



**Πρώτη ανακοίνωση - Σχέδιο προκήρυξης<sup>1</sup>**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ  
ΑΝΑΠΤΥΞΗ & ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

(Τμήμα Πλήρους Φοίτησης – Ακαδημαϊκό έτος 2020-21)

Το ΠΜΣ στα Πληροφοριακά Συστήματα του Τμήματος Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, το οποίο λειτουργεί από το 1994, **ανασχεδιάστηκε εκ βάθρων και αναβαθμίστηκε** με σκοπό να ανταποκρίνεται πλήρως στις διαρκώς αυξανόμενες, σημερινές και μελλοντικές, ανάγκες της έρευνας και της αγοράς εργασίας.

Το νέο ΠΜΣ θα λειτουργήσει, με **νέο πρόγραμμα μαθημάτων, νέα ονομασία και εξειδικεύσεις-κατευθύνσεις αιχμής**, ήδη από το αμέσως προσεχές ακαδημαϊκό έτος (2020-21). Η νέα ονομασία και οι νέες εξειδικεύσεις που παρέχει το ΠΜΣ είναι:

**Πρόγραμμα Μεταπτυχιακών Σπουδών  
Ανάπτυξη και Ασφάλεια Πληροφοριακών Συστημάτων**

**Κατεύθυνση Α Ανάπτυξη Ευφυών Πληροφοριακών Συστημάτων Μεγάλης Κλίμακας**  
(Intelligent Large-Scale Information Systems Development)

**Κατεύθυνση Β Κυβερνοασφάλεια & Προστασία Ψηφιακών Υποδομών**  
(Cybersecurity & Digital Infrastructures Protection)

Το αναβαθμισμένο ΠΜΣ αποσκοπεί στην κατάρτιση εξειδικευμένων επιστημόνων, εφοδιασμένων με θεωρητικές, αλλά και πρακτικές γνώσεις και δεξιότητες, ικανών να καλύψουν με πλήρη επάρκεια τις ανάγκες επιχειρήσεων και οργανισμών στα πεδία της **ασφάλειας, σχεδιασμού, υλοποίησης και διαχείρισης πληροφοριακών συστημάτων**.

Η αναβάθμιση του ΠΜΣ εγκρίθηκε από τη **Σύγκλητο του ΟΠΑ** (συνεδρίαση 07.05.2020) και η **τελική** προκήρυξη υποβολής αιτήσεων για το ακαδημαϊκό έτος 2020-21 θα αναρτηθεί στην ιστοσελίδα του προγράμματος αφού δημοσιευθεί το αναγκαίο ΦΕΚ. Ο προγραμματισμός της διαδικασίας επιλογής μεταπτυχιακών φοιτητών είναι ο ακόλουθος:

**Φάση 1**

**Υποβολή αιτήσεων** (το αργότερο μέχρι την **Παρασκευή, 26 Ιουνίου**).

**Συνηντεύξεις<sup>2</sup> για την επιλογή υποψηφίων.**

**Επιτυχόντες Φάσης 1** (ανακοίνωση: Μέχρι **13 Ιουλίου**).

<sup>1</sup> Η παρούσα πρώτη ανακοίνωση περιλαμβάνει το **σχέδιο προκήρυξης** του ΠΜΣ. Η **τελική προκήρυξη** - η οποία δεσμεύει τυπικώς το ΟΠΑ - θα αναρτηθεί **μετά την έγκριση** του προγράμματος από το αρμόδιο Υπουργείο (ΥΠ.ΑΙ.Θ).

<sup>2</sup> Οι συνηντεύξεις μπορεί να γίνουν μέσω διαδικτύου, τηλεφωνικά ή με φυσική παρουσία των αιτούντων.

## Φάση 2

**Υποβολή αιτήσεων** (το αργότερο μέχρι τη **Δευτέρα, 14 Σεπτεμβρίου**).

**Συνεντεύξεις<sup>2</sup> για την επιλογή υποψηφίων.**

1. **Επιτυχόντες Φάσης 2** (ανακοίνωση: Μέχρι **21 Σεπτεμβρίου**).

## Φάση 3

**Εγγραφή επιτυχόντων και έναρξη μαθημάτων** (1-12 Οκτωβρίου)

Η παρακολούθηση του ΠΜΣ προϋποθέτει καταβολή τελών φοίτησης. Για το **ακαδημαϊκό έτος 2020-21 τα τέλη φοίτησης** ανέρχονται σε **4.000€** ανά φοιτητή και καταβάλλονται τμηματικά. Υπάρχει δυνατότητα απαλλαγής (οικονομικοί λόγοι) ή παροχής υποτροφίας (λόγω αριστείας), σε περιορισμένο αριθμό δικαιούμενων και με βάση τα εκάστοτε ισχύοντα.

Οι ενδιαφερόμενοι μπορούν να υποβάλλουν, **ήδη από σήμερα**, τα εξής έγγραφα (αν επιθυμούν, μπορούν να τα οριστικοποιήσουν αμέσως μετά την τελική προκήρυξη):

- α. **Έντυπο αίτησης** (συμπληρώνεται στο <https://e-graduate.applications.aueb.gr> και **κατατίθεται εκτυπωμένη**, μαζί με τα άλλα δικαιολογητικά, **και** στη Γραμματεία του ΠΜΣ).
- β. **Πρόσφατη φωτογραφία**, τύπου ταυτότητας.
- γ. **Αντίγραφο πτυχίου** (οι πτυχιούχοι). Οι τελειόφοιτοι πρέπει να υποβάλλουν υπεύθυνη δήλωση του Ν. 1599/86 ότι η αποδοχή της αίτησής τους γίνεται με την αίρεση απόκτησης πτυχίου μέχρι και την εξεταστική περίοδο του **Σεπτέμβρη 2020**.
- δ. **Βεβαίωση ισοτιμίας και αντιστοιχίας πτυχίου (ΔΟΑΤΑΠ)**, από όσους είναι πτυχιούχοι ΑΕΙ εξωτερικού). Η αίτηση προς τον ΔΟΑΤΑΠ δεν υποκαθιστά την απαιτούμενη αναγνώριση, η οποία πρέπει να υποβληθεί μαζί με την αίτηση υποψηφιότητας.
- ε. **Αντίγραφο αναλυτικής βαθμολογίας** όλων των ετών σπουδών.
- στ. **Δύο συστατικές επιστολές**, κατά προτίμηση στο έντυπο που υπάρχει στην ιστοσελίδα του ΠΜΣ.
- ζ. **Αναλυτικό βιογραφικό σημείωμα**, με αναφορές σε τυχόν επιστημονικές εργασίες του υποψηφίου και ενδεχόμενη επαγγελματική εμπειρία.
- η. **Αντίγραφα αποδεικτικών επαγγελματικής προϋπηρεσίας** (προαιρετικά).
- θ. **Σύντομη έκθεση ενδιαφερόντων** (μέχρι 300 λέξεις), στην οποία αναφέρονται οι λόγοι για τους οποίους η/ο υποψήφιος/-ος ενδιαφέρεται για το συγκεκριμένο ΠΜΣ.
- ι. **Αποδεικτικό καλής γνώσης της αγγλικής γλώσσας** (επικυρωμένο αντίγραφο). Η καλή γνώση της γλώσσας αποδεικνύεται με πιστοποιητικό “*First Certificate*” των παν/μί-ων Cambridge ή Michigan ή με αντίστοιχο και ισόκυρο πιστοποιητικό γλωσσομάθειας.

Για επιπλέον πληροφορίες οι ενδιαφερόμενοι μπορούν να απευθύνονται στη **Γραμματεία Μεταπτυχιακών Σπουδών** (Ευελπίδων 47<sup>Α</sup> & Λευκάδος 33, 7<sup>ος</sup> όροφος, Γραφ. 706), **Δευτέρα-Παρασκευή** (11:00-13:00), τηλ. **210-82.03.643**, κα. **Άννα Παπάζογλου**.

(Κενά) υποδείγματα συστατικών επιστολών υπάρχουν στην ιστοσελίδα του ΠΜΣ:

[http://mscis.cs.aueb.gr/el/static/information#application\\_forms](http://mscis.cs.aueb.gr/el/static/information#application_forms)

Για επιπλέον πληροφορίες οι υποψήφιοι μπορούν να επισκέπτονται την ιστοσελίδα του ΠΜΣ:



## Νέα δομή και νέο πρόγραμμα μεταπτυχιακών μαθημάτων

### **A. Κατευθύνσεις μεταπτυχιακών σπουδών**

Το **Δίπλωμα Μεταπτυχιακών Σπουδών** παρέχεται στους απόφοιτους με εξειδίκευση σε μια από τις παρακάτω κατευθύνσεις, σύμφωνα με τα σχετικώς οριζόμενα στον Κανονισμό Μεταπτυχιακών Σπουδών του παρόντος ΠΜΣ:

**Κατεύθυνση A: Ανάπτυξη Ευφύων Πληροφοριακών Συστημάτων Μεγάλης Κλίμακας**  
(Intelligent Large-Scale Information Systems Development)

**Κατεύθυνση B: Κυβερνοασφάλεια & Προστασία Ψηφιακών Υποδομών**  
(Cybersecurity & Digital Infrastructures Protection)

### **B. Πρόγραμμα μεταπτυχιακών μαθημάτων**

Το σύνολο των Πιστωτικών Μονάδων (ΠΜ) του ΠΜΣ ανέρχεται σε **ενενήντα (90)**. Το πρόγραμμα των διδασκόμενων και εξεταζόμενων μαθημάτων είναι το εξής:

| <b>A' Εξάμηνο</b> (κάθε φοιτητής επιλέγει υποχρεωτικά και τα πέντε (5) μαθήματα)   |   | <b>ΠΜ</b> |
|--|---|-----------|
| Συστήματα Ανάλυσης & Διαχείρισης Μεγάλων Δεδομένων   |   | 6         |
| Προηγμένες Μέθοδοι Ανάπτυξης Λογισμικού  |   | 6         |
| Διοίκηση & Τεχνολογίες Κυβερνοασφάλειας  |   | 6         |
| Τεχνολογίες Ψηφιακών Υποδομών  |   | 6         |
| Τεχνολογίες & Υπηρεσίες Διαδικτύου   |   | 6         |
| <b>B' Εξάμηνο</b> (κάθε φοιτητής επιλέγει πέντε (5) μαθήματα. Αν επιθυμεί να επιλέξει κατεύθυνση, τότε πρέπει να επιλέξει τα δύο (2) υποχρεωτικά μαθήματα της κατεύθυνσης, καθώς και τουλάχιστον δύο (2) από τα μαθήματα επιλογής της κατεύθυνσης) |   | <b>ΠΜ</b> |
| <b>Υποχρεωτικά μαθήματα κατευθύνσεων</b>   |   |           |
| Κατεύθυνση A   | Υπηρεσιοστρεφής Ανάπτυξη Λογισμικού σε Υπολογιστικό Νέφος | 6         |
|  | Μοντελοποίηση Συστημάτων & Οργάνωση Γνώσεων               | 6         |
| Κατεύθυνση B   | Ασφάλεια Λογισμικού & Δικτύων                             | 6         |
|  | Εφαρμοσμένη Κρυπτογραφία                                  | 6         |
| <b>Μαθήματα επιλογής κατευθύνσεων</b>  |   |           |
| Κατεύθυνση A   | Βαθιά Μάθηση  | 6         |
|  | Ανάπτυξη Εφαρμογών στον Ιστό                              | 6         |
|  | Ανάπτυξη Εφαρμογών για Κινητές Συσκευές                   | 6         |
|  | Επεξεργασία Φυσικής Γλώσσας                               | 6         |
| Κατεύθυνση B   | Ψηφιακά Πειστήρια   | 6         |
|  | Έλεγχος Ασφάλειας   | 6         |

|   |   |    |
|---|---|----|
|   | Ελεγκτική Πληροφοριακών Συστημάτων                    | 6  |
|   | Αλυσίδες Καταχωρίσεων & Ευφυείς Συμβάσεις             | 6  |
| Κατευθύνσεις A&B  | Έλεγχος, Αξιοπιστία & Διασφάλιση Ποιότητας Λογισμικού | 6  |
|   | Δίκαιο της Πληροφορίας                                | 6  |
|   | Διοίκηση & Διαχείριση Έργων Πληροφορικής              | 6  |
| <b>Γ' Εξάμηνο</b> (κάθε φοιτητής επιλέγει και τα δύο (2)) |   |    |
| Σεμινάριο Ψηφιακής Καινοτομίας & Επιχειρηματικότητας      |   | 6  |
| Εκπόνηση Διπλωματικής Εργασίας                            |   | 24 |

## Γ. Συνοπτική περιγραφή μαθημάτων

### 1. Υποχρεωτικά μαθήματα

#### **Συστήματα Ανάλυσης & Διαχείρισης Μεγάλων Δεδομένων (Big Data Analysis & Management Systems)**

Αποθήκες δεδομένων και Επιχειρηματική Ευφυΐα, τελεστής του Κύβου. Συστήματα διαχείρισης μεγάλων δεδομένων (big data) (Hadoop Map-Reduce, Hive, Apache Spark). Συστήματα διαχείρισης διασυνδεδεμένων δεδομένων και graph databases (Neo4j, Pregel, Spark GraphX). Συστήματα επεξεργασίας ροών δεδομένων (Storm, Kafka, Spark Streaming). Εφαρμογές ανάλυσης μεγάλων δεδομένων: Τεχνικές εξόρυξης γνώσης, ανάλυση ψηφιακών κοινωνικών δικτύων, ανάλυση ροών, τεχνικές μηχανικής μάθησης για επεξεργασία γράφων.

#### **Προηγμένες Μέθοδοι Ανάπτυξης Λογισμικού (Advanced Software Development Methods)**

Μοντέλα και διαδικασίες ανάπτυξης λογισμικού. Ευέλικτες διαδικασίες ανάπτυξης (agile development). Αρχιτεκτονική λογισμικού και αρχιτεκτονικά πρότυπα (architectural patterns). Αντικειμενοστρεφής σχεδίαση και πρότυπα σχεδίασης (design patterns). Διαχείριση εκδόσεων και στρατηγικές ομαδικής ανάπτυξης. Συντήρηση και αναδόμηση λογισμικού (software refactoring). Στρατηγικές διανομής λογισμικού (π.χ. Continuous Delivery). Σύγχρονες πλατφόρμες ανάπτυξης λογισμικού (Github κλπ.).

#### **Τεχνολογίες & Διοίκηση Κυβερνοασφάλειας (Cybersecurity Technologies & Management)**

Εννοιολογική θεμελίωση: Βασικές έννοιες και ορισμοί. Μορφότυποι κυβερνοασφάλειας και τεχνολογικά παραδείγματα. Θεωρία τεσσάρων ασυνεχειών. Κομβικές τεχνολογίες διαχείρισης κυβερνοασφάλειας (αποτίμηση επικινδυνότητας, διαχείριση ψηφιακής ταυτότητας, αντι-ιομορφικό λογισμικό, κρυπτοσυστήματα). Παραδείγματα (paradigms) ΤΠΕ και μορφότυποι κυβερνοασφάλειας. Προστασία ψηφιακών υποδομών (ενέργεια, δίκτυα πληροφορικής κλπ.). Κυβερνοασφάλεια στο (Βιομηχανικό) Διαδίκτυο των Αντικειμένων ((IIoT)). Διοίκηση κυβερνοασφάλειας: Κοινωνικο-πολιτικό συμφραζόμενο, hacking και hacktivism, κυβερνοσυγκρούσεις (cyber warfare), ψευδο-ειδήσεις (fake news), ιδιωτικότητα (privacy) σε ψηφιακά κοινωνικά δίκτυα (open social networks), κρυπτοσυστήματα,

διεθνείς σχέσεις και συγκρούσεις (Enigma machine, Purple Code, Clipper chip κλπ.). Ατομικά δικαιώματα και ελευθερίες: Μέθοδοι και μέσα αντιμετώπισης τεχνολογιών και δράσεων αυταρχισμού και κοινωνικού ελέγχου.

### **Τεχνολογίες Ψηφιακών Υποδομών (Digital Infrastructure Technologies)**

Βασικές θεωρητικές αρχές και έννοιες ψηφιακών υποδομών. Τρέχουσες εξελίξεις και τεχνολογίες ψηφιακών υποδομών: Αισθητήρες (sensors), Διαδίκτυο των Αντικειμένων (IoT), Υπολογιστικό Νέφος (Cloud Computing), Υπολογιστική Ομίχλη (Fog Computing), Υπολογιστικά Συστήματα Υψηλών Επιδόσεων (High Performance Computing), σχεδίαση ψηφιακών υποδομών. Αρχιτεκτονικές ψηφιακών υποδομών, ασφάλεια, διαλειτουργικότητα, επεκτασιμότητα. Ανθεκτικότητα και βιωσιμότητα ψηφιακής υποδομής (resiliency and sustainability). Παρακολούθηση, βελτιστοποίηση και έλεγχος συστημάτων ψηφιακών υποδομών σε πραγματικό χρόνο (real-time monitoring, optimization and control). Υποδομές έξυπνων πόλεων (smart cities). Προβλήματα που αφορούν έξυπνες ψηφιακές υποδομές.

### **Τεχνολογίες & Υπηρεσίες Διαδικτύου (Internet Technologies & Services)**

Επισκόπηση τεχνολογιών και αρχιτεκτονικής του Διαδικτύου. Πρωτόκολλα επιπέδου δικτύου. Τοπικά δίκτυα μεταγωγής, VLAN δίκτυα μεταγωγής ευρείας κλίμακας (MPLS). Πρωτόκολλα και υπηρεσίες επιπέδων εφαρμογής και μεταφοράς. Δίκτυα διανομής περιεχομένου (CDN), ομότιμα δίκτυα (P2P), ροή βίντεο (πχ. Netflix). Δίκτυα κέντρων δεδομένων (DCN). Μετάδοση πολυμεσικής πληροφορίας. Δίκτυα προσδιοριζόμενα με λογισμικό (SDN).

## **2. Σεμινάριο**

### **Σεμινάριο Καινοτομίας & Επιχειρηματικότητας (Digital Innovation & Entrepreneurship Seminar)**

Καινοτομία, δημιουργικότητα και ανάπτυξη-σχεδίαση καινοτόμων ψηφιακών προϊόντων-υπηρεσιών. Στρατηγική αναγνώρισης καινοτομικών τάσεων και τεχνικές δημιουργικότητας. Ανάλυση αγοράς και ανταγωνισμού, σχεδίαση και αξιολόγηση του επιχειρηματικού μοντέλου. Παρουσίαση καινοτόμων μελετών περίπτωσης. Ανάπτυξη πρωτοτύπου (mock-up) και πελατο-κεντρική σχεδίαση. Ανάπτυξη ικανοτήτων παρουσίασης και Pitching. Χρηματοοικονομική ανάλυση για νεοφυείς επιχειρήσεις. Παρακίνηση και διαχείριση ομάδας. Ψηφιακό μάρκετινγκ και πωλήσεις. Νομικός οδηγός για μια καινοτόμο ιδέα. Δυνατότητες χρηματοδότησης, τα μοντέλα μεταφοράς τεχνολογίας. Βιομηχανική ιδιοκτησία.

## **3. Υποχρεωτικά μαθήματα κατευθύνσεων**

### **Υπηρεσιοστρεφής Ανάπτυξη Λογισμικού στο Υπολογιστικό Νέφος (Service Oriented Software Development in the Cloud) (*Κατεύθυνση Α*)**

Λογισμικό ως Υπηρεσία. Αρχιτεκτονικές SOA (Service Oriented Architecture). Υπηρεσίες REST. Αρχιτεκτονική Microservices. Σχεδιαστικά πρότυπα για κλιμακωσιμότητα και ανοχή σε σφάλματα (Event Sourcing, CQRS, Circuit Breaker κλπ). Εποπτεία και διαχείριση υπηρεσιοστρεφών αρχιτεκτονικών. Μεθοδολογία 12 παραγόντων (The Twelve-Factor App). Στρατηγικές και πρακτικές DevOps. Τεχνολογίες εικονικοποίησης: Paravirtualization, translation, containers, unikernels, βασικές τεχνολογίες IaaS, συμβιβασμοί απόδοσης, CAP theorem. Πλατφόρμα ως υπηρεσία: Βασικές τεχνολογίες PaaS. Σύγχρονες τεχνικές ανάπτυξης εφαρμογών (micro services, docker containers/swarms - Kubernetes). Χρήση

στο Υπολογιστικό Νέφος (Cloud Computing). Παραδείγματα με πραγματικούς providers (AWS, Azure κλπ.). Τεχνικές Continuous Integration και Continuous Deployment.

### **Μοντελοποίηση Συστημάτων & Οργάνωση Γνώσεων (Systems Modelling & Knowledge Organization) (Κατεύθυνση Α)**

Παράσταση πληροφορίας. Όψεις και κύκλος ανάπτυξης συστημάτων. Λεξιλογικό, πληροφοριακό και οντολογικό επίπεδο λειτουργίας. Εννοιολογικά μοντέλα. Μηχανισμοί δόμησης, κληρονομικότητα, μετα-μοντέλα. Κανόνες, παράγωγοι τύποι, περιορισμοί ακεραιότητας. Πρακτικές μοντελοποίησης. Περιβάλλοντα και γλώσσες μοντελοποίησης. Ανάλυση και διαχείριση επιχειρησιακών διεργασιών (Business Process Management), περιβάλλοντα BPM. Οντολογίες. Τύποι οντολογιών, δομή οντολογίας. Επιχειρησιακή οντολογία. Υποδείγματα ανάλυσης (model patterns). Συστήματα οργάνωσης γνώσεων. Θεματικοί όροι, θεματικές γλώσσες, αρχεία καθιερωμένων όρων. Ταξινομίες, ταξινομικά συστήματα. Πολυεδρική ταξινόμηση. Θησαυροί όρων, πρότυπο ISO 25964. Στοιχεία παράστασης και διαχείρισης γνώσης στον Ιστό. Μεταδεδομένα, κωδικοποίηση με τη γλώσσα XML, πρότυπο Dublin Core, μορφότυποι εφαρμογών. Γλώσσες παράστασης γνώσης RDF/RDFS, OWL. Πρότυπο SKOS για την κωδικοποίηση θησαυρών. Επερωτήσεις και συλλογισμός.

### **Ασφάλεια Λογισμικού & Δικτύων (Software & Network Security) (Κατεύθυνση Β)**

Θεωρία και τεχνολογίες ασφάλειας δικτύων, λογισμικού (εφαρμογών και λειτουργικών συστημάτων). Ασφάλεια δικτύων: Επιθέσεις και απειλές σε δίκτυα υπολογιστών (πχ. Sniffing, επιθέσεις DNS, ARP Poisoning, (D)DoS). Πρωτόκολλα δικτύωσης και αυθεντικοποίησης (πχ. Kerberos, PAP/CHAP/EAP), SSL, IPsec και ασύρματης ασφάλειας. Ασφάλεια λογισμικού: Υπερχείλιση μνήμης (buffer overflow), επιθέσεις και εκμετάλλευση τρωτοτήτων (Windows, Linux). Εγκατάσταση και παραμετροποίηση τειχών προστασίας (firewall), προηγμένα και ευφυή συστήματα ανίχνευσης/αντιμετώπισης εισβολών (IPS/-IPS), παραδείγματα υπερχείλισης σε πραγματική μνήμη, έλεγχος πρόσβασης, πρωτόκολλα OTP/2FA, ασφάλεια, ανωνυμία, αντιμετώπιση συμπερασμού σε βάσεις δεδομένων, τεχνικές ανωνυμίας/ανωνυμοποίησης/ψευδωνυμοποίησης - χρήση στο Γενικό Κανονισμό Προστασίας Δεδομένων, ιομορφικό λογισμικό και Rootkits, sandboxing/cheat-engines.

### **Εφαρμοσμένη Κρυπτογραφία (Applied Cryptography) (Κατεύθυνση Β)**

Βασικές αρχές, μαθηματικές έννοιες και ορισμοί της Κρυπτολογίας. Μαθηματικό υπόβαθρο (Θεωρία Ομάδων, Πεδία Galois, Αριθμητική Υπολοίπων - Chinese remainder theorem, Κανόνες Shannon). Κλασικά συστήματα (Shift, Affine, Vigenere ciphers), συμμετρική κρυπτογράφηση (μέθοδοι λειτουργίας, DES/3DES, AES-Rijndael) και ασύμμετρη κρυπτογράφηση (RSA, ElGamal, Elliptic Curve). Μηχανισμοί κατακερματισμού (hashing, SH2/SHA3), ψηφιακές υπογραφές, επικυρωμένη ανταλλαγή κλειδιών (Digital Signature Algorithm, blind digital signatures). Μέθοδοι secret sharing, commitment schemes, zero knowledge proofs, multiparty computation, private-information-retrieval. Κρυπτογραφία - εφαρμογές διαδικτυακών παιχνιδιών. Εφαρμογές Κρυπτογραφίας (SSL/TLS, SSH, ToR).

## **4. Μαθήματα επιλογής κατευθύνσεων**

### **Βαθιά Μάθηση (Deep Learning) (Κατεύθυνση Α)**

Εισαγωγή στη μηχανική μάθηση, επιβλεπόμενη μάθηση, μη επιβλεπόμενη μάθηση, ενισχυτική μάθηση (reinforcement learning). Ταξινόμηση με softmax, βελτιστοποίηση με διασταυρωμένη εντροπία, κατάβαση κλίσης, στοχαστική κατάβαση κλίσης. Εισαγωγή στη

βαθιά μάθηση και τα νευρωνικά δίκτυα, πολυ-επίπεδα Perceptrons, προς τα πίσω μετάδοση σφάλματος, το πρόβλημα της παραγωγής που χάνεται, συναρτήσεις ενεργοποίησης. Προχωρημένη βαθιά μάθηση με συνελκτικά νευρωνικά δίκτυα (CNN). Εφαρμογή σε εικόνα και κείμενο. Τεχνικές ομαλοποίησης (regularization), όπως dropout, batch normalization κλπ. Βελτιστοποίηση στη βαθιά μάθηση με στοχαστική κατάβαση κλίσης και προχωρημένους αλγορίθμους (Adagrad, Adam κλπ.). Ανατροφοδοτούμενα νευρωνικά δίκτυα (RNN), μάθηση από ακολουθιακά δεδομένα. Μη επιβλεπόμενη βαθιά μάθηση με variational auto-encoders και GAN. Παραγωγή κειμένου από εικόνες με συνδυασμό CNN και RNN. Εντοπισμός αντικειμένων σε εικόνες, κατακερματισμός εικόνας (image segmentation).

### **Ανάπτυξη Εφαρμογών στον Ιστό (Web Applications Development) (Κατεύθυνση Α)**

Αρχιτεκτονική εφαρμογών Ιστού: Πελάτης και εξυπηρετητής, βασικές τεχνολογίες και πρότυπα. Εμφάνιση: HTML και CSS, προσαρμογή σε διαφορετικές συσκευές. Εισαγωγή στη Javascript, εισαγωγή στο DOM, χειρισμός του DOM με Javascript, επικοινωνία με χρήστη. Εξυπηρετητές Ιστού, NodeJS, ασύγχρονη είσοδος και έξοδος. Διασύνδεση με βάσεις δεδομένων. Αποδοτικότητα (performance) εφαρμογών Ιστού.

### **Ανάπτυξη Εφαρμογών για Κινητές Συσκευές (Mobile Applications Development) (Κατεύθυνση Α)**

Κινητές συσκευές: Υλικό, Λειτουργικό σύστημα. Εισαγωγή στα εργαλεία ανάπτυξης για κινητές συσκευές. Σχεδίαση διεπαφής, υλοποίηση διεπαφής, ιδιαιτερότητες κινητών συσκευών. Υπηρεσίες συστήματος, διασύνδεση εφαρμογών και υπηρεσιών. Αποθήκευση και ανάκληση δεδομένων. Επικοινωνία μέσω δικτύου. Ενημερώσεις και ειδοποιήσεις. Γραφικά, ήχος, βίντεο, απόδοση συσκευών. Διασύνδεση με αισθητήρες. Διαχείριση ενέργειας, καταστάσεις αναμονής. Ασφάλεια εφαρμογών. Δημιουργία πακέτων εγκατάστασης.

### **Επεξεργασία Φυσικής Γλώσσας (Natural Language Processing) (Κατεύθυνση Α)**

Γλωσσικά μοντέλα n-γραμμάτων. Εντροπία, διασταυρωμένη εντροπία, περιπλοκή. Ορθογραφική διόρθωση. Παραστάσεις κειμένων με σάκους λέξεων. Επιλογή και εξαγωγή χαρακτηριστικών. Κατηγοριοποίηση κειμένων με k κοντινότερους γείτονες και Αφελή Bayes. Ομαδοποίηση λέξεων και κειμένων με k-means. Λογιστική παλινδρόμηση, στοχαστική κατάβαση κλίσης, πολυ-επίπεδα Perceptrons, ανάστροφη μετάδοση σφάλματος για κατηγοριοποίηση κειμένων. Προ-εκπαίδευση ενσωματώσεων λέξεων, Word2Vec, FastText. Ανατροφοδοτούμενα νευρωνικά δίκτυα (RNNs), κελιά GRU LSTM, RNN με αυτο-προσοχή, διπλής κατεύθυνσης, στοιβαγμένα, ιεραρχικά RNN και εφαρμογές σε γλωσσικά μοντέλα, κατηγοριοποίηση κειμένων και επισημείωση ακολουθιών. Μοντέλα RNN μετατροπής ακολουθίας σε ακολουθία, μηχανική μετάφραση. Προ-εκπαίδευση γλωσσικών μοντέλων RNN, ELMo. Συνελκτικά νευρωνικά δίκτυα και εφαρμογές στην επεξεργασία κειμένου. Transformers, BERT. Ανάλυση συντακτικών εξαρτήσεων και εξαγωγή σχέσεων με μοντέλα βαθιάς μάθησης. Συστήματα ερωταποκρίσεων για συλλογές εγγράφων.

### **Ψηφιακά Πειστήρια (Digital Forensics) (Κατεύθυνση Β)**

Βασικές έννοιες των ψηφιακών πειστηρίων. Διεθνή πρότυπα και βέλτιστες πρακτικές (ISO 27037, NIST, SANS, ACPO κλπ.). Διαδικασίες αντιμετώπισης περιστατικών ασφάλειας. Διαδικασίες και εργαλεία ανάλυσης και εξέτασης ψηφιακών πειστηρίων. Μεθοδολογία αντιμετώπισης περιστατικών. Διαδικασία συλλογής και κατάσχεσης αποδεικτικών στοιχείων. Τεχνικές συλλογής πειστηρίων από ενεργό υπολογιστή (ανάλυση μνήμης, registry



κλπ.). Τεχνικές συλλογής πειστηρίων από κλειστό υπολογιστή. Τεχνικές και εργαλεία ανάλυσης ψηφιακών πειστηρίων (registry analysis, files systems analysis, internet artefacts, log files κλπ.). Τεκμηρίωση τελικής έκθεσης διερεύνησης ψηφιακών πειστηρίων.

### **Έλεγχος Ασφάλειας (Penetration Testing - Ethical Hacking)**

Βασικές έννοιες κυβερνοεπιθέσεων. Τεχνικές και κατηγορίες επιθέσεων. Διαδικασίες αντιμετώπισης περιστατικών ασφάλειας. Μέθοδοι και εργαλεία τεχνικών ελέγχων τρωτοτήτων (vulnerability assessment) (ZAP, Metasploit, netcat, Ettercap, Wireshark, NetworkMiner, ShodanHQ). Penetration Testing με χρήση Python/Ruby. Οργανωτικά μέτρα προστασίας. Τεχνικά μέτρα προστασίας διαδικτυακών εφαρμογών, δικτύων και ψηφιακών υποδομών. Τεκμηρίωση έκθεσης τεχνικού ελέγχου τρωτοτήτων. OWASP Top 10, OWASP SAMM. Εναλλακτικά εργαλεία (Kali, CANE). Αντίστροφη Μηχανική (reverse engineering), scripting, συγγραφή exploit kits, παραμετροποίηση scripts για παραβίαση περιορισμών σε λειτουργικά συστήματα.

### **Ελεγκτική Πληροφοριακών Συστημάτων (Information Systems Audit) (Κατεύθυνση Β)**

Σημασία, στόχοι και οφέλη του ελέγχου των Πληροφοριακών Συστημάτων (ΠΣ). Είδη ελέγχων ΠΣ. Τομεακά πλαίσια διαχείρισης επιχειρησιακών κινδύνων και η σχέση τους με τον έλεγχο ΠΣ. Η λειτουργία του ελέγχου ΠΣ σε ένα οργανισμό. Σχεδιασμός ελέγχου ΠΣ, πλάνο και έκταση ελέγχου, νομικά και κανονιστικά θέματα. Απαιτούμενες δεξιότητες. Τεχνικά θέματα και μηχανισμοί ελέγχου ΠΣ. Πλαίσια ελέγχου προσανατολισμένα σε πόρους ΠΣ και σε διεργασίες ΠΣ. Σύγκριση και συγκλίσεις προσεγγίσεων. Πρότυπα πλαίσια στο χώρο της Ελεγκτικής ΠΣ. Διαδικασίες ελέγχου ΠΣ. Κατηγοριοποίηση μηχανισμών ελέγχου. Διεξαγωγή ελέγχου ΠΣ. Κατηγοριοποίηση ελέγχων, διαφορές και ομοιότητες. Προγράμματα ελέγχου. Περιορισμοί και κίνδυνοι κατά τον έλεγχο. Έλεγχος και πιστοποίηση συστημάτων και ελεγκτών ΠΣ. Έλεγχος και πιστοποίηση (πρότυπο ISO 27001).

### **Αλυσίδες Καταχωρίσεων και Ευφυείς Συμβάσεις (Blockchains & Smart Contracts) (Κατεύθυνση Β)**

Λειτουργία αλυσίδων καταχωρίσεων (blockchains). Βασικά παραδείγματα (Bitcoin και Ethereum). Βασικές αρχές και κρυπτογραφικά εργαλεία. Ευφυή συμβόλαια (smart contracts) με χρήση Ethereum. Χρήση αλυσίδων καταχωρίσεων στο Διαδίκτυο των Αντικειμένων (IoT). Θέματα ασφάλειας: Decentralized identifiers, verifiable credentials, sidechains. Τεχνολογίες Interledger.

### **Έλεγχος, Αξιοπιστία & Διασφάλιση Ποιότητας Λογισμικού (Software Testing, Reliability & Quality Assurance) (Κατευθύνσεις Α&Β)**

Παράγοντες που επηρεάζουν την ποιότητα λογισμικού. Μετρικές ποσοτικοποίησης ποιότητας λογισμικού παραδοσιακού και αντικειμενοστρεφούς λογισμικού. Περί ελέγχου λογισμικού. Μέθοδοι Τυπικής Επαλήθευσης και Τεχνικές Ελέγχου. Σημασία Συστηματικών Μεθόδων Ελέγχου. Τεχνικές ανάλυσης προγραμμάτων, τεχνικές ελέγχου λογισμικού. Σύγκριση τεχνικών ελέγχου. Εργαλεία γένεσης δεδομένων ελέγχου. Αυτοματοποίηση ελέγχου λογισμικού. Αξιοπιστία λογισμικού. Σύγκριση αξιοπιστίας υλικού-λογισμικού. Ανάπτυξη μοντέλων αξιοπιστίας. Εκτίμηση παραμέτρων μοντέλων και πρόβλεψη επιπέδων αξιοπιστίας. Σύγκριση μοντέλων. Συσχέτιση αξιοπιστίας και τεχνικών ελέγχου για τον τερματισμό του ελέγχου και παράδοση λογισμικού προς χρήση. Εφαρμογή ελέγχου λογισμικού και αξιοπιστίας λογισμικού κρίσιμων συστημάτων. Τρόποι αντιμετώπισης ελέγχου

λογισμικού αντικειμενοστρεφών προγραμμάτων, λογισμικού βάσεων δεδομένων, Γραφικές Διεπαφές (GUI). Εφαρμογές στο Διαδίκτυο (web testing). Νέες μεθοδολογίες (πχ. UML) και προβλήματα.

### **Δίκαιο της Πληροφορίας (Information Law) (Κατευθύνσεις A&B)**

Βασικές έννοιες και χαρακτηριστικά Δικαίου της Πληροφορίας. Προστασία ιδιωτικότητας και προσωπικών δεδομένων: Ευρωπαϊκό και εθνικό νομικό πλαίσιο με έμφαση στην εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Προστασία ιδιωτικότητας και διαχείριση δεδομένων με έμφαση στο Διαδίκτυο των Αντικειμένων (IoT), ανάλυση δεδομένων μεγάλης κλίμακας και Τεχνητή Νοημοσύνη. Ζητήματα e-privacy: Προστασία δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών (υποχρεώσεις παρόχων, δικαιώματα χρηστών, cookies). Ζητήματα διανοητικής ιδιοκτησίας: Προστασία λογισμικού. Βάσεις δεδομένων - Ψηφιακές βιβλιοθήκες. Πνευματική ιδιοκτησία σε ψηφιακά δικτυακά περιβάλλοντα. Παραβατικότητα και Ποινικό Δίκαιο στην Κοινωνία της Πληροφορίας (αδικήματα σχετικά με επεμβάσεις σε πληροφοριακά συστήματα και στο κυβερνοέγκλημα). Νομικά ζητήματα ψηφιακών πειστηρίων.

### **Διοίκηση & Διαχείριση Έργων Πληροφορικής (ICT Project Management) (Κατευθύνσεις A&B)**

Αρχές και μέθοδοι διαχείρισης έργων πληροφορικής, με έμφαση στα έργα ανάπτυξης λογισμικού. Σχεδιασμός, εκτέλεση, έλεγχος και ολοκλήρωση έργου πληροφορικής. Απόκτηση δεξιοτήτων για χρονοπρογραμματισμό έργου, κατάτμηση έργου (tasks ή sprints), καθορισμός κρίσιμων σημείων (milestones) και παραδοτέων του έργου, ανάθεση εργασιών στο ανθρώπινο δυναμικό, προγραμματισμός προϋπολογισμού. Γραφήματα PERT και GANT. Πρότυπο ISO 21500. Μέθοδοι διαχείρισης Waterfall, Lean, CPM, Agile, Scrum, Six Sigma, PMI/ PMBOK, PriSM, PRINCE2, διαφορές, πλεονεκτήματα/μειονεκτήματα, εφαρμοσιμότητα. Προγραμματισμός πόρων έργου (λογισμικού και υλικού), ανάπτυξη και κατανομή ομάδας έργου ανά task/sprint, μετρικές απόδοσης έργου, διαδικασίες ελέγχου αποτελεσμάτων ενδιάμεσων εργασιών και τελικών παραδοτέων. Μέθοδοι ανάλυσης κινδύνων. Προσομοίωση ασκήσεων, διαδικτυακά προγράμματα διαχείρισης έργων (project management & collaboration tools).