίκευση καθώς και οι πιστωτικές μονάδες ECTS (συντομογραφία ΠΜ) παρουσιάζονται ενδεικτικά στον ακόλουθο πίνακα. Τα υποχρεωτικά (Υ) μαθήματα κάθε ειδίκευσης, δύναται να είναι μαθήματα επιλογής στις άλλες ειδικεύσεις. Τα υπόλοιπα μαθήματα τα οποία προσφέρονται αποκλειστικά ως μαθήματα επιλογής και δεν είναι υποχρεωτικά σε κάποια ειδίκευση, θα προσαρμόζονται δυναμικά, με βάση τον αριθμό των ενεργών φοιτητών ανά κύκλο σπουδών και τις τρέχουσες επιστημονικές εξελίξεις. Η τροποποίηση του προγράμματος μαθημάτων και η ανακατανομή των μαθημάτων μεταξύ των εξαμήνων μπορεί να γίνει με αποφάσεις των αρμοδίων οργάνων και θα περιλαμβάνονται στον Κανονισμό Μεταπτυχιακών Σπουδών.

Τα μαθήματα, η κατανομή τους ανά εξάμηνο και ανά ειδίκευση καθώς και οι πιστωτικές μονάδες ECTS (συντομογραφία ΠΜ) παρουσιάζονται ενδεικτικά στον ακόλουθο πίνακα.

Στο πρώτο εξάμηνο, οι φοιτητές της ειδίκευσης ΑΠΕΣ υποχρεούνται να παρακολουθήσουν τέσσερα (4) μαθήματα υποχρεωτικά, καθώς και ένα (1) μάθημα επιλογής 6 πιστωτικών μονάδων ή δύο (2) μαθήματα επιλογής 3 πιστωτικών μονάδων από τα υπόλοιπα προσφερόμενα μαθήματα. Στο πρώτο εξάμηνο, οι φοιτητές των ειδικεύσεων ΑΑΕΣ και ΕΑΑΔ υποχρεούνται να παρακολουθήσουν πέντε (5) μαθήματα υποχρεωτικά, καθώς και ένα (1) μάθημα επιλογής 6 πιστωτικών μονάδων ή δύο (2) μαθήματα επιλογής 3 πιστωτικών μονάδων από τα υπόλοιπα προσφερόμενα μαθήματα. Στο δεύτερο εξάμηνο, οι φοιτητές των ειδικεύσεων ΑΠΕΣ και ΕΑΑΔ υποχρεούνται να παρακολουθήσουν τέσσερα (4) μαθήματα υποχρεωτικά, καθώς και δύο (2) μαθήματα επιλογής 6 πιστωτικών μονάδων ή τέσσερα (4) μαθήματα επιλογής 3 πιστωτικών μονάδων ή τρία (3) μαθήματα επιλογής εκ των οποίων το ένα (1) 6 πιστωτικών μονάδων και τα υπόλοιπα δύο (2) πιστωτικών μονάδων από τα υπόλοιπα προσφερόμενα μαθήματα. Στο δεύτερο εξάμηνο, οι φοιτητές της ειδίκευσης ΑΑΕΣ υποχρεούνται να παρακολουθήσουν τρία (3) μαθήματα υποχρεωτικά, καθώς και δύο (2) μαθήματα επιλογής 6 πιστωτικών μονάδων ή τέσσερα (4) μαθήματα επιλογής 3 πιστωτικών μονάδων ή τρία (3) μαθήματα επιλογής εκ των οποίων το ένα (1) 6 πιστωτικών μονάδων και τα υπόλοιπα δύο (2) πιστωτικών μονάδων από τα υπόλοιπα προσφερόμενα μαθήματα.

Το πρόγραμμα των μαθημάτων ανά ειδίκευση διαμορφώνεται ως εξής έχοντας τις εξής ειδικεύσεις:

- 1. Ειδίκευση: «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων» (Information and Communication Systems Security), συντομογραφία ΑΠΕΣ**
- 2. Ειδίκευση: «Ασφάλεια και Αξιοπιστία Ενσωματωμένων Συστημάτων» (Embedded Systems Security and Reliability), συντομογραφία ΑΑΕΣ**
- 3. Ειδίκευση: «Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων» (Business and Data Analytics), συντομογραφία ΕΑΑΔ**

Στον παρακάτω πίνακα παρατίθενται τα μαθήματα που διατίθενται για το 1^ο εξάμηνο του ΠΜΣ "Κυβερνοασφάλεια και Επιστήμη Δεδομένων".

Α' ΕΞΑΜΗΝΟ				
(με Υ σημειώνονται τα υποχρεωτικά ειδίκευσης)				
Τίτλος μαθήματος	ΑΠΕΣ	ΑΑΕΣ	ΕΑΑΔ	ΠΜ
Ασφάλεια Δικτύων και Επικοινωνιών (Network and Communications Security)	Υ			6
Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων (Information Security Governance)	Υ			6
Σχεδίαση Αρχιτεκτονικών Ασφάλειας (Security Architecture Design)	Υ	Υ		6
Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων (Secure Internet of Things Applications)		Υ		3

Σχεδίαση Ενσωματωμένων Συστημάτων (Embedded Systems Design)		Υ		6
Αξιόπιστα Υπολογιστικά Συστήματα (Dependable Computing Systems)		Υ		3
Προστασία Κρίσιμων Υποδομών (Critical Infrastructure Protection)				3
Αναλυτική Δεδομένων και Μηχανική Μάθηση (Data Analytics and Machine Learning)	Υ	Υ	Υ	6
Διοικητική Πληροφοριακών Συστημάτων (Information Systems Management)			Υ	3
Τεχνικές Βελτιστοποίησης (Optimization Techniques)			Υ	6

Διαχείριση Μεγάλων Δεδομένων (Big Data Management)			Υ	6
Βαθιά Μηχανική Μάθηση (Deep Learning)			Υ	3
Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής (Computational Tools for Business Analytics)				3
Αλγόριθμοι και Πολυπλοκότητα (Algorithms and Complexity)				3
Εφαρμοσμένη Κρυπτογραφία (Applied Cryptography)				3
ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ Α΄ ΕΞΑΜΗΝΟΥ ΑΝΑ ΕΙΔΙΚΕΥΣΗ				30

Στον παρακάτω πίνακα παρατίθενται τα μαθήματα που διατίθενται για το 2^ο εξάμηνο του ΠΜΣ "Κυβερνοασφάλεια και Επιστήμη Δεδομένων".

Β' ΕΞΑΜΗΝΟ

(με Υ σημειώνονται τα υποχρεωτικά ειδίκευσης)

Τίτλος μαθήματος	ΑΠΕΣ	ΑΑΕΣ	ΕΑΑΔ	ΠΜ
Έλεγχος Εισβολών Δικτύων και Συστημάτων (Penetration Testing)	Υ			6

Ανάλυση Ψηφιακών Πειστηρίων (Digital Forensics)	Y			3
Ανάλυση Κακόβουλου Λογισμικού (Malware Analysis)	Y			3
Ασφάλεια Λογισμικού (Software Security)	Y	Y		6
Ασφάλεια Υλικού (Hardware Security)		Y		6
Αξιοπιστία Ενσωματωμένων Συστημάτων (Embedded Systems Reliability)		Y		6
Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής (Mathematical Methods for Business Analytics)			Y	6
Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων (Deep Learning with Applications in Cybersecurity)			Y	3

and Analytics)				
Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας (Geospatial Data Management and Analytics)			Y	3
Οπτική Ανάλυση Δεδομένων (Visual Analytics)			Y	6
Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας (Advanced Cryptographic and Security Technologies)				3
Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας (Special Topics in Security and Privacy)				3
Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων (Legal and Ethical Issues in Cybersecurity and Data Science)				3
Αναλυτική Γράφων και Δικτύων (Graph and Network				3

Analytics)				
Αναλυτική Χρονοσειρών και Πρόβλεψη (Time-Series Analytics and Forecasting)				3
ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ Β΄ ΕΞΑΜΗΝΟΥ ΑΝΑ ΕΙΔΙΚΕΥΣΗ				30

Γ΄ ΕΞΑΜΗΝΟ				
Τίτλος μαθήματος	ΑΠΕΣ	ΑΑΕΣ	ΕΑΑΔ	ΠΜ
Μεταπτυχιακή Διπλωματική Εργασία (MSc thesis)	Υ	Υ	Υ	30
ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ Γ΄ ΕΞΑΜΗΝΟΥ				30
ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ ΠΜΣ				90

7) ΕΠΙΣΤΗΜΟΝΙΚΟΙ ΣΤΟΧΟΙ

Οι βασικοί επιστημονικοί στόχοι των τριών ειδικοτήσεων είναι οι εξής:

- **Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων:** Στόχος της κατεύθυνσης αυτής είναι η εξειδίκευση των φοιτητών και η απόκτηση των απαιτούμενων γνώσεων σε θεωρητικό και σε πρακτικό επίπεδο, στην ανάλυση, το σχεδιασμό, τη διαμόρφωση και την υλοποίηση τεχνολογιών ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. Το πρόγραμμα σπουδών παρέχει εξειδικευμένες γνώσεις σε ζητήματα ασφάλειας όπως είναι η ασφάλεια δικτύων και επικοινωνιών, η διοίκηση ασφάλειας πληροφοριακών συστημάτων, η σχεδίαση αρχιτεκτονικών ασφάλειας, ο έλεγχος για τον εντοπισμό και την πρόληψη εισβολών σε δίκτυα και συστήματα, η ασφάλεια λογισμικού και η ανάλυση ψηφιακών πειστηρίων και κακόβουλου λογισμικού, σε συνδυασμό με θεμελιώδεις γνώσεις αναλυτικής δεδομένων και μηχανικής μάθησης. Μέσω των μαθημάτων επιλογής, οι φοιτητές μπορούν να εμβαθύνουν σε ειδικά θέματα

κρυπτογραφίας, ασφάλειας και ιδιωτικότητας, ενώ έχουν τη δυνατότητα να κατανοήσουν ζητήματα ασφάλειας ενσωματωμένων συστημάτων και μεθόδους βαθιάς μηχανικής μάθησης, με σκοπό την εφαρμογή τους στην ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων.

- **Ασφάλεια και Αξιοπιστία Ενσωματωμένων Συστημάτων:** Στόχος της κατεύθυνσης αυτής είναι η εξειδίκευση των φοιτητών και η απόκτηση των απαιτούμενων γνώσεων σε θεωρητικό και σε πρακτικό επίπεδο, στην ανάλυση, το σχεδιασμό, τη διαμόρφωση και την υλοποίηση τεχνολογιών ασφάλειας υπολογιστικών συστημάτων καθώς και υποδομών. Το πρόγραμμα σπουδών παρέχει εξειδικευμένες γνώσεις σε ζητήματα ασφάλειας όπως είναι η σχεδίαση αρχιτεκτονικών ασφάλειας, η ασφάλεια ενσωματωμένων συστημάτων και κρίσιμων υποδομών, οι εφαρμογές ασφάλειας στο διαδίκτυο των πραγμάτων (Internet of Things), η ασφάλεια σε επίπεδο υλικού, η ασφάλεια λογισμικού και η αξιοπιστία ενσωματωμένων συστημάτων, σε συνδυασμό με θεμελιώδεις γνώσεις αναλυτικής δεδομένων και μηχανικής μάθησης. Μέσω των μαθημάτων επιλογής, οι φοιτητές μπορούν να εμβαθύνουν στις απαιτήσεις ασφάλειας ενσωματωμένων υπολογιστικών συστημάτων, ενώ έχουν τη δυνατότητα να κατανοήσουν θέματα ασφάλειας δικτύων, κρυπτογραφίας και τεχνολογιών βαθιάς μάθησης, με σκοπό την εφαρμογή τους στην ασφάλεια υποδομών και συστημάτων.
- **Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων:** Στόχος της κατεύθυνσης αυτής είναι η εξειδίκευση των φοιτητών και η απόκτηση των απαιτούμενων γνώσεων σε θεωρητικό και σε πρακτικό επίπεδο, στην επιστήμη δεδομένων, την επιχειρηματική αναλυτική καθώς και στις αναδυόμενες τεχνολογίες πληροφορίας. Το πρόγραμμα σπουδών συνδυάζει τη μελέτη μεθοδολογιών και εργαλείων ανάπτυξης πληροφοριακών συστημάτων και διαχείρισης μεγάλων δεδομένων και επιχειρηματικών διαδικασιών, τεχνικών βελτιστοποίησης, αναλυτικής δεδομένων, στατιστικών μεθόδων επιχειρηματικής αναλυτικής, με ζητήματα διοίκησης ασφάλειας πληροφοριακών συστημάτων. Μέσω των μαθημάτων επιλογής, οι φοιτητές εμβαθύνουν περαιτέρω σε ζητήματα επιχειρηματικής αναλυτικής και αναλυτικής δεδομένων όπως είναι σύγχρονα εργαλεία επιχειρηματικής αναλυτικής, οπτική αναλυτική δεδομένων και αναλυτική γεωγραφικής πληροφορίας, και έχουν τη δυνατότητα να κατανοήσουν τις απαιτήσεις ασφάλειας πληροφοριακών και ενσωματωμένων συστημάτων με σκοπό τη μελέτη επιχειρηματικών μοντέλων και τεχνολογιών διαχείρισης δεδομένων.

11. ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΩΝ ΑΝΑ ΕΙΔΙΚΕΥΣΗ ΚΑΙ ΕΞΑΜΗΝΟ

Σε αυτή την ενότητα περιγράφονται αναλυτικά τα μαθήματα που προσφέρονται ανά ειδίκευση (κατεύθυνση) και εξάμηνο. Εφόσον το πρόγραμμα διδασκαλίας το επιτρέπει, οι φοιτητές μπορούν να επιλέξουν μάθημα που προσφέρεται από άλλη κατεύθυνση είτε υποχρεωτικό είτε προαιρετικό, ως μάθημα επιλογής.

1) ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΑΠΕΣ)

Η κατεύθυνση **Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων** επικεντρώνεται στη μελέτη των τελευταίων τεχνολογιών και μεθόδων για την ασφάλεια στον κυβερνοχώρο. Με βάση ένα αρθρωτό πρόγραμμα, οι σπουδαστές θα είναι σε θέση να αποκτήσουν βαθιά γνώση των βασικών θεμάτων κυβερνοασφάλειας, όπως η διακυβέρνηση της ασφάλειας, ο σχεδιασμός της αρχιτεκτονικής ασφάλειας, η ασφάλεια δικτύων, η ασφάλεια λογισμικού, ο έλεγχος διείσδυσης, η ψηφιακή εγκληματολογία και η ανάλυση κακόβουλου λογισμικού. Ταυτόχρονα, οι φοιτητές θα μπορούν να εστιάσουν στο προσωπικό τους επιστημονικό υπόβαθρο και τα ενδιαφέροντά τους, μέσω επιλεκτικών μαθημάτων σε ειδικά θέματα ασφάλειας και ιδιωτικότητας, αλλά και να εμπλουτίσουν τις γνώσεις τους με θέματα που σχετίζονται με την αξιοπιστία συστημάτων και την επιστήμη των δεδομένων. Οι φοιτητές πρέπει να παρακολουθήσουν με επιτυχία έναν αριθμό μαθημάτων που ανέρχεται σε 30 ECTS ανά εξάμηνο. Κατά τη διάρκεια του 1ου και 2ου εξαμήνου, η κατεύθυνση προσφέρει 4 υποχρεωτικά μαθήματα και αρκετά επιλεκτικά μαθήματα σχετικά με την ασφάλεια, ενώ οι φοιτητές μπορούν επίσης να επιλέξουν 1-2 μαθήματα από άλλες κατευθύνσεις. Το 3ο εξάμηνο είναι αφιερωμένο στη διπλωματική εργασία σε ένα σύγχρονο θέμα της κυβερνοασφάλειας, υπό την επίβλεψη ενός από τους διδάσκοντες της κατεύθυνσης.

Α' ΕΞΑΜΗΝΟ

CDS101: Ασφάλεια δικτύων και επικοινωνιών

(ECTS: 6, Υποχρεωτικό)

Η ασφάλεια δικτύων και επικοινωνιών περιλαμβάνει μεθόδους, τεχνικές και εργαλεία ασφάλειας που χρησιμοποιούνται στο σχεδιασμό, την εφαρμογή και τον έλεγχο μιας πολιτικής ασφάλειας δικτύου. Το θεωρητικό μέρος του μαθήματος περιλαμβάνει την ανάλυση των τρωτών σημείων ασφαλείας στα πρωτόκολλα επικοινωνίας για όλα τα επίπεδα της στοίβας δικτύων TCP/IP και τον ορισμό μιας πολιτικής ασφαλείας δικτύου. Το πρακτικό μέρος του μαθήματος περιλαμβάνει την εφαρμογή ελέγχων ασφαλείας δικτύου, όπως τείχη προστασίας, συστήματα ανίχνευσης/πρόληψης

εισβολών (IDS/IPS) και εικονικά ιδιωτικά δίκτυα. Τα κύρια θέματα που καλύπτονται περιλαμβάνουν:

- Εισαγωγή στην ασφάλεια δικτύων
- Ασφάλεια επιπέδου σύνδεσης δεδομένων (Ethernet, ARP, WiFi)
- Ασφάλεια επιπέδου δικτύου (IP, IPSec)
- Ασφάλεια επιπέδου μεταφοράς (SSL/TLS)
- Σχεδιασμός πολιτικών ασφάλειας δικτύου
- Μηχανισμοί ασφάλειας δικτύου πολλαπλών επιπέδων (τείχη προστασίας, συστήματα ανίχνευσης εισβολών)
- Τείχη προστασίας επιπέδου εφαρμογής και IDS

Εργαστήρια: snort, ossec, wireshark και nmap και υλοποιήσεις πρωτοκόλλων ασφαλείας, συμπεριλαμβανομένων των strongswan και openssl.

Συντονιστής μαθήματος: [Παναγιώτης Κοτζανικολάου](#)

CDS102: Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων

(ECTS: 6, Υποχρεωτικό)

Το μάθημα αυτό επικεντρώνεται στη διαχείριση της ασφάλειας και της ιδιωτικότητας των πληροφοριακών συστημάτων (ΠΣ). Περιγράφονται οι κύριες φάσεις της εφαρμογής του ISMS (Σύστημα διαχείρισης της ασφάλειας των πληροφοριών). Παρουσιάζονται οι απαιτήσεις των προτύπων διαχείρισης της ασφάλειας των πληροφοριών (π.χ. ISO 27001, 27002, ISO15408, ETSI-TVRA), καθώς και τα κύρια βήματα των μεθοδολογιών αξιολόγησης / διαχείρισης κινδύνων (π.χ. OCTAVE, CRAMM, ISO 27005, ISO18045). Το δεύτερο μέρος εξετάζει τη διακυβέρνηση της ασφάλειας των πληροφοριών που περιλαμβάνει την αξιολόγηση της εφαρμογής των προτύπων ασφάλειας και επιχειρησιακής συνέχειας (π.χ. ISO 22301) με βάση τις επιχειρησιακές ανάγκες του οργανισμού. Για το σκοπό αυτό παρουσιάζεται το πρότυπο COBIT 5. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Βασικές έννοιες και ορολογία
- Πρότυπα αξιολόγησης κινδύνων
- Μεθοδολογίες και εργαλεία διαχείρισης κινδύνων
- Πολιτικές και διαδικασίες ασφαλείας
- Έλεγχος και πιστοποίηση ασφαλείας
- Εφαρμογή νομικών και πολιτικών απαιτήσεων
- Επιχειρησιακή συνέχεια
- Χειρισμός περιστατικών
- Ασφάλεια εφοδιαστικής αλυσίδας
- Εργαλεία για την αξιολόγηση κινδύνων στην αλυσίδα εφοδιασμού

Πεδίο εφαρμογής του μαθήματος: Οι στόχοι του μαθήματος είναι η εξοικείωση με:

- Πρότυπα και εργαλεία διαχείρισης της ασφάλειας
- Μεθοδολογίες και εργαλεία εκτίμησης κινδύνου
- Πρότυπα και διαδικασίες για την επιχειρησιακή συνέχεια και την ανάκαμψη από καταστροφές
- Έλεγχος και πιστοποίηση ασφάλειας

Εργαστήρια: CRAMM, eBIOS, MITIGATE

Συντονιστής μαθήματος: [Πολέμη Δέσποινα \(Νινέτα\)](#)

CDS103: Σχεδίαση Αρχιτεκτονικών Ασφάλειας

(ECTS: 6, Υποχρεωτικό)

Στόχος αυτού του μαθήματος είναι ο προσδιορισμός και η ανάλυση των βασικών αρχών σχεδιασμού ασφαλών πληροφοριακών συστημάτων. Αυτό επιτυγχάνεται μέσω της εισαγωγής γνωστών βέλτιστων πρακτικών για την εφαρμογή μηχανισμών ασφαλείας και πρωτοκόλλων επικοινωνίας για σύγχρονα συστήματα που βασίζονται κυρίως στην κρυπτογραφία. Οι κύριοι στόχοι του μαθήματος είναι:

- Προσδιορισμός των κύριων στοιχείων της σύγχρονης αρχιτεκτονικής των πληροφοριακών συστημάτων.
- Να αποτυπώσει το εύρος και την πολυπλοκότητα των τρωτών σημείων ασφαλείας των πληροφοριακών συστημάτων.
- Καθορισμός των βασικών αρχών ασφαλείας όσον αφορά το σχεδιασμό προηγμένων μηχανισμών και στοιχείων.

Η κατανόηση των σχετικών μοντέλων ασφάλειας που βασίζονται στις παραπάνω βασικές αρχές, η εφαρμογή των οποίων μετριάζει και ελαχιστοποιεί τις απειλές ασφαλείας.

Το μάθημα καλύπτει τους ακόλουθους τομείς:

- Εισαγωγή στην ασφάλεια πληροφοριών
- Απαιτήσεις αρχιτεκτονικής ασφάλειας πληροφοριών
- Η διαδικτυακή πλατφόρμα και οι απειλές της
- Απειλές και επιθέσεις της διαδικτυακής πλατφόρμας
- Σχεδιασμός ασφαλείας κινητών τηλεφώνων
- Σενάρια πραγματικών περιπτώσεων

Εργαστήρια: που έχουν ως κύριο στόχο την εμπέδωση και εφαρμογή όλων των παραπάνω στη διαδικασία σχεδιασμού ασφαλών Πληροφοριακών Συστημάτων.

Συντονιστής μαθήματος: [Χρήστος Δουληγέρης](#)

CDS107: Αναλυτική Δεδομένων και Μηχανική Μάθηση

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στην ανάλυση δεδομένων (αρχές, αγωγός, προεπεξεργασία). Κοινές μέθοδοι μηχανικής μάθησης (ταξινόμηση, ομαδοποίηση). Νευρωνικά δίκτυα και βαθιά μάθηση. Προηγμένες τεχνικές ομαδοποίησης (DBSCAN, OPTICS κ.λπ.). Εφαρμογές στην εξόρυξη δεδομένων κειμένου/ήχου/βίντεο.

Εργαστηριακές ώρες με Python, R, Spark MLlib.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

CDS113: Εφαρμοσμένη Κρυπτογραφία

(ECTS: 3)

Στόχος αυτού του μαθήματος είναι να εξοικειωθούν οι φοιτητές με τις τελευταίες εξελίξεις στην κρυπτογραφία, από πρακτική σκοπιά. Το μάθημα καλύπτει όλα τα απαραίτητα κρυπτογραφικά πρωτεύοντα στοιχεία και τον τρόπο με τον οποίο χρησιμοποιούνται ενεργά σε διάφορους τομείς για να παρέχουν τα απαραίτητα δομικά στοιχεία για δομές που σχετίζονται με την ασφάλεια και την ιδιωτικότητα. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Συμμετρική και ασύμμετρη κρυπτογράφηση
- Λειτουργίες κατακερματισμού
- Ψηφιακές υπογραφές
- Δημιουργία και ανταλλαγή κλειδιών
- Ομομορφική κρυπτογράφηση
- Πρωτόκολλα κρυπτογράφησης
- Ασφαλείς υπολογισμοί

Εργαστήρια: Πρακτικές ασκήσεις και υλοποίηση κρυπτογραφικών πρωτοβουλιών. Εντοπισμός προβλημάτων εφαρμογής και εκμετάλλευσή τους.

Συντονιστής μαθήματος: [Κώστας Πατσάκης](#)

CDS114: Προστασία Κρίσιμων Υποδομών

(ECTS: 3)

Εισαγωγή στα κρίσιμα συστήματα και υποδομές (πρότυπα, μέθοδοι, κανονισμοί). Ανάλυση εξαρτήσεων για κρίσιμες υποδομές (διάδοση κινδύνων/απειλών, αλυσιδωτές επιθέσεις, μοντέλα με βάση το χρόνο). Ανθεκτικότητα σε υποδομές ζωτικής σημασίας (ανθεκτικότητα μέσω σχεδιασμού, ευρωστία, πλεονασμός, αποκατάσταση). Μελέτες περιπτώσεων και παραδείγματα από τον πραγματικό κόσμο σχετικά με επιθέσεις και άμυνες σε κρίσιμες υποδομές.

Συντονιστής μαθήματος: [Παναγιώτης Κοτζανικολάου](#)

ΔΕΥΤΕΡΟ ΕΞΑΜΗΝΟ:

CDS201: Έλεγχος Εισβολών Δικτύων και Συστημάτων

(ECTS: 6, Υποχρεωτικό)

Αυτό το μάθημα είναι μια εισαγωγή στη διαδικασία του “ethical hacking”, γνωστή και ως “δοκιμή διείσδυσης” (penetration testing). Το μάθημα είναι ιδιαίτερα πρακτικό με εργαστήρια, χωρίς όμως να παραμελεί τη θεωρία. Κατά τη διάρκεια του μαθήματος θα προσομοιώσουμε πραγματικές επιθέσεις σε ένα δίκτυο, μια εφαρμογή ή ένα σύστημα που έχει ευπάθειες και αδυναμίες. Στόχος του μαθήματος είναι η κατανόηση της διαδικασίας επίθεσης και των απειλών στον κυβερνοχώρο, προκειμένου να προστατεύονται αποτελεσματικά πολύπλοκα δίκτυα και συστήματα, εντοπίζοντας λανθασμένες ρυθμίσεις, αδυναμίες και ευπάθειες. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Εισαγωγή στη μεθοδολογία δοκιμής διείσδυσης
- Τεχνικές αναγνώρισης
- Τεχνικές σάρωσης
- Τεχνικές απόκτησης αρχικής πρόσβασης (Εκμετάλλευση, Brute forcing, επίθεση από την πλευρά του πελάτη)
- Διατήρηση της πρόσβασης (Trojans, rootkits, back doors)
- Τεχνικές παράκαμψης AV, EDR
- Post τεχνικές εκμετάλλευσης
- Πλευρική κίνηση
- Περιστροφή δικτύου
- Κάλυψη διαδρομών

Εργαστήρια: Θα καλύψουμε τα εργαλεία και τις τεχνικές που χρησιμοποιούν οι σημερινοί επαγγελματίες ελεγκτές διείσδυσης (penetration testers).

Συντονιστής μαθήματος: [Παναγιώτης Κοτζανικολάου](#)

CDS202: Ανάλυση Ψηφιακών Πειστηρίων

(ECTS: 3, Υποχρεωτικό)

Το μάθημα Ανάλυση Ψηφιακών Πειστηρίων (Digital Forensics) επικεντρώνεται στην ανάπτυξη ικανοτήτων χειρισμού περιστατικών και ψηφιακής εγκληματολογίας που καλύπτουν τα λειτουργικά συστήματα Windows και Linux. Το μάθημα καλύπτει όλες τις βασικές πληροφορίες που αφορούν τον ορθό εντοπισμό, την αντιμετώπιση, τον μετριάσμό και την ανάκαμψη από περιστατικά ασφάλειας στον κυβερνοχώρο. Πρόκειται για ένα πλήρως τεχνικό μάθημα με εργαστήρια. Σκοπός αυτού του μαθήματος είναι, αφού κατανοήσετε τη διαδικασία επίθεσης, να μάθετε πώς να

αντιμετωπίζετε κυβερνοεπιθέσεις σε λειτουργικά συστήματα windows και linux. Θα μάθετε τη διαδικασία αντιμετώπισης/διαχείρισης περιστατικών και τη διαδικασία ψηφιακής εγκληματολογίας. Θα επικεντρωθούμε στην ψηφιακή εγκληματολογία για Windows, Linux και δίκτυα. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Διαδικασία χειρισμού περιστατικών
- Εγκληματολογία των Windows (εγκληματολογία μνήμης, εγκληματολογία μητρώου, ανάλυση συστήματος file, εγκληματολογία εφαρμογών)
- Ανάλυση αρχείων καταγραφής
- Εγκληματολογία Linux
- Εγκληματολογία δικτύου

Εργαστήρια: Θα καλύψουμε τα εργαλεία και τις τεχνικές που χρησιμοποιούν οι σημερινοί ειδικοί χειρισμού περιστατικών και εγκληματολόγοι στον πραγματικό κόσμο. Τα εργαστήρια περιέχουν: Συλλογή πληροφοριών, ανάλυση μνήμης, ανάλυση μητρώου και συστήματος αρχείων, εγκληματολογία δικτύου και επίσης εγκληματολογία Linux.

Συντονιστής μαθήματος: [Κώστας Πατσάκης](#)

CDS203: Ανάλυση κακόβουλου λογισμικού

(ECTS: 3, Υποχρεωτικό)

Το μάθημα αυτό επικεντρώνεται σε μεθόδους ανάλυσης κακόβουλου λογισμικού (malware analysis) όπως trojans, rootkits, ransomware κ.λπ.. Αυτό περιλαμβάνει την ανάλυση πραγματικού και πρόσφατου κακόβουλου λογισμικού σε πραγματικό χρόνο και σε ζωντανά περιβάλλοντα. Μελετάμε εργαλεία συλλογής κακόβουλου λογισμικού, τεχνικές για στατική ανάλυση κώδικα, καθώς και δυναμική ανάλυση μέσω disassemblers και debuggers. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Κακόβουλο λογισμικό
- Εξυπηρετητές C&C (πρωτόκολλα και μέθοδοι)
- Συγκάλυψη
- Στατική ανάλυση κακόβουλου λογισμικού
- Δυναμική ανάλυση κακόβουλου λογισμικού
- Μηχανική μάθηση για την ανίχνευση κακόβουλου λογισμικού

Εργαστήρια: Τα εργαστήρια θα καλύψουν πρακτικές πτυχές της ανάλυσης κακόβουλου λογισμικού, όπου οι φοιτητές θα χρησιμοποιήσουν VMs για να εξάγουν χαρακτηριστικά από κακόβουλο λογισμικό και θα αλληλεπιδράσουν με αυτά μέσω

debuggers και sandboxes για να κατανοήσουν πώς λειτουργεί ένα κακόβουλο λογισμικό και πώς μπορεί να αναλυθεί.

Συντονιστής μαθήματος: [Κώστας Πατσάκης](#)

CDS204: Ασφάλεια λογισμικού

(ECTS: 6, Υποχρεωτικό)

Οι εταιρείες και οι οργανισμοί σε όλο τον κόσμο αναγνωρίζουν σήμερα, πολύ περισσότερο από ποτέ άλλοτε, την αξία της ασφάλειας στο λογισμικό. Επιπλέον, οι πωλητές επενδύουν σημαντικά σε διαδικασίες ασφαλείας που θα τους επιτρέψουν να παράγουν λογισμικό που θα πληροί υψηλά πρότυπα ασφαλείας. Το μάθημα αυτό περιγράφει τις θεμελιώδεις αρχές πίσω από την ασφάλεια λογισμικού και εξηγεί την αξία του ασφαλούς λογισμικού σε αξιόπιστες υποδομές ΤΠΕ. Περιγράφει επίσης λεπτομερώς τους βασικούς τύπους τρωτών σημείων λογισμικού και δείχνει πώς αυτά μπορούν να βαθμολογηθούν και να διαχειριστούν ανάλογα με τον αντίστοιχο κίνδυνο.

Μέσω διαλέξεων, εργασιών και εργαστηρίων οι φοιτητές θα μάθουν πώς να εντοπίζουν σφάλματα ασφαλείας τόσο σε λογισμικό για το οποίο έχει διατεθεί ο πηγαίος κώδικας (επισκόπηση κώδικα) όσο και σε λογισμικό όπου ο πηγαίος κώδικας δεν είναι διαθέσιμος (επισκόπηση μαύρου κουτιού). Οι ευπάθειες που μελετώνται σε αυτό το μάθημα προέρχονται από ένα ευρύ πεδίο εφαρμογών, όπως: λογισμικό λειτουργικών συστημάτων, λογισμικό ενσωματωμένων συστημάτων, υπηρεσίες Διαδικτύου, λογισμικό γραφείου, εφαρμογές ιστού και εφαρμογές κινητών τηλεφώνων.

Πεδίο εφαρμογής του μαθήματος: Ο πρωταρχικός στόχος αυτού του μαθήματος είναι η ανάπτυξη των ακόλουθων δεξιοτήτων: η εφαρμογή βέλτιστων πρακτικών ασφαλείας στο υπό ανάπτυξη λογισμικό, ο εντοπισμός θεμάτων ασφαλείας σε λογισμικό ανοικτού και κλειστού κώδικα, η επίδειξη μιας ευπάθειας, η αξιολόγηση μιας ευπάθειας και η διαχείριση των ευπαθειών σε όλες τις φάσεις σχεδιασμού, υλοποίησης και συντήρησης έργων λογισμικού. Οι σπουδαστές θα εισαχθούν επίσης στις πιο σύγχρονες μεθόδους για τον εντοπισμό τρωτών σημείων και στις πρόσφατες τεχνικές για τον προληπτικό μετριασμό των κινδύνων.

Εργαστήρια: Διάφορα εργαλεία για στατική και δυναμική ανάλυση κώδικα (όπως nm, file, objdump, strace, ltrace), εργαλεία εντοπισμού σφαλμάτων (gdb), fuzzing πρωτοκόλλων (peach), fuzzing αρχείων (j0nggfuzz) και ασφάλεια εφαρμογών ιστού (bwapp).

Συντονιστής μαθήματος: [Παναγιώτης Κοτζανικολάου](#)

CDS211: Προηγμένες τεχνολογίες κρυπτογραφίας και ασφάλειας

(ECTS: 3)

Το μάθημα αυτό επικεντρώνεται στην εισαγωγή των φοιτητών στην τεχνολογία blockchain. Αφού παρουσιάσουμε τις βασικές έννοιες πίσω από την αλυσίδα μπλοκ, παρουσιάζουμε τους διάφορους αλγόριθμους συναίνεσης και τη λειτουργικότητα που παρέχεται. Αφού εξερευνήσουμε την ιχνηλασιμότητα σε δημόσιες αλυσίδες μπλοκ, μεταβαίνουμε στην ανάπτυξη έξυπνων συμβολαίων για την ανάπτυξη πρακτικών εφαρμογών σε πραγματικές αλυσίδες μπλοκ. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Εισαγωγή στο blockchain
- Αλγόριθμοι απογραφής (Proof of work, Proof of stake, Byzantine fault tolerance)
- Ιχνηλασιμότητα στην αλυσίδα μπλοκ (εντοπισμός συναλλαγών στην αλυσίδα μπλοκ)
- Ανάπτυξη έξυπνων συμβολαίων στο Ethereum/Hyperledger (θα εξαρτηθεί από το έτος)

Εργαστήρια: Τα εργαστήρια θα επικεντρωθούν κυρίως στην ανάπτυξη έξυπνων συμβολαίων για ευρέως χρησιμοποιούμενες αλυσίδες μπλοκ, όπως το Ethereum και το Hyperledger. Επιπλέον, θα πραγματοποιηθούν εργαστηριακές ασκήσεις για την κατανόηση και τη διερεύνηση των χαρακτηριστικών ιχνηλασιμότητας που επιτρέπουν οι αλυσίδες μπλοκ.

Συντονιστής μαθήματος: [Κώστας Πατσάκης](#)

CDS212: Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας

(ECTS: 3)

Το μάθημα αυτό επικεντρώνεται στη μελέτη ειδικών πτυχών που σχετίζονται με την ασφάλεια πληροφοριών και την προστασία της ιδιωτικής ζωής, με έμφαση σε διατομεακές πτυχές, όπως η οικονομία, η εκπαίδευση, η κατάρτιση, οι νομικές και ρυθμιστικές πτυχές. Ο απώτερος στόχος είναι να εξεταστεί η κυβερνοασφάλεια από μια μικτή κοινωνικο-τεχνική οπτική γωνία. Πιο συγκεκριμένα, το μάθημα αυτό καλύπτει τα ακόλουθα θέματα:

- Οικονομικά της ασφάλειας
- Ασφάλεια στην εκπαίδευση
- Ενημέρωση για την ασφάλεια
- Νομικές και κανονιστικές πτυχές της ασφάλειας και του απορρήτου

Συντονιστής μαθήματος: [Χρήστος Δουληγέρης](#)

CDS212: Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων

(ECTS: 3)

Περιγραφή μαθήματος: Το μάθημα επικεντρώνεται στις ηθικές προκλήσεις της λειτουργίας και της χρήσης του δικτύου και τα ηθικά ζητήματα που σχετίζονται με την επιστήμη των δεδομένων, καθώς και τις νομικές ρυθμίσεις των ζητημάτων αυτών σε εθνικό και διεθνές επίπεδο. Ο απώτερος στόχος του μαθήματος είναι οι μαθητές να αξιολογεί το και να εκτιμήσει τη σοβαρότητα, την πολυπλοκότητα και το ευρύ πεδίο εφαρμογής των ηθικών διλημάτων στον κυβερνοχώρο και να προετοιμάσει τους ολιστικά για τους μελλοντικούς τους ρόλους ως επαγγελματίες της κυβερνοασφάλειας. Ειδικότερα, το μάθημα καλύπτει τα ακόλουθα θέματα:

- Εισαγωγή στην εφαρμοσμένη ηθική – Το ηθικό πλαίσιο της κυβερνοασφάλειας
- Κοινωνία και κυβερνοασφάλεια (Μελέτες περίπτωσης)
- Δίκαιο και δεοντολογία (ιδιωτικότητα, προσωπικά δεδομένα, εμπιστευτικότητα)
- Εθνική, Ευρωπαϊκή και διεθνής νομοθεσία για την ασφάλεια στον κυβερνοχώρο

2) ΑΣΦΑΛΕΙΑ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΕΝΣΩΜΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ (ΑΑΕΣ)

Η κατεύθυνση **Ασφάλεια και αξιοπιστία ενσωματωμένων συστημάτων** επικεντρώνεται στη μελέτη των τελευταίων τεχνολογιών και μεθόδων για τον σχεδιασμό ασφαλών και αξιόπιστων ενσωματωμένων συστημάτων, του Διαδικτύου των Πραγμάτων (IoT) και των υποδομών ζωτικής σημασίας. Το πρόγραμμα έχει σχεδιαστεί προσεκτικά ώστε να παρέχει στους σπουδαστές γνώσεις και δεξιότητες στους τομείς της ασφάλειας και της αξιοπιστίας των υπολογιστικών συστημάτων, συμπεριλαμβανομένων της σχεδίασης ενσωματωμένων συστημάτων, των ασφαλών εφαρμογών IoT, των αξιόπιστων συστημάτων και των κρίσιμων υποδομών, της σχεδίασης αρχιτεκτονικής ασφάλειας, της ασφάλειας λογισμικού, της ασφάλειας υλικού και της αξιοπιστίας ενσωματωμένων συστημάτων. Οι φοιτητές πρέπει να παρακολουθήσουν με επιτυχία έναν αριθμό μαθημάτων που ανέρχονται σε 30 ECTS ανά εξάμηνο. Η κατεύθυνση προσφέρει 5 υποχρεωτικά μαθήματα με 24 ECTS συνολικά στο 1ο εξάμηνο και 3 υποχρεωτικά μαθήματα με 18 ECTS συνολικά στο 2ο εξάμηνο, ενώ οι φοιτητές μπορούν να συμπληρώσουν τις απαιτούμενες ECTS ανά εξάμηνο παρακολουθώντας 1 ή 2 μαθήματα επιλογής ή υποχρεωτικά μαθήματα από άλλες κατευθύνσεις. Το 3ο εξάμηνο είναι αφιερωμένο στη διπλωματική εργασία σε ένα σύγχρονο θέμα στους τομείς της ασφάλειας και της αξιοπιστίας των υπολογιστικών συστημάτων, υπό την επίβλεψη ενός από τους διδάσκοντες της κατεύθυνσης.

ΠΡΩΤΟ ΕΞΑΜΗΝΟ:

CDS103: Σχεδίαση Αρχιτεκτονικών Ασφάλειας

(ECTS: 6, Υποχρεωτικό)

Στόχος αυτού του μαθήματος είναι ο προσδιορισμός και η ανάλυση των βασικών αρχών σχεδιασμού ασφαλών πληροφοριακών συστημάτων. Αυτό επιτυγχάνεται μέσω της εισαγωγής γνωστών βέλτιστων πρακτικών για την εφαρμογή μηχανισμών ασφαλείας και πρωτοκόλλων επικοινωνίας για σύγχρονα συστήματα που βασίζονται κυρίως στην κρυπτογραφία. Οι κύριοι στόχοι του Σχεδιασμού Αρχιτεκτονικής Ασφάλειας είναι:

- Προσδιορισμός των κύριων στοιχείων της σύγχρονης αρχιτεκτονικής των πληροφοριακών συστημάτων.
- Να αποτυπώσει το εύρος και την πολυπλοκότητα των τρωτών σημείων ασφαλείας των πληροφοριακών συστημάτων.
- Καθορισμός των βασικών αρχών ασφαλείας όσον αφορά το σχεδιασμό προηγμένων μηχανισμών και στοιχείων.

Η κατανόηση των σχετικών μοντέλων ασφαλείας που βασίζονται στις παραπάνω βασικές αρχές, η εφαρμογή των οποίων μετριάξει και ελαχιστοποιεί τις απειλές ασφαλείας.

Το μάθημα καλύπτει τους ακόλουθους τομείς:

- Εισαγωγή στην ασφάλεια πληροφοριών
- Απαιτήσεις αρχιτεκτονικής ασφαλείας πληροφοριών
- Η διαδικτυακή πλατφόρμα και οι απειλές της
- Απειλές και επιθέσεις της διαδικτυακής πλατφόρμας
- Σχεδιασμός ασφαλείας κινητών τηλεφώνων
- Σενάρια πραγματικών περιπτώσεων

Εργαστήρια: που έχουν ως κύριο στόχο την εμπέδωση και εφαρμογή όλων των παραπάνω στη διαδικασία σχεδιασμού ασφαλών Πληροφοριακών Συστημάτων.

Συντονιστής μαθήματος: [Χρήστος Δουληγέρης](#)

CDS104: Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων

(ECTS: 3, Υποχρεωτικό)

Εισαγωγή στο Διαδίκτυο των Πραγμάτων (ΔτΠ - IoT). Αρχιτεκτονικές μικροελεγκτών για IoT. Πτυχές συνδεσιμότητας IoT. Προσεγγίσεις σχεδιασμού για ασφαλές ΔτΠ. Υποστήριξη υλικού για την ασφάλεια του ΔτΠ. Μονάδες ασφαλείας υλικού. Ασφαλείς και κρυπτογραφικές υλοποιήσεις για IoT.

Εργαστήρια: Εργαστήρια για το σχεδιασμό ασφαλών εφαρμογών IoT. Υλοποίηση μιας ασφαλούς εφαρμογής IoT.

Συντονιστής μαθήματος: [Αθανάσιος Παπαδημητρίου](#)

CDS105: Σχεδίαση Ενσωματωμένων Συστημάτων

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στα Ενσωματωμένα Συστήματα. Ενσωματωμένες εφαρμογές, προδιαγραφές και απαιτήσεις. Ενσωματωμένες υπολογιστικές πλατφόρμες (CPUs, ASIC, FPGA). Μεθοδολογία σχεδιασμού με FPGA. Εισαγωγή στη VHDL. Μελέτη περίπτωσης: Xilinx Zynq-7000 System-on-Chip.

Εργαστήρια: Εργαστηριακά μαθήματα σχεδιασμού, προσομοίωσης και επαλήθευσης ενσωματωμένων συστημάτων σε FPGA. Χρήση αυτοματοποιημένων εργαλείων σχεδίασης (Vivado) και πλακετών ανάπτυξης FPGA (Zybo boards).

Συντονιστής μαθήματος: [Μιχάλης Ψαράκης](#)

CDS106: Αξιόπιστα Υπολογιστικά Συστήματα

(ECTS: 3, Υποχρεωτικό)

Μοντέλα σφαλμάτων, απειλές ασφάλειας και αστοχίες συστημάτων. Βασικές έννοιες της αξιοπιστίας (αξιοπιστία, διαθεσιμότητα, ασφάλεια, προστασία). Ανοχή σφαλμάτων υλικού και λογισμικού. Αξιολόγηση της αξιοπιστίας (FMEA, πειράματα ακτινοβολίας, έγχυση σφαλμάτων). Πρότυπα αξιοπιστίας.

Μελέτη περίπτωσης: FMEA σε ένα κρίσιμο σύστημα.

Συντονιστής μαθήματος: [Μιχάλης Ψαράκης](#)

CDS107: Αναλυτική Δεδομένων και Μηχανική Μάθηση

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στην ανάλυση δεδομένων (αρχές, αγωγός, προεπεξεργασία). Κοινές μέθοδοι μηχανικής μάθησης (ταξινόμηση, ομαδοποίηση). Νευρωνικά δίκτυα και βαθιά μάθηση. Προηγμένες τεχνικές ομαδοποίησης (DBSCAN, OPTICS κ.λπ.). Εφαρμογές στην εξόρυξη δεδομένων κειμένου/ήχου/βίντεο.

Εργαστηριακές ώρες με Python, R, Spark MLlib.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

ΔΕΥΤΕΡΟ ΕΞΑΜΗΝΟ:**CDS204: Ασφάλεια λογισμικού**

(ECTS: 6, Υποχρεωτικό)

Το μάθημα αυτό περιγράφει τις θεμελιώδεις αρχές της ασφάλεια λογισμικού. Περιγράφει επίσης λεπτομερώς τους βασικούς τύπους τρωτών σημείων λογισμικού και δείχνει πώς αυτά μπορούν να βαθμολογηθούν και να διαχειριστούν ανάλογα με τον αντίστοιχο κίνδυνο. Μέσω διαλέξεων, εργασιών και εργαστηρίων οι φοιτητές θα μάθουν πώς να εντοπίζουν σφάλματα ασφαλείας τόσο σε λογισμικό για το οποίο έχει

διατεθεί ο πηγαίος κώδικας (επισκόπηση κώδικα) όσο και σε λογισμικό όπου ο πηγαίος κώδικας δεν είναι διαθέσιμος (επισκόπηση μαύρου κουτιού). Οι ευπάθειες που μελετώνται σε αυτό το μάθημα προέρχονται από ένα ευρύ πεδίο εφαρμογών, όπως: λογισμικό λειτουργικών συστημάτων, λογισμικό ενσωματωμένων συστημάτων, υπηρεσίες Διαδικτύου, λογισμικό γραφείου, εφαρμογές ιστού και εφαρμογές κινητών τηλεφώνων.

Πεδίο εφαρμογής του μαθήματος: Ο πρωταρχικός στόχος του μαθήματος είναι η ανάπτυξη των ακόλουθων δεξιοτήτων: η εφαρμογή βέλτιστων πρακτικών ασφάλειας στο υπό ανάπτυξη λογισμικό, ο εντοπισμός θεμάτων ασφάλειας σε λογισμικό ανοικτού και κλειστού κώδικα, η επίδειξη μιας ευπάθειας, η αξιολόγηση μιας ευπάθειας και η διαχείριση των ευπαθειών σε όλες τις φάσεις σχεδιασμού, υλοποίησης και συντήρησης έργων λογισμικού. Οι σπουδαστές θα εισαχθούν επίσης στις πιο σύγχρονες μεθόδους για τον εντοπισμό τρωτών σημείων και στις πρόσφατες τεχνικές για τον προληπτικό μετριασμό των κινδύνων.

Εργαστήρια: Διάφορα εργαλεία για στατική και δυναμική ανάλυση κώδικα (όπως nm, file, objdump, strace, ltrace), εργαλεία εντοπισμού σφαλμάτων (gdb), fuzzing πρωτοκόλλων (peach), fuzzing αρχείων (jonggfuzz) και ασφάλεια εφαρμογών ιστού (bwarpp).

Συντονιστής μαθήματος: [Παναγιώτης Κοτζανικολάου](#)

CDS205: Ασφάλεια υλικού

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στην ασφάλεια υλικού. Ασφαλή ενσωματωμένα συστήματα. Επιθέσεις έγχυσης σφαλμάτων – δυσλειτουργίες τάσης και ρολογιού. Επιθέσεις ανάλυσης πλευρικών καναλιών – ανάλυση ισχύος και ηλεκτρομαγνητική ανάλυση. Αντιμετώπιση επιθέσεων υλικού – έγχυση σφαλμάτων: πλεονασμός υλικού και χρόνου, κώδικες ανίχνευσης σφαλμάτων – ανάλυση πλευρικών καναλιών: με βάση την απόκρυψη και τη συγκάλυψη. Φυσικά μη-κλωνοποιήσιμες συναρτήσεις (Physically Unclonable Functions – PUF).

Εργαστήρια: Εργαστήρια για επιθέσεις Fault Injection και επιθέσεις Side Channel Analysis. Αξιολόγηση υλοποιήσεων ασφαλών ενσωματωμένων συστημάτων. Σχεδιασμός αντιμέτρων.

Συντονιστής μαθήματος: [Αθανάσιος Παπαδημητρίου](#)

CDS206: Αξιοπιστία Ενσωματωμένων Συστημάτων

(ECTS: 6, Υποχρεωτικό)

Ανοχή σφαλμάτων υλικού. Τεχνικές πλεονασμού (διπλά συστήματα- τριπλός αρθρωτός πλεονασμός). πλεονασμός πληροφοριών (κώδικες ανίχνευσης και διόρθωσης σφαλμάτων). Επιπτώσεις ακτινοβολίας σε ενσωματωμένα συστήματα (SEEs, SEUs, SEFIs). Μεθοδολογίες ανοχής σφαλμάτων για ενσωματωμένους μικροεπεξεργαστές (Ανοχή σφαλμάτων υλικού με εφαρμογή λογισμικού, μνήμες ECCs, κλειδώματα πυρήνα, checkpointing, χρονοδιακόπτες watchdog) και SRAM FPGAs (TMR, scrubbing). Τεχνικές έγχυσης σφαλμάτων (με βάση την προσομοίωση, FPGA) για την ανάλυση αξιοπιστίας.

Εργαστήρια: SRAM FPGAs. Χρήση εμπορικών εργαλείων σχεδίασης (Vivado, Synplify), πλατφορμών έγχυσης σφαλμάτων ανοικτού κώδικα και πλακετών ανάπτυξης FPGA (πλακέτες Zybo).

Συντονιστής μαθήματος: [Μιχάλης Ψαράκης](#)

3) ΕΠΙΧΕΙΡΗΜΑΤΙΚΗ ΑΝΑΛΥΤΙΚΗ ΚΑΙ ΑΝΑΛΥΤΙΚΗ ΔΕΔΟΜΕΝΩΝ (ΕΑΑΔ)

Η κατεύθυνση **Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων** αποτελείται από μια σειρά προηγμένων μαθημάτων στον τομέα της Επιστήμης Δεδομένων. Για να εκπληρώσουν τις υποχρεώσεις τους, οι φοιτητές πρέπει να παρακολουθήσουν επιτυχώς έναν αριθμό μαθημάτων που ανέρχεται σε 30 ECTS ανά εξάμηνο. Κατά τη διάρκεια του 1ου και 2ου εξαμήνου, η κατεύθυνση προσφέρει 6 μαθήματα σε κάθε κατεύθυνση, ενώ οι φοιτητές μπορούν επίσης να επιλέξουν 1-2 μαθήματα από άλλες κατευθύνσεις. Το 3ο εξάμηνο είναι αφιερωμένο στη διπλωματική εργασία σε ένα σύγχρονο θέμα της Επιστήμης Δεδομένων, υπό την επίβλεψη ενός από τους διδάσκοντες της κατεύθυνσης.

ΠΡΩΤΟ ΕΞΑΜΗΝΟ:

CDS107: Αναλυτική Δεδομένων και Μηχανική Μάθηση

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στην ανάλυση δεδομένων (αρχές, αγωγός, προεπεξεργασία). Κοινές μέθοδοι μηχανικής μάθησης (ταξινόμηση, ομαδοποίηση). Νευρωνικά δίκτυα και βαθιά μάθηση. Προηγμένες τεχνικές ομαδοποίησης (DBSCAN, OPTICS κ.λπ.). Εφαρμογές στην εξόρυξη δεδομένων κειμένου/ήχου/βίντεο.

Εργαστηριακές ώρες με Python, R, Spark MLlib.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

CDS108: Διοικητική Πληροφοριακών Συστημάτων

(ECTS: 3, Υποχρεωτικό)

Διαχείριση έργων πληροφορικής (προγραμματισμός έργων, προγραμματισμός πόρων, προγραμματισμός κόστους). Οικονομικά της Διαχείρισης Έργων. Διαχείριση της ασφάλειας των πληροφοριακών συστημάτων, καινοτόμες ηλεκτρονικές υπηρεσίες και υπηρεσίες εφοδιαστικής αλυσίδας. Διακυβέρνηση της ασφάλειας των επιχειρήσεων και των έξυπνων οικοσυστημάτων.

Εργαστηριακές ώρες με το MS Project, εργαλεία διαχείρισης κινδύνων ανοικτού κώδικα.

Συντονιστής μαθήματος: [Δημήτρης Αποστόλου](#)

CDS109: Τεχνικές βελτιστοποίησης

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στη μαθηματική μοντελοποίηση και βελτιστοποίηση. Βελτιστοποίηση με περιορισμούς. Κυρτά και μη κυρτά κύτταρα δεδομένων. Τεχνικές βελτιστοποίησης για την ανάλυση δεδομένων (μοντέλα και εφαρμογές ανάλυσης συνόρων και περιβάλλουσας ανάλυσης δεδομένων). Ανάλυση περιβάλλουσας δεδομένων με δεδομένα ροής.

Εργαστηριακές ώρες με EMS, LP Solve.

Συντονιστής μαθήματος: [Δημήτρης Δεσπότης](#)

CDS110: Διαχείριση μεγάλων δεδομένων

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή - ανασκόπηση των σχεσιακών και αντικειμενοσχεσιακών βάσεων δεδομένων. Σύγχρονες τάσεις στο σχεδιασμό βάσεων δεδομένων. Μη παραδοσιακοί τύποι δεδομένων (κείμενο, πολυμέσα, χωρικές πληροφορίες). Μη παραδοσιακή αρχιτεκτονική βάσεων δεδομένων (δίκτυα αισθητήρων, ροές δεδομένων, καταμεμημένες, στο σύννεφο). Η εποχή των “μεγάλων δεδομένων” (αρχιτεκτονική MapReduce κ.λπ.).

Εργαστηριακές ώρες με PostgreSQL, MongoDB, Spark (Batch Processing, Streaming, MLib).

Συντονιστής μαθήματος: [Γιάννης Θεοδωρίδης](#)

CDS115: Βαθιά Μηχανική Μάθηση

(ECTS: 3, Υποχρεωτικό)

Το μάθημα παρουσιάζει κοινές και σύγχρονες αρχιτεκτονικές βαθιών νευρωνικών δικτύων, όπως: Συνελκτικές αρχιτεκτονικές, Αναδρομικά Νευρωνικά Δίκτυα,

μηχανισμοί προσοχής και μετασχηματιστές. Επιπλέον, το μάθημα συζητά έννοιες και ζητήματα που σχετίζονται με την εκπαίδευση και είναι ζωτικής σημασίας για την απόκτηση μιας σταθερής κατανόησης των υποκείμενων αρχών των πιο σημαντικών διαδικασιών εκπαίδευσης, όπως η μηχανική του αλγορίθμου backpropagation, ο συντονισμός των παραμέτρων και τα ζητήματα σύγκλισης/υπερπροσαρμογής. Το μάθημα εξελίσσεται σε πέντε διαλέξεις και η πρόοδος των φοιτητών αξιολογείται μέσω ενός ομαδικού έργου.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

CDS111: Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής

(ECTS: 3)

Επιχειρηματική αναλυτική με Python (επεξεργασία και αποθήκευση δεδομένων, χρήση αλγορίθμων μηχανικής μάθησης και βελτιστοποίησης, οπτικοποίηση των αποτελεσμάτων). Μέθοδοι, αλγόριθμοι και μελέτες περιπτώσεων επιχειρηματικής ανάλυσης για τη διαχείριση και βελτιστοποίηση χαρτοφυλακίου. Μέθοδοι, αλγόριθμοι και μελέτες περιπτώσεων για την επιχειρηματική ανάλυση στη βιομηχανία 4.0.

Εργαστηριακές ώρες με Pyomo (γλώσσα μοντελοποίησης βελτιστοποίησης), SymPy (εκτέλεση συμβολικών μαθηματικών υπολογισμών), Gurobi Optimizer (επιλυτής μαθηματικού προγραμματισμού).

Συντονιστής μαθήματος: [Δημήτρης Αποστόλου](#)

CDS112: Αλγόριθμοι και πολυπλοκότητα

(ECTS: 3)

Βασικές τεχνικές σχεδιασμού και ανάλυσης αλγορίθμων. Κατηγορίες πολυπλοκότητας. Αλγόριθμοι για υπολογιστικά δυσεπίλυτα προβλήματα. Στοιχεία αλγοριθμικής θεωρίας παιγνίων. Σχεδιασμός αλγορίθμων με βάση τη μηχανική μάθηση.

Συντονιστής μαθήματος: [Χαράλαμπος Κωνσταντόπουλος](#)

ΔΕΥΤΕΡΟ ΕΞΑΜΗΝΟ:

CDS207: Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής

(ECTS: 6, Υποχρεωτικό)

Ανάλυση διακύμανσης (ANOVA). Ανάλυση παλινδρόμησης. Ανάλυση κύριων συνιστωσών, ανάλυση παραγόντων. Κυρτή βελτιστοποίηση. Ακέραιος

προγραμματισμός και συνδυαστική βελτιστοποίηση. Μη γραμμικός προγραμματισμός (ευρετικές μέθοδοι, παραμετρικές τεχνικές, αλγόριθμοι προσέγγισης). Δυναμικός προγραμματισμός.

Εργαστηριακές ώρες με MATLAB.

Συντονιστής μαθήματος: [Γρηγόρης Κορωνάκος](#)

CDS208: Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων

(ECTS: 3, Υποχρεωτικό)

Έννοιες νευρωνικών δικτύων (perceptron, feed-forward δίκτυα, συναρτήσεις κόστους, εκπαίδευση και επικύρωση). Αρχιτεκτονικές βαθιών NN (MLPs, Convolutional, Recurrent, κ.λπ.). Εφαρμογές στις επιχειρήσεις και στην ανάλυση δεδομένων. Εφαρμογές στην κυβερνοασφάλεια και τα ενσωματωμένα συστήματα.

Εργαστηριακές ώρες με Tensorflow, Keras, PyTorch.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

CDS209: Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας

(ECTS: 3, Υποχρεωτικό)

Μοντέλα γεωγραφικών πληροφοριών και τεχνικές αναπαράστασης. Συστήματα διαχείρισης χωρικών βάσεων δεδομένων (λογικό – φυσικό επίπεδο). Ανάλυση γεωχωρικών δεδομένων (κατανόηση, προεπεξεργασία, αποθήκευση, ανακάλυψη γνώσης, οπτικοποίηση). Επεξεργασία και ανάλυση δεδομένων κινητικότητας. Πρόκληση Επιστήμης Δεδομένων (Kaggle).

Εργαστηριακές ώρες με PostGIS, Apache Sedona (πρώην GeoSpark), Python (GeoPandas, MovingPandas).

Συντονιστής μαθήματος: [Γιάννης Θεοδωρίδης](#)

CDS210: Οπτική Ανάλυση Δεδομένων

(ECTS: 6, Υποχρεωτικό)

Εισαγωγή στην οπτικοποίηση δεδομένων και πληροφοριών. Διαδικασία και μοντέλα σχεδιασμού οπτικοποίησης δεδομένων – Οπτική επίλυση προβλημάτων. Οπτικοποίηση μοτίβων με την πάροδο του χρόνου, οπτικοποίηση αναλογιών, οπτικοποίηση γραφημάτων και δικτύων, οπτικοποίηση γεωγραφικών δεδομένων σε

χάρτες. Διαδραστικές τεχνικές οπτικοποίησης. Συστήματα και τεχνικές οπτικοποίησης για μεγάλα δεδομένα και τεχνητή νοημοσύνη.

Εργαστηριακές ώρες με JS (D3, ChartJS, HighCharts), Python (Matplotlib, Plotly), R (ggplot2).

Συντονιστής μαθήματος: [Γιώργος Παπαστεφανάτος](#)

CDS213: Αναλυτική Γράφων και Δικτύων

(ECTS: 3)

Εισαγωγή. Θεωρητικά μέτρα κεντρικότητας γραφημάτων. Αλγόριθμοι ανίχνευσης κοινοτήτων. Μοντέλα εξέλιξης δικτύων. Δίκτυα συν-συγγραφής. Twitter streaming API. Ανάλυση συναισθήματος. Μοντέλα διαμόρφωσης γνώμης.

Εργαστηριακές ώρες με MATLAB, Python.

Συντονιστής μαθήματος: [Διονύσιος Σωτηρόπουλος](#)

CDS214: Αναλυτική Χρονοσειρών και Πρόβλεψη

(ECTS: 3)

Εισαγωγή – βασικές έννοιες των χρονοσειρών. Συνήθη μοντέλα χρονολογικών σειρών (γραμμικά, αυτοπαλινδρομούμενα, ARMA, ARIMA κ.λπ.). Πρόβλεψη με νευρωνικά δίκτυα (π.χ. μοντέλα LSTM). Επιλεγμένες προηγμένες μέθοδοι (π.χ. Prophet του Facebook). Επικύρωση προβλέψεων και μέτρα ποιότητας. Πρόκληση Επιστήμης Δεδομένων (Kaggle).

Εργαστηριακές ώρες με R, Python (scikit-learn), TensorFlow (Keras), PyTorch.

Συντονιστής μαθήματος: [Άγγελος Πικράκης](#)

12. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Με την ολοκλήρωση του ΠΜΣ αναμένεται οι απόφοιτοι/απόφοιτες να έχουν αποκτήσει τις εξής γενικές ικανότητες, γνωστικές ικανότητες, γνώσεις και λοιπές δεξιότητες.

1) ΓΕΝΙΚΕΣ ΙΚΑΝΟΤΗΤΕΣ

Οι απόφοιτοι του ΠΜΣ θα είναι σε θέση να:

- Κατέχουν πολύ εξειδικευμένες γνώσεις σχετικά με τις αρχές της κυβερνοασφάλειας της ασφάλειας υπολογιστικών, πληροφοριακών και επικοινωνιακών συστημάτων, της επιχειρηματικής αναλυτικής και της αναλυτικής δεδομένων.
- Διαμορφώνουν επιστημονικά θεμελιωμένες και καινοτόμες λύσεις στην περιοχή της κυβερνοασφάλειας της ασφάλειας υπολογιστικών, πληροφοριακών και επικοινωνιακών συστημάτων, της επιχειρηματικής αναλυτικής και της αναλυτικής δεδομένων.
- Κατανοούν τις βασικές αρχές των τεχνολογικών, διοικητικών και ηθικών πτυχών της υλοποίησης έργων πληροφορικής και τηλεπικοινωνιών.
- Εφαρμόζουν τις γνώσεις που αποκόμισαν και τις δεξιότητες που ανέπτυξαν κατά τη διάρκεια του προγράμματος στην ανάλυση και την επίλυση προβλημάτων με βάση διαθεματικά, τεχνολογικά και κοινωνικά κριτήρια, μέσω διεπιστημονικής προσέγγισης και βάσει επιστημονικής/ επαγγελματικής δεοντολογίας.
- Σχεδιάζουν, αναπτύσσουν και διεξάγουν/ διεκπεραιώνουν έργα, ανεξάρτητα ή σε συνεργασία.
- Συλλέγουν, αξιολογούν, επεξεργάζονται, επικοινωνούν και χρησιμοποιούν δεδομένα/ πληροφορίες καθώς και αξιολογούν με κριτική προσέγγιση μεθόδους, τεχνικές και αποτελέσματα με σκοπό τη βελτίωση της διαδικασίας λήψης αποφάσεων και επιλογής ενεργειών.
- Συνεχίσουν τις σπουδές τους στον υψηλότερο ακαδημαϊκό κύκλο επιπέδου 8.

2) ΓΝΩΣΕΙΣ

Οι απόφοιτοι/απόφοιτες του ΠΜΣ:

στην ειδίκευση **“Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων”**

1. Αντιλαμβάνονται σε βάθος και αξιοποιούν τις απαραίτητες θεωρητικές και πρακτικές γνώσεις για την ανάλυση, τον σχεδιασμό, τη διαμόρφωση και την υλοποίηση τεχνολογιών ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. *(Ενδεικτικά μαθήματα: Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Εφαρμοσμένη Κρυπτογραφία, Ασφάλεια Λογισμικού, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας)*
2. Διαθέτουν ευρεία γνώση τεχνολογιών και εργαλείων ασφάλειας δικτύων και επικοινωνιών, διοίκησης ασφάλειας συστημάτων, εφαρμοσμένης κρυπτογραφίας, ελέγχου και πρόληψης εισβολών δικτύων και συστημάτων, ασφάλειας λογισμικού και ανάλυσης ψηφιακών πειστηρίων και κακόβουλου λογισμικού. *(Ενδεικτικά μαθήματα: Ασφάλεια Δικτύων και Επικοινωνιών, Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων, Σχεδίαση Αρχιτεκτονικών ασφάλειας, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Εφαρμοσμένη Κρυπτογραφία, Έλεγχος Εισβολών Δικτύων και Συστημάτων, Ανάλυση Ψηφιακών Πειστηρίων, Ανάλυση Κακόβουλου Λογισμικού, Ασφάλεια Λογισμικού)*
3. Η εξειδικευμένη γνώση που αποκτούν συνιστά τη βάση για πρωτότυπη σκέψη, καθώς και για ερευνητική και επαγγελματική δραστηριότητα. *(Ενδεικτικά μαθήματα: Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων)*
4. Διαθέτουν ευρύ επιστημονικό υπόβαθρο και ικανότητα συνδυασμού γνώσεων από τους τομείς της κυβερνοασφάλειας και της επιστήμης δεδομένων. *(Ενδεικτικά μαθήματα: Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Αλγόριθμοι και Πολυπλοκότητα, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Προστασία Κρίσιμων Υποδομών)*
5. Διαθέτουν αυξημένη κριτική αντίληψη της εξελικτικής δυναμικής και των θεμάτων αιχμής του γνωστικού τους πεδίου. *(Ενδεικτικά μαθήματα: Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας)*

στην ειδίκευση **“Ασφάλεια και Αξιοπιστία Ενσωματωμένων Συστημάτων”**

1. Αντιλαμβάνονται σε βάθος και αξιοποιούν τις απαραίτητες θεωρητικές και πρακτικές γνώσεις για την ανάλυση, τον σχεδιασμό, τη διαμόρφωση και την υλοποίηση τεχνολογιών ασφάλειας υπολογιστικών συστημάτων και υποδομών. *(Ενδεικτικά μαθήματα: Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων, Ασφάλεια Λογισμικού, Ασφάλεια Υλικού)*
2. Διαθέτουν ευρεία γνώση τεχνολογιών και εργαλείων ασφάλειας ενσωματωμένων συστημάτων, ασφάλειας στο διαδίκτυο των πραγμάτων, ασφάλειας υλικού, ασφάλειας λογισμικού, αξιοπιστίας υπολογιστικών συστημάτων και ασφάλειας υποδομών. *(Ενδεικτικά μαθήματα: Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων, Σχεδίαση Ενσωματωμένων Συστημάτων, Αξιόπιστα Υπολογιστικά Συστήματα, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Ασφάλεια Λογισμικού, Ασφάλεια Υλικού, Αξιοπιστία Ενσωματωμένων Συστημάτων)*
3. Η εξειδικευμένη γνώση που αποκτούν συνιστά τη βάση για πρωτότυπη σκέψη, καθώς και για ερευνητική και επαγγελματική δραστηριότητα. *(Ενδεικτικά μαθήματα: Σχεδίαση Ενσωματωμένων Συστημάτων, Αξιόπιστα Υπολογιστικά Συστήματα, Αξιοπιστία Ενσωματωμένων Συστημάτων, Προστασία Κρίσιμων Υποδομών)*
4. Διαθέτουν ευρύ επιστημονικό υπόβαθρο και ικανότητα συνδυασμού γνώσεων από τους τομείς της κυβερνοασφάλειας και της επιστήμης δεδομένων. *(Ενδεικτικά μαθήματα: Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Αλγόριθμοι και Πολυπλοκότητα, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη)*
5. Διαθέτουν αυξημένη κριτική αντίληψη της εξελικτικής δυναμικής και των θεμάτων αιχμής του γνωστικού τους πεδίου. *(Ενδεικτικά μαθήματα: Σχεδίαση Ενσωματωμένων Συστημάτων, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Αξιοπιστία Ενσωματωμένων Συστημάτων)*

στην ειδίκευση **“Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων”**

1. Αντιλαμβάνονται σε βάθος και αξιοποιούν τις απαραίτητες θεωρητικές και πρακτικές γνώσεις για τη μελέτη μεθοδολογιών ανάλυσης και διαχείρισης επιχειρηματικών διαδικασιών, αναλυτικής δεδομένων, τεχνικών βελτιστοποίησης και στατιστικών μεθόδων επιχειρηματικής αναλυτικής. (Ενδεικτικά μαθήματα: Διοικητική Πληροφοριακών Συστημάτων, Διαχείριση Μεγάλων Δεδομένων, Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Οπτική Ανάλυση Δεδομένων, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Βαθιά Μηχανική Μάθηση)
2. Διαθέτουν ευρεία γνώση τεχνολογιών και εργαλείων ανάπτυξης πληροφοριακών συστημάτων, επιχειρηματικής αναλυτικής, αναλυτικής δεδομένων, διαχείρισης επιχειρηματικών διαδικασιών, τεχνικών βελτιστοποίησης και στατιστικής επεξεργασίας επιχειρηματικής αναλυτικής. (Ενδεικτικά μαθήματα: Αναλυτική Δεδομένων και Μηχανική Μάθηση, Διοικητική Πληροφοριακών Συστημάτων, Τεχνικές Βελτιστοποίησης, Διαχείριση Μεγάλων Δεδομένων, Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Αλγόριθμοι και Πολυπλοκότητα, Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής, Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Οπτική Ανάλυση Δεδομένων, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Βαθιά Μηχανική Μάθηση)
3. Η εξειδικευμένη γνώση που αποκτούν συνιστά τη βάση για πρωτότυπη σκέψη, καθώς και για ερευνητική και επαγγελματική δραστηριότητα. (Ενδεικτικά μαθήματα: Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Οπτική Ανάλυση Δεδομένων, Αναλυτική Γράφων και Δικτύων)
4. Διαθέτουν ευρύ επιστημονικό υπόβαθρο και ικανότητα συνδυασμού γνώσεων από τους τομείς της κυβερνοασφάλειας και της επιστήμης δεδομένων. (Ενδεικτικά μαθήματα: Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Προστασία Κρίσιμων Υποδομών)
5. Διαθέτουν αυξημένη κριτική αντίληψη της εξελικτικής δυναμικής και των

θεμάτων αιχμής του γνωστικού τους πεδίου. (Ενδεικτικά μαθήματα: Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Οπτική Ανάλυση Δεδομένων, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη)

3) ΔΕΞΙΟΤΗΤΕΣ

Οι απόφοιτοι/απόφοιτες του ΠΜΣ:

στην ειδίκευση **“Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων”**

1. Αναλύουν, σχεδιάζουν και αναπτύσσουν αρχιτεκτονικές ασφάλειας πληροφοριακών και δικτυακών συστημάτων. (Ενδεικτικά μαθήματα: *Ασφάλεια Δικτύων και Επικοινωνιών, Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων, Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Αναλυτική Δεδομένων και Μηχανική Μάθηση*)
2. Βελτιστοποιούν τις απαιτήσεις ασφάλειας κατανεμημένων συστημάτων με τη βοήθεια μεθοδολογιών και τεχνολογιών επιχειρηματικής αναλυτικής. (Ενδεικτικά μαθήματα: *Αναλυτική Δεδομένων και Μηχανική Μάθηση, Ανάλυση Κακόβουλου Λογισμικού*)
3. Εφαρμόζουν με ευχέρεια τις θεωρίες και μεθοδολογίες του γνωστικού τους πεδίου στις έρευνες, μελέτες και εργασίες τους με κριτικό και δημιουργικό τρόπο. (Ενδεικτικά μαθήματα: *Ασφάλεια Δικτύων και Επικοινωνιών, Διοίκηση Ασφάλειας Πληροφοριακών Συστημάτων, Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Έλεγχος Εισβολών Δικτύων και Συστημάτων, Ανάλυση Ψηφιακών Πειστηρίων, Ανάλυση Κακόβουλου Λογισμικού, Ασφάλεια Λογισμικού*)
4. Εφαρμόζουν με πρωτοτυπία τις αποκτηθείσες γνώσεις στην έρευνα, την ανάλυση και την ανάπτυξη καινοτόμων λύσεων σε σύνθετα, διαθεματικά και πρωτοποριακά ζητήματα. (Ενδεικτικά μαθήματα: *Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας*)
5. Είναι σε θέση να αξιολογούν, να ερμηνεύουν και να προωθούν σύγχρονες

επιστημονικές έρευνες και μελέτες συναφείς με το γνωστικό τους πεδίο. (Ενδεικτικά μαθήματα: *Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Αλγόριθμοι και Πολυπλοκότητα, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Προστασία Κρίσιμων Υποδομών*)

6. Αρθρώνουν επαγωγικά με επιστημονικά τεκμηριωμένο τρόπο, λύσεις στα σύνθετα και νέα ζητήματα και διαμορφώνουν έγκυρες κρίσεις λαμβάνοντας υπόψη τις εκάστοτε συναφείς κοινωνικές, οικονομικές, πολιτιστικές και ηθικές διαστάσεις. (Ενδεικτικά μαθήματα: *Αναλυτική Δεδομένων και Μηχανική Μάθηση, Ανάλυση Κακόβουλου Λογισμικού, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων*)

στην ειδίκευση **“Ασφάλεια και Αξιοπιστία Ενσωματωμένων Συστημάτων”**

1. Αναλύουν, σχεδιάζουν και αναπτύσσουν αρχιτεκτονικές ασφάλειας υπολογιστικών συστημάτων και υποδομών. (Ενδεικτικά μαθήματα: *Σχεδίαση Αρχιτεκτονικών Ασφάλειας, Εφαρμογές Ασφάλειας στο Διαδίκτυο των Πραγμάτων, Σχεδίαση Ενσωματωμένων Συστημάτων, Αξιόπιστα Υπολογιστικά Συστήματα, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Προστασία Κρίσιμων Υποδομών*)
2. Βελτιστοποιούν τις απαιτήσεις ασφάλειας υπολογιστικών συστημάτων και υποδομών με τη βοήθεια μεθοδολογιών και τεχνολογιών επιχειρηματικής αναλυτικής και αναλυτικής δεδομένων. (Ενδεικτικά μαθήματα: *Αξιόπιστα Υπολογιστικά Συστήματα, Αναλυτική Δεδομένων και Μηχανική Μάθηση, Ασφάλεια Λογισμικού, Ασφάλεια Υλικού, Αξιοπιστία Ενσωματωμένων Συστημάτων*)
3. Εφαρμόζουν με ευχέρεια τις θεωρίες και μεθοδολογίες του γνωστικού τους πεδίου στις έρευνες, μελέτες και εργασίες τους με κριτικό και δημιουργικό τρόπο. (Ενδεικτικά μαθήματα: *Ασφάλεια Λογισμικού, Ασφάλεια Υλικού, Αξιοπιστία Ενσωματωμένων Συστημάτων*)
4. Εφαρμόζουν με πρωτοτυπία τις αποκτηθείσες γνώσεις στην έρευνα, την ανάλυση και την ανάπτυξη καινοτόμων λύσεων σε σύνθετα, διαθεματικά και πρωτοποριακά ζητήματα. (Ενδεικτικά μαθήματα: *Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Αλγόριθμοι και Πολυπλοκότητα, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και*

Επιστήμης Δεδομένων)

5. Είναι σε θέση να αξιολογούν, να ερμηνεύουν και να προωθούν σύγχρονες επιστημονικές έρευνες και μελέτες συναφείς με το γνωστικό τους πεδίο. (Ενδεικτικά μαθήματα: *Σχεδίαση Ενσωματωμένων Συστημάτων, Αξιοπίστα Υπολογιστικά Συστήματα, Ασφάλεια Λογισμικού, Ασφάλεια Υλικού, Αξιοπιστία Ενσωματωμένων Συστημάτων*)
6. Αρθρώνουν επαγωγικά με επιστημονικά τεκμηριωμένο τρόπο, λύσεις στα σύνθετα και νέα ζητήματα και διαμορφώνουν έγκυρες κρίσεις λαμβάνοντας υπόψη τις εκάστοτε συναφείς κοινωνικές, οικονομικές, πολιτιστικές και ηθικές διαστάσεις. (Ενδεικτικά μαθήματα: *Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων*)

στην ειδίκευση “Επιχειρηματική Αναλυτική και Αναλυτική Δεδομένων”

1. Κατανοούν και εφαρμόζουν μεθόδους διοίκησης ασφάλειας πληροφοριακών συστημάτων. (Ενδεικτικά μαθήματα: *Αναλυτική Δεδομένων και Μηχανική Μάθηση, Διοικητική Πληροφοριακών Συστημάτων, Διαχείριση Μεγάλων Δεδομένων*)
2. Οργανώνουν, διαχειρίζονται και διοικούν έργα με τη χρήση διεθνώς αναγνωρισμένων, αποδεκτών και αποτελεσματικών τεχνικών διοίκησης έργων και μεθοδολογιών βελτιστοποίησης έργων με την εφαρμογή μεθόδων αναλυτικής δεδομένων. (Ενδεικτικά μαθήματα: *Τεχνικές Βελτιστοποίησης, Υπολογιστικά Εργαλεία Επιχειρηματικής Αναλυτικής, Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής, Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Οπτική Ανάλυση Δεδομένων, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Βαθιά Μηχανική Μάθηση*)
3. Εφαρμόζουν με ευχέρεια τις θεωρίες και μεθοδολογίες του γνωστικού τους πεδίου στις έρευνες, μελέτες και εργασίες τους με κριτικό και δημιουργικό

τρόπο. (Ενδεικτικά μαθήματα: Διαχείριση Μεγάλων Δεδομένων, Αλγόριθμοι και Πολυπλοκότητα, Διαχείριση και Αναλυτική Γεωγραφικής Πληροφορίας, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη, Βαθιά Μηχανική Μάθηση)

4. Εφαρμόζουν με πρωτοτυπία τις αποκτηθείσες γνώσεις στην έρευνα, την ανάλυση και την ανάπτυξη καινοτόμων λύσεων σε σύνθετα, διαθεματικά και πρωτοποριακά ζητήματα. (Ενδεικτικά μαθήματα: Εφαρμοσμένη Κρυπτογραφία, Προηγμένες Τεχνολογίες Κρυπτογραφίας και Ασφάλειας, Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Critical Infrastructure Protection)
5. Είναι σε θέση να αξιολογούν, να ερμηνεύουν και να προωθούν σύγχρονες επιστημονικές έρευνες και μελέτες συναφείς με το γνωστικό τους πεδίο. (Ενδεικτικά μαθήματα: Μαθηματικές Μέθοδοι Επιχειρηματικής Αναλυτικής, Βαθιά μάθηση και Εφαρμογές στην Ασφάλεια και στην Αναλυτική Δεδομένων, Αναλυτική Γράφων και Δικτύων, Αναλυτική Χρονοσειρών και Πρόβλεψη)
6. Αρθρώνουν επαγωγικά με επιστημονικά τεκμηριωμένο τρόπο, λύσεις στα σύνθετα και νέα ζητήματα και διαμορφώνουν έγκυρες κρίσεις λαμβάνοντας υπόψη τις εκάστοτε συναφείς κοινωνικές, οικονομικές, πολιτιστικές και ηθικές διαστάσεις. (Ενδεικτικά μαθήματα: Ειδικά Θέματα Ασφάλειας και Ιδιωτικότητας, Νομικά και Ηθικά Θέματα Κυβερνοασφάλειας και Επιστήμης Δεδομένων)

4) ΙΚΑΝΟΤΗΤΕΣ

Οι απόφοιτοι/απόφοιτες του ΠΜΣ:

1. Παρουσιάζουν προβλήματα, ιδέες, λύσεις και τεχνικές πληροφορίες με αποτελεσματικό και παραγωγικό τρόπο, γραπτά αλλά και προφορικά, τόσο σε εξειδικευμένα όσο και σε μη εξειδικευμένα ακροατήρια.
2. Παράγουν τεχνικές αναφορές επί των δραστηριοτήτων που διεκπεραίωσαν και παρουσιάζουν συνόψεις των κυριότερων αποτελεσμάτων σε ομάδες.
3. Συνεχίζουν να αναπτύσσουν με αυτονομία τις γνώσεις και τις ικανότητές τους σε υψηλό επίπεδο.
4. Εφαρμόζουν με επαγγελματισμό τις εξειδικευμένες γνώσεις και ικανότητες που απέκτησαν και αντιμετωπίζουν αποτελεσματικά νέα, διεπιστημονικά ή

απρόβλεπτα ζητήματα.

5. Επιλύουν προβλήματα και λαμβάνουν στρατηγικές αποφάσεις με αφετηρία την επαγωγική σκέψη.



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Κυβερνοασφάλεια και την Επιστήμη Δεδομένων

<https://cybersecdatasci.cs.unipi.gr/>

ΟΔΗΓΟΣ ΣΠΟΥΔΩΝ 2025 - 2026

Πειραιάς, Οκτώβριος 2025