ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Εξ Αποστάσεως Πρόγραμμα Μεταπτυχιακών Σπουδών
Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση
(M.Sc. in Advanced Cybersecurity Technologies and Governance)

Οδηγός Σπουδών
του Π.Μ.Σ.
«Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση»
ακαδημαϊκού έτους 2026-2027

Πειραιάς, Μάρτιος 2026

ΠΕΡΙΕΧΟΜΕΝΑ

1 Το Πανεπιστήμιο Πειραιώς 6

1.1 Ιστορία Πανεπιστημίου 6

1.2 Οργανωτική Δομή 7

1.2.1 Πρυτανική Αρχή 7

1.2.2 Οργανόγραμμα 8

2 Το Τμήμα Ψηφιακών Συστημάτων 9

2.1 Αντικείμενο του Τμήματος 9

2.2 Επαγγελματικά Δικαιώματα Αποφοίτων 9

2.3 Διδακτικό Ερευνητικό Προσωπικό 10

2.4 Διοικητικό Προσωπικό 11

2.5 Υλικοτεχνική Υποδομή 12

3 Το Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» 13

3.1 Γνωστικό Αντικείμενο – Στόχος 13

3.2 Μεταπτυχιακός Τίτλος Σπουδών 15

3.3 Δομή και Όργανα του Π.Μ.Σ. 16

3.4 Αριθμός και Κατηγορίες Εισακτέων 18

3.5 Κριτήρια και Διαδικασία Επιλογής Υποψηφίων για τα Π.Μ.Σ. 19

3.6 Αξιολόγηση των υποψηφίων 21

3.7 Τέλη υποβολής υποψηφιοτήτων, φοίτησης και τρόπος καταβολής τους 22

3.8 Εγγραφές μεταπτυχιακών φοιτητών και φοιτητριών 23

3.9 Χρονική Διάρκεια Φοίτησης 23

3.10 Ευρωπαϊκό Σύστημα Μεταφοράς Πιστωτικών Μονάδων 24

3.10.1 Πιστωτικές Μονάδες του Προγράμματος Σπουδών 24

3.10.2 Φόρτος Εργασίας 25

3.10.3 Απόδοση πιστωτικών μονάδων 25

3.10.4 Μεταφορά πιστωτικών μονάδων (ECTS) 25

3.11 Γλώσσα Προγράμματος 25

3.12 Διδακτικό Προσωπικό 26

3.12.1 Διευθυντής του Π.Μ.Σ. 26

3.12.2 Διδάσκοντες και Διδάσκουσες 27

3.13 Επαγγελματική αποκατάσταση αποφοίτων 35

3.14 Ακαδημαϊκό ημερολόγιο....37
3.15 Πρόγραμμα Σπουδών....37
3.15.1 Κατάλογος μαθημάτων ανά ακαδημαϊκό εξάμηνο....38
3.15.1.1 Ακαδημαϊκό Εξάμηνο 1....38
3.15.1.2 Ακαδημαϊκό Εξάμηνο 2....39
3.15.1.3 Ακαδημαϊκό Εξάμηνο 3....39
3.15.2 Περιγραφή μαθημάτων ανά ακαδημαϊκό εξάμηνο....40
3.15.2.1 Ακαδημαϊκό Εξάμηνο 1....40
3.15.2.1.1 Ιδιωτικότητα και Προστασία Δεδομένων (Privacy and Data Protection)....40
3.15.2.1.2 Διακυβέρνηση Κυβερνοασφάλειας (Cybersecurity Governance)....41
3.15.2.1.3 Ασφάλεια Δικτύων (Network Security)....41
3.15.2.1.4 Ασφάλεια Διαδικτύου των Πραγμάτων (IoT Security)....43
3.15.2.2 Ακαδημαϊκό Εξάμηνο 2....45
3.15.2.2.1 Ψηφιακή Ενημερία στον Κυβερνοχώρο (Digital Wellbeing in Cyber-space)....45
3.15.2.2.2 Τεχνικές Δοκιμαστικών Επιθέσεων (Offensive Security)....49
3.15.2.2.3 Ψηφιακή Δικανική (Forensics)....50
3.15.2.2.4 Ασφαλή Αυτόνομα Συστήματα (Secure Autonomous Systems)....51
3.15.2.2.5 Κυβερνοασφάλεια: Λειτουργικές πρακτικές στον εντοπισμό και αντιμετώπιση επιθέσεων (Cybersecurity: Attack, Defence, and Operational Practice)....53
3.15.2.2.6 Κυβερνοασφάλεια σε Βιομηχανικά Περιβάλλοντα (Cybersecurity in Industrial Scenarios)....54
3.15.2.2.7 Κυβερνοασφάλεια στον Πολιτικό Τομέα: Εσωτερικές και Εξωτερικές Διαστάσεις (Cybersecurity in the Political Domain: Internal and External Dimensions)....56
3.15.2.3 Ακαδημαϊκό Εξάμηνο 3....61
3.15.2.3.1 Μεταπτυχιακή Διπλωματική Εργασία (MSc Thesis)....61
3.16 Μαθησιακά Αποτελέσματα....62
3.16.1 Γνώσεις....62
3.16.2 Δεξιότητες....63
3.16.3 Ικανότητες....63
3.17 Εκπόνηση εργασιών....64
3.18 Εκπόνηση Μεταπτυχιακής Διπλωματικής Εργασίας μέσω Erasmus....64
3.19 Ηλεκτρονικές Υπηρεσίες....65
3.19.1 Ηλεκτρονικές Υπηρεσίες Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση»....65
3.19.1.1 Ιστοσελίδες Π.Μ.Σ., Τμήματος Ψηφιακών Συστημάτων, Πανεπιστημίου Πειραιώς 65
3.19.1.2 Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων «ΛΕΥΚΙΠΠΟΣ» (Open eClass) 65
3.19.1.3 Εικονικό Campus....66

3.19.1.4 Σύστημα Ηλεκτρονικής Υποβολής Αιτήσεων Π.Μ.Σ. «ΑΡΙΣΤΥΛΛΟΣ» 67
3.19.1.5 Σύστημα Φοιτητολογίου & Ακαδημαϊκής Αξιολόγησης Π.Μ.Σ. «SIS-PORTAL» ... 68
3.19.1.6 Σύστημα σύγχρονης διδασκαλίας (Microsoft Teams) 69
3.19.1.7 Πανεπιστημιακά Εργαστήρια 69
3.19.1.8 Απόφοιτοι Π.Μ.Σ.: Ηλεκτρονική Εγγραφή στο Club Alumni 70
3.19.2 Ηλεκτρονικές Υπηρεσίες Ακαδημαϊκής Μονάδας 70
3.19.2.1 Ιστοσελίδα Πανεπιστημίου Πειραιώς 70
3.19.2.2 Σίτιση μεταπτυχιακών φοιτητών και φοιτητριών 70
3.19.2.3 Βιβλιοθήκη Πανεπιστήμιου Πειραιώς 71
3.19.2.4 Υγειονομική περίθαλψη 72
3.19.2.5 Ευρωπαϊκή Κάρτα Ασφάλισης Ασθένειας (Ε.Κ.Α.Α.) 72
3.19.2.6 Ιατρείο 72
3.19.2.7 Συμβουλευτικό Κέντρο 73
3.19.2.8 Εθελοντική ομάδα Πανεπιστήμιου Πειραιώς - Kerykes 73
3.19.2.9 Πολιτιστικές δραστηριότητες στο Πανεπιστήμιο Πειραιώς 73
3.19.2.10 Αθλητικές δραστηριότητες στο Πανεπιστήμιο Πειραιώς 74
3.19.2.11 Ψηφιακός πίνακας ανακοινώσεων 74
3.19.2.12 Κέντρο Υποστήριξης Διδασκαλίας και Μάθησης (ΚΕΔΙΜΑ) 74
3.19.3 Οδηγός ενεργοποίησης ηλεκτρονικών υπηρεσιών Π.Μ.Σ. και Ακαδημαϊκής Μονάδας 75
3.19.3.1 Δημιουργία και διαχείριση ιδρυματικού λογαριασμού 75
3.19.3.2 Υπηρεσία mypassword 76
3.19.4 Ηλεκτρονικές Υπηρεσίες Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού 76
3.19.4.1 Υπηρεσία Ηλεκτρονικής Ακαδημαϊκής Ταυτότητας 77
3.19.4.2 Πλατφόρμα ΔΗΛΟΣ365 78
3.19.5 Υποστηρικτικές Υπηρεσίες μεταπτυχιακών φοιτητών και φοιτητριών του Πανεπιστήμιου Πειραιώς 78
3.19.5.1 Ιστοσελίδα διανομής λογισμικού 79
3.19.5.2 Υπηρεσίες ασύρματου δικτύου και εικονικά τοπικά δίκτυα (VPN) 79
3.19.6 Υποστηρικτικές Υπηρεσίες μεταπτυχιακών φοιτητών και φοιτητριών από εξωτερικούς φορείς 79
3.20 Υποχρεώσεις και δικαιώματα μεταπτυχιακών φοιτητών και φοιτητριών 80
3.21 Χορήγηση υποτροφιών 82
3.22 Κινητικότητα μεταπτυχιακών φοιτητών και φοιτητριών 82
3.23 Ακαδημαϊκός Σύμβουλος Σπουδών 82
3.24 Μηχανισμός διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών 82

3.25 Αξιολόγηση μεταπτυχιακών φοιτητών και φοιτητριών 83
3.25.1 Περιγραφή συστήματος αξιολόγησης μαθησιακών αποτελεσμάτων 83
3.25.2 Μαθησιακά Αποτελέσματα 83
3.25.3 Σύστημα Αξιολόγησης 84
3.25.4 Προσαρμογή του συστήματος αξιολόγησης για μεταπτυχιακούς φοιτητές και φοιτήτριες με σοβαρές παθήσεις και μαθησιακές δυσκολίες 87
3.26 Διαδικασίες και κριτήρια επιλογής διδακτικού προσωπικού 88
3.27 Καθομολόγηση / ορκωμοσία 88
3.28 Υποδομή Π.Μ.Σ. 89
3.29 Αξιολόγηση Π.Μ.Σ. 89
3.30 Πρόσβαση στους χώρους του Πανεπιστημίου Πειραιώς 91
3.30.1 Πρόσβαση στους χώρους του Πανεπιστημίου με Μέσα Μαζικής Μεταφοράς 91
3.30.2 Υποδομές προσβασιμότητας για ΑΜΕΑ 93
3.31 Στοιχεία Επικοινωνίας 93
3.31.1 Ακαδημαϊκή Γραμματεία Τμήματος 93
3.31.2 Γραμματεία Μεταπτυχιακών Σπουδών 94
3.31.3 Κοινωνικά Δίκτυα 94
4 ΠΑΡΑΡΤΗΜΑΤΑ 95
4.1 Παράρτημα 1: Έντυπο αίτησης υποψηφιότητας 95
4.2 Παράρτημα 2: Πρότυπο Συστατικής Επιστολής 101
4.3 Παράρτημα 3: Κανονισμός Κινητικότητας Φοιτητών και Φοιτητριών και Προσωπικού (Πρόγραμμα ERASMUS+ και ERASMUS+ International) 104
4.4 Παράρτημα 4: Κανονισμός Ακαδημαϊκού Συμβούλου Σπουδών 104
4.5 Παράρτημα 5: Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών 104
4.6 Παράρτημα 6: Κανονισμός Εκπόνησης Εργασιών 104
4.7 Παράρτημα 7: Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας 104

1 Το Πανεπιστήμιο Πειραιώς

1.1 Ιστορία Πανεπιστημίου

Το Πανεπιστήμιο Πειραιώς ιδρύθηκε ως «Σχολή Βιομηχανικών Σπουδών» το 1938 από το Σύνδεσμο Βιομηχάνων και Βιοτεχνών, σύμφωνα με το Ν.5197/1931 και τον Α.Ν. 28/1936, που σε συνεργασία με το Σύνδεσμο Ανωνύμων Εταιριών της Ελλάδας έβαλαν ως βάσεις την οικονομική, νομική και τεχνική παιδεία των στελεχών της βιομηχανίας.

Ακολούθως:

- Το 1945 μετονομάσθηκε σε Ανωτέρα Σχολή Βιομηχανικών Σπουδών και σκοπός της ορίσθηκε η συστηματική, θεωρητική και πρακτική κατάρτιση διοικητικών στελεχών.
- Το 1949, με το Ν.Δ. 1245/49, ολοκληρώθηκε η οργάνωση της.
- Το 1958 η Ανωτέρα Σχολή Βιομηχανικών Σπουδών μετονομάσθηκε σε Ανωτάτη Βιομηχανική Σχολή και ορίσθηκε έδρα της ο Πειραιάς (ΝΔ 3876/58). Η φοίτηση ήταν τετραετής και τα πτυχία που χορηγούνταν ήταν ισότιμα των άλλων ΑΕΙ.
- Από το 1966 (ΝΔ 4578/1966) η σχολή λειτούργησε ως ΝΠΔΔ.
- Από το ακαδημαϊκό έτος 1971-1972 οι σπουδές στη Σχολή διαχωρίστηκαν από το δεύτερο έτος σε σπουδές Οικονομικών Επιστημών και Οργάνωσης και Διοίκησης Επιχειρήσεων (υπ. απόφ. 146652/71)
- Από το ακαδημαϊκό έτος 1977-1978 λειτούργησαν σπουδές στην Στατιστική και Ασφαλιστική Επιστήμη.
- Με το Ν.1268/82 η Σχολή λειτούργησε αρχικά ως μονοτμηματικό ΑΕΙ. Με το ΠΔ 43/1984 η Σχολή οργανώθηκε ώστε να περιλαμβάνει τρία Τμήματα: Οικονομικών Επιστημών, Οργάνωσης και Διοίκησης Επιχειρήσεων και Στατιστικής και Ασφαλιστικής Επιστήμης.
- Τον Ιούνιο του 1989, με το ΠΔ 377/89, η Σχολή μετονομάσθηκε σε Πανεπιστήμιο Πειραιώς, στο οποίο προστέθηκαν τρία ακόμα Τμήματα Σπουδών, δηλαδή:
    - Χρηματοοικονομικής και Τραπεζικής Διοικητικής
    - Ναυτιλιακών Σπουδών
    - Τεχνολογίας και Συστημάτων Παραγωγής
- Από το ακαδημαϊκό έτος 1990-1991 στα ήδη λειτουργούντα τρία Τμήματα (Οικονομικής Επιστήμης, Οργάνωσης και Διοίκησης Επιχειρήσεων, Στατιστικής και Ασφαλιστικής Επιστήμης), προστέθηκαν σε λειτουργία μόνο τα δύο από τα τρία νέα προβλεπόμενα.
    - Τμήμα Χρηματοοικονομικής και Τραπεζικής Διοικητικής
    - Τμήμα Ναυτιλιακών Σπουδών
- Το Τμήμα Βιομηχανικής Διοίκησης και Τεχνολογίας άρχισε να λειτουργεί από το ακαδημαϊκό έτος 1991-1992 ως Τμήμα Τεχνολογίας και Συστημάτων Παραγωγής και μετονομάσθηκε με το Π.Δ. 113/30-4-2002/ ΦΕΚ 95
- Το Τμήμα Πληροφορικής άρχισε να λειτουργεί από το ακαδημαϊκό έτος 1992-1993.
- Το Τμήμα Τεχνολογικής Εκπαίδευσης άρχισε να λειτουργεί από το ακαδημαϊκό έτος 1999-2000, το οποίο σύμφωνα με το άρθρο 3 παρ.2δ.γγ. του Ν.3027/28-6-2002/ΦΕΚ 152, μετονομάσθηκε σε Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων.

Κατόπιν, σύμφωνα με το Π.Δ. 151/2009, ΦΕΚ 194/Α'/1-11-2009, το Τμήμα μετονομάστηκε σε Τμήμα Ψηφιακών Συστημάτων.

- Το Τμήμα Διεθνών και Ευρωπαϊκών Σπουδών άρχισε να λειτουργεί από το ακαδημαϊκό έτος 2000-2001.
- Το Τμήμα Τουριστικών Σπουδών άρχισε να λειτουργεί από το ακαδημαϊκό έτος 2017-2018.

Το Πανεπιστήμιο Πειραιώς, σήμερα με δέκα Τμήματα, λειτουργεί ως Νομικό Πρόσωπο Δημοσίου δικαίου (Ν.Π.Δ.Δ.), σύμφωνα με την ελληνική νομοθεσία και τις κείμενες διατάξεις για την Ανώτατη Εκπαίδευση.

1.2 Οργανωτική Δομή

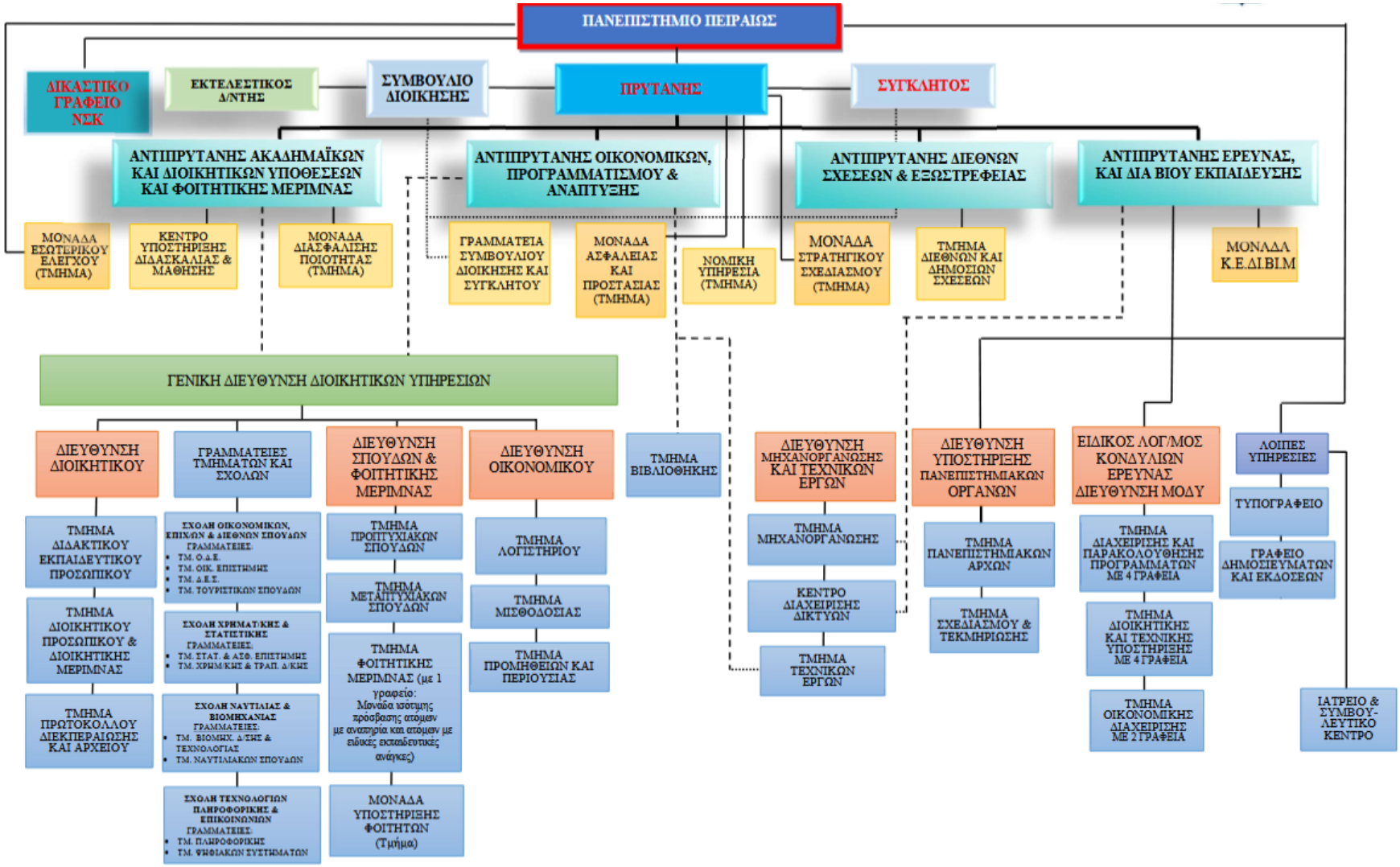
1.2.1 Πρυτανική Αρχή

Πρύτανης του Πανεπιστημίου Πειραιώς είναι ο Μιχαήλ Σφακιανάκης, Καθηγητής του Τμήματος Οργάνωσης και Διοίκησης Επιχειρήσεων.

Αντιπρυτάνεις

- Αντιπρύτανης Έρευνας και Διά Βίου Εκπαίδευσης: Δημοσθένης Κυριαζής, Καθηγητής του Τμήματος Ψηφιακών Συστημάτων της Σχολής Τεχνολογιών, Πληροφορικής και Επικοινωνιών
- Αντιπρύτανης Οικονομικών, Προγραμματισμού και Ανάπτυξης: Στυλιανή Σοφιανοπούλου, Καθηγήτρια του Τμήματος Βιομηχανικής Διοίκησης και Τεχνολογίας της Σχολής Ναυτιλίας και Βιομηχανίας
- Αντιπρύτανης Ακαδημαϊκών και Διοικητικών Υποθέσεων και Φοιτητικής Μέριμνας: Σπυρίδων Ρουκανάς, Αναπληρωτής Καθηγητής του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών της Σχολής Οικονομικών, Επιχειρηματικών και Διεθνών Σπουδών
- Αντιπρύτανης Διεθνών Σχέσεων και Εξωστρέφειας: Γεωργία Βερροπούλου, Καθηγήτρια του Τμήματος Στατιστικής και Ασφαλιστικής Επιστήμης της Σχολής Χρηματοοικονομικής και Στατιστικής

1.2.2 Οργανόγραμμα



2 Το Τμήμα Ψηφιακών Συστημάτων

2.1 Αντικείμενο του Τμήματος

Το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς καλύπτει δύο σημαντικούς κλάδους της Ψηφιακής Οικονομίας και της Κοινωνίας της Γνώσης:

- Τον κλάδο των Δικτυοκεντρικών Ψηφιακών Συστημάτων και Υπηρεσιών,
- Τον κλάδο των Τηλεπικοινωνιακών Συστημάτων και Δικτύων.

Η μετάβαση στην Κοινωνία της Πληροφορίας και της Γνώσης απαιτεί την ανάδειξη εξειδικευμένων επιστημόνων ικανών να συμβάλλουν στην ανάπτυξη, υλοποίηση και διαχείριση συστημάτων σύγχρονης ψηφιακής τεχνολογίας. Στη βάση αυτή έχει σχεδιαστεί το Πρόγραμμα Προπτυχιακών Σπουδών του Τμήματος, σύμφωνα με το οποίο λειτουργούν οι εξής πρωτεύουσες κατευθύνσεις σπουδών:

- Συστήματα Λογισμικού & Δεδομένων (ΣΛΔ) με έμφαση στα σύγχρονα πληροφοριακά συστήματα και στις τεχνολογίες διαχείρισης και αξιοποίησης δεδομένων.
- Υπολογιστικές Υποδομές & Υπηρεσίες (ΥΥΥ) με έμφαση σε Διαδικτυακές Υπηρεσίες, όπως η-Μάθηση (e-learning), η-Υγεία (e-health), η-Επιχειρηματικότητα (e-business), η-Διακυβέρνηση (e-government).
- Τηλεπικοινωνίες & Δίκτυα (Τ&Δ) με έμφαση στις σύγχρονες και επερχόμενες ενσύρματες και ασύρματες ευρυζωνικές τεχνολογίες, για το Διαδίκτυο και άλλες τηλεπικοινωνιακές υποδομές.

Επιπλέον, το Πρόγραμμα Προπτυχιακών Σπουδών υποστηρίζει τις ακόλουθες «οριζόντιες» κατευθύνσεις ειδίκευσης, που «κατανέμονται» στις προαναφερθείσες πρωτεύουσες κατευθύνσεις, συνεισφέροντας στο πρόγραμμα μαθήματα κορμού και διαθέσιμα προς επιλογή από κάθε πρωτεύουσα κατεύθυνση:

- Ασφάλεια Τηλεπικοινωνιακών και Πληροφοριακών Συστημάτων (ΑΣΦ)
- Παιδαγωγικές και Διδακτικές Ικανότητες (ΠΔΙ) που υποστηρίζει την απόκτηση της βασικής παιδαγωγικής και διδακτικής θεωρητικής κατάρτισης και πρακτικής εξάσκησης στο Ειδικό Αντικείμενο (ΠΕ86, Πληροφορική).

Το Τμήμα Ψηφιακών Συστημάτων προσφέρει τετραετές Πρόγραμμα Προπτυχιακών Σπουδών το οποίο αντιστοιχεί σε 240 Πιστωτικές Μονάδες του Ευρωπαϊκού Συστήματος Μεταφοράς και Συσσώρευσης Πιστωτικών Μονάδων (ECTS) και απονέμει, με την επιτυχή ολοκλήρωσή του, Πτυχίο στα «Ψηφιακά Συστήματα».

2.2 Επαγγελματικά Δικαιώματα Αποφοίτων

Το Πρόγραμμα Προπτυχιακών Σπουδών του Τμήματος έχει σχεδιαστεί για να προετοιμάζει επιστήμονες ικανούς να αντιμετωπίζουν με επιτυχία σύνθετα προβλήματα σχεδίασης, ανάπτυξης και εφαρμογής συστημάτων της σύγχρονης ψηφιακής τεχνολογίας. Απόφοιτοι του Τμήματος στελεχώνουν εταιρείες πληροφορικής και τηλεπικοινωνιών του Δημόσιου και Ιδιωτικού τομέα, στην Ελλάδα και στο εξωτερικό, καθώς και εκπαιδευτικούς οργανισμούς.

Επίσης, πολλοί από τους αποφοίτους του Τμήματός μας ακολουθούν την οδό της έρευνας τόσο στην Ελλάδα όσο και στο εξωτερικό.

Οι απόφοιτοι του Τμήματος έχουν πλήρως κατοχυρωμένα επαγγελματικά δικαιώματα που ορίζονται από το Προεδρικό Διάταγμα 44/2009 ΦΕΚ 58/8-4-2009 «Επαγγελματική Κατοχύρωση των Διπλωματούχων Μηχανικών και των Πτυχιούχων Πανεπιστημιακής Εκπαίδευσης στα αντικείμενα Πληροφορικής και Τηλεπικοινωνιών». Επιπλέον, οι απόφοιτοι του Τμήματος έχουν πλήρως κατοχυρωμένα επαγγελματικά δικαιώματα αναφορικά με την απασχόλησή τους στον Δημόσιο Τομέα, αφού το Πτυχίο του Τμήματος συμπεριλαμβάνεται στα προσόντα διορισμού στον κλάδο ΠΕ Πληροφορικής σε θέσεις φορέων του Δημοσίου Προεδρικό Διάταγμα 347/2003, ΦΕΚ 315/Α'/31-12-2003.

2.3 Διδακτικό Ερευνητικό Προσωπικό

I. Καθηγητές

- Αγγελική Αλεξίου
- Γεώργιος Βούρος
- Στέφανος Γκρίτζαλης
- Παναγιώτης Δεμέστιχας
- Χρήστος Δουλκερίδης
- Γεώργιος Ευθύμογλου
- Αθανάσιος Κανάτας
- Δημοσθένης Κυριαζής
- Κωνσταντίνος Λαμπρινουδάκης
- Ηλίας Μαγκλογιάννης
- Χρήστος Ξενάκης
- Ανδριάνα Πρέντζα
- Συμεών Ρετάλης
- Άγγελος Ρούσκας
- Δημήτριος Σάμψων
- Νικήτας-Μαρίνος Σγούρος
- Απόστολος Μηλιώνης
- Φωτεινή Παρασκευά
- Μιχαήλ Φιλιππάκης
- Μαρία Χαλκίδη

II. Αναπληρωτές Καθηγητές

- Δημοσθένης Βουγιούκας

III. Επίκουροι Καθηγητές

- Ανδρέας Μενύχτας
- Ορέστης Τελέλης

IV. Ομότιμοι Καθηγητές

- Γεώργιος Βασιλακόπουλος
- Σωκράτης Κάτσικας
- Ιωάννης Μανιάτης

V. Μέλη Ε.ΔΙ.Π.

- Αρίστη Γαλάνη
- Δημήτριος Γκότζος
- Βασιλική Κούφη
- Ελένη-Λασκαρίνα Μακρή
- Χρήστος Μανουσόπουλος
- Κωνσταντίνος Μούτσελος
- Αγγελική Πάνου
- Ελευθερία Στουγιάννου
- Ευάγγελος Χαλεπλίδης

VI. Μέλη Ε.Τ.Ε.Π.

- Κατερίνα Πούπουζα

2.4 Διοικητικό Προσωπικό

Ακαδημαϊκή Γραμματεία Τμήματος

Ομαδικό E-mail Γραμματείας : gramds@unipi.gr

- Παρασκευή Αντωνίου (Προϊσταμένη)
  - Τηλ.: 210-4142235
  - email: panton@unipi.gr
- Σοφία Σκούντζου
  - Τηλ.: 210-4142373
  - email: sskountz@unipi.gr
- Ιωάννης Φρεντζάς
  - Τηλ.: 210-4142426
  - email: fretzas@unipi.gr
- Παναγιώτης Θεοδωρόπουλος
  - Τηλ.: 210-4142369
  - e-mail: ptheodor@unipi.gr

2.5 Υλικοτεχνική Υποδομή

Το Πανεπιστήμιο Πειραιώς στεγάζεται στο κεντρικό κτίριο επί της οδού Καραολή και Δημητρίου 80, όπου βρίσκονται οι διοικητικές υπηρεσίες, τα γραφεία μέρους του διδακτικού και ερευνητικού προσωπικού και οι αίθουσες διδασκαλίας. Επιπλέον, χρησιμοποιεί κτιριακές εγκαταστάσεις στο κτίριο επί της οδού Δεληγιώργη (Τμήμα Βιομηχανικής Διοίκησης και Τεχνολογίας), στο κτίριο επί της οδού Τσαμαδού 78 και Δεληγιώργη (Αίθουσες Διδασκαλίας), στο κτίριο επί της οδού Καραολή Δημητρίου 40 (Τμήμα Ναυτιλιακών Σπουδών και Αίθουσες Διδασκαλίας), στο κτίριο επί της οδού Τσαμαδού 78 (Φοιτητικό Εστιατόριο), στο κτίριο επί της Λεωφ. Α. Παπαναστασίου 91 (Κέντρο Ερευνών Πανεπιστημίου Πειραιώς), στο κτίριο επί της οδού Ζέας 80 (Γραμματεία του Τμήματος Ψηφιακών Συστημάτων) και στο κτίριο επί της οδού Ανδρούτσου 150 (Γραφεία του Διδακτικού και Ερευνητικού Προσωπικού και Εργαστήρια του Τμήματος Ψηφιακών Συστημάτων).

Το Τμήμα Ψηφιακών Συστημάτων στεγάζεται σε ιδιόκτητο κτίριο του Πανεπιστημίου Πειραιώς, το οποίο βρίσκεται στην οδό Ανδρούτσου 150 και στο οποίο λειτουργούν έξι (6) πλήρως εξοπλισμένα εργαστήρια Ηλεκτρονικών Υπολογιστών χωρητικότητας εκατόν εξήντα (160) θέσεων εργασίας, για τους προπτυχιακούς και μεταπτυχιακούς φοιτητές και φοιτήτριες του Τμήματος. Τα εργαστήρια του Τμήματος λειτουργούν όλες τις εργάσιμες ημέρες 09:00 – 21:00 και διαθέτουν σύγχρονο εργαστηριακό εξοπλισμό (υλικό και λογισμικό), ο οποίος εμπλουτίζεται και αναβαθμίζεται διαρκώς.

3 Το Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση»

Το ΠΜΣ «**Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση**» ιδρύεται στο πλαίσιο του Ευρωπαϊκού έργου EU-iNSPIRE (EU **iN**novative multi-di**S**ci**P**linary **I**ndustry-focused cybersecurity education for upskilling and **R**eskilling the EU workforce**)** το οποίο ξεκίνησε τον Ιανουάριο του 2025, έχει διάρκεια (4) τέσσερα χρόνια και χρηματοδοτείται από το πρόγραμμα DIGITAL-2023-SKILLS-05 (Αρ. Συμβολαίου 101190054). Συγκεκριμένα, τα έξοδα οργάνωσης και λειτουργίας του ΠΜΣ, συμπεριλαμβανομένων των τελών φοίτησης φοιτητριών και φοιτητών προερχομένων από χώρες της ΕΕ, για τους πρώτους δύο (2) κύκλους λειτουργίας του ΠΜΣ καλύπτονται από τη χρηματοδότηση του συγκεκριμένου έργου.

Οι στόχοι του έργου EU-iNSPIRE και κατ' επέκταση του ΠΜΣ «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» είναι να καλύψει τις πολύπλευρες εκπαιδευτικές και επαγγελματικές ανάγκες εξειδίκευσης που είναι κρίσιμες για την υποστήριξη του μελλοντικού οικοσυστήματος Κυβερνοανθεκτικότητας (Cyber Resilience) της ΕΕ, μέσα από μια καινοτόμα τριπλή προσέγγιση:

- Επιστημονική ανάπτυξη προσωπικού ΤΠΕ, ώστε να είναι σε θέση να αξιοποιήσει τεχνολογίες κυβερνοασφάλειας (cyber security) για την ενίσχυση της ανθεκτικότητας (resilience) διαδικασιών, συστημάτων και ψηφιακών υποδομών.
- Εκπαίδευση επιστημόνων σε θέματα προστασίας από κυβερνοκινδύνους (cyber risks) και στην εφαρμογή μηχανισμών αποτίμησης απειλών (threats), ευπαθειών (vulnerabilities) και κινδύνων (risk) στον κυβερνοχώρο.
- Ενδυνάμωση εμπειρογνωμόνων με εξειδικευμένες γνώσεις ψηφιακού μετασχηματισμού, οι οποίοι να είναι σε θέση να εφαρμόζουν αποδοτικές καινοτόμες λύσεις σε διαδικασίες αξιολογήσεων συμμόρφωσης (compliance) κυβερνοασφάλειας.

Στο παρόν ΠΜΣ συμμετέχουν και έχουν συμφωνήσει να δραστηριοποιηθούν με διδάσκοντες και διδάσκουσες στην εκπαιδευτική διαδικασία τα ακόλουθα Πανεπιστημιακά Ιδρύματα, τα οποία αποτελούν εταίρους (partners) στο προαναφερόμενο έργο:

- Πανεπιστήμιο Πειραιώς (Ελλάδα),
- Technical University of Munich (Γερμανία),
- University of Oslo (Νορβηγία),
- University of Malaga (Ισπανία),
- Open University of Cyprus (Κύπρος),
- ενώ το Business School της École des Ponts (Γαλλία) θα υποστηρίξει το πρόγραμμα με διακεκριμένους καθηγητές και καθηγήτριες για στοχευμένες διαλέξεις σεμιναριακού χαρακτήρα

3.1 Γνωστικό Αντικείμενο – Στόχος

Η ευρεία χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών - ΤΠΕ (Information and Communication Technologies - ICT) μεταβάλλει το διεθνές κοινωνικό, οικονομικό, τεχνολογικό, πολιτικό και πολιτισμικό περιβάλλον, καθώς επιτρέπει την ταχύτατη δημιουργία, μεταφορά, επεξεργασία και αποθήκευση μεγάλου όγκου δεδομένων.

Το γεγονός αυτό παράγει νέες δυνατότητες τόσο για τους πολίτες και την επιχειρηματική κοινότητα που αξιοποιούν τα δεδομένα αυτά προς όφελος της οικονομικής, κοινωνικής, τεχνολογικής, πολιτιστικής και επιστημονικής τους ανάπτυξης, όσο και για τη δημόσια διοίκηση που προσβλέπει στην ψηφιακή τεχνολογία ως μετασχηματιστικό μέσο βελτίωσης των παρεχόμενων υπηρεσιών στους πολίτες και την επιχειρηματικότητα, αναιρώντας χρόνιες διοικητικές αβελτηρίες.

Παράλληλα, όμως, όσο περισσότερο δραστηριότητες των ανθρώπων αποκτούν ψηφιακή διάσταση ή ψηφιοποιούνται καθ' ολοκληρία, τόσο πιο ευάλωτες (vulnerable) γίνονται σε κυβερνοεπιθέσεις (cyber attacks) που μπορούν να απειλήσουν την εύρυθμη λειτουργία της κοινωνίας, την ασφάλειά της, καθώς - σε περιπτώσεις κρίσιμων υποδομών (critical infrastructures) - και τις ίδιες τις ανθρώπινες ζωές.

Ιδιαίτερα κρίσιμη στις συνθήκες αυτές είναι η δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, ψηφιακών υποδομών και ψηφιακών υπηρεσιών που θα εμπνέει την εμπιστοσύνη πολιτών και επιχειρήσεων, οδηγώντας στην περαιτέρω χρήση και διάθεση νέων ψηφιακών προϊόντων και υπηρεσιών, συχνά καινοτόμων με υψηλή προστιθέμενη αξία. Στην κατεύθυνση αυτή βρίσκονται και ποικίλες ρυθμιστικές / κανονιστικές πρωτοβουλίες στην ΕΕ, όπως η Οδηγία Network and Information Systems Directive-2 NIS2 2022/2555, ο Κανονισμός Digital Operational Resilience Act DORA 2022/2554, ο Κανονισμός General Data Protection Regulation GDPR 2016/679, η Οδηγία e-Privacy 2002/58, Cybersecurity Act 2019/881, κ.ά.

Το παρόν Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση», διαθεματικό και διεπιστημονικό, έχει ως αντικείμενο την εξειδίκευση επιστημόνων στα γνωστικά αντικείμενα της κυβερνοασφάλειας, της προστασίας δεδομένων και της διακυβέρνησης σχετικών περιβαλλόντων.

Ο σκοπός του Π.Μ.Σ. είναι η προαγωγή της επιστημονικής γνώσης στα πεδία των τεχνολογιών κυβερνοασφάλειας, προστασίας δεδομένων και της διακυβέρνησης σχετικών περιβαλλόντων. Στο πλαίσιο αυτό, οι απόφοιτοι του Π.Μ.Σ. θα είναι σε θέση να δραστηριοποιηθούν επαγγελματικά σε θέματα τεχνολογιών κυβερνοασφάλειας, προστασίας δεδομένων και διακυβέρνησης σχετικών περιβαλλόντων, σε επιχειρήσεις και οργανισμούς του ιδιωτικού και του δημόσιου τομέα, καθώς και να παράξουν νέα γνώση στο πλαίσιο συναφών ερευνητικών πρωτοβουλιών.

Οι στόχοι του Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση», δηλαδή -κατά την Επιστημολογία- τα μέσα επίτευξης του προαναφερόμενου σκοπού, περιλαμβάνουν:

- Τη διεπιστημονική διαθεματική εξειδίκευση επιστημόνων από τον χώρο των τεχνολογιών πληροφορικής και επικοινωνιών και γενικότερα της τεχνολογίας των θετικών επιστημών και των επιστημών της διοίκησης, στα γνωστικά πεδία της κυβερνοασφάλειας, της προστασίας δεδομένων και της διακυβέρνησης σχετικών περιβαλλόντων

- Την εκ μέρους των αποφοίτων απόκτηση των κατάλληλων γνώσεων και δεξιοτήτων ώστε να είναι σε θέση να δραστηριοποιηθούν ερευνητικά σε συναφή επιστημονικά θέματα, με σκοπό τη διεξαγωγή έρευνας για παραγωγή νέας γνώσης
- Τη δυνατότητα των αποφοίτων να συνεισφέρουν στην ανάπτυξη γνώσεων και τεχνολογιών και υιοθέτηση πρακτικών στον επαγγελματικό χώρο και να αποκτήσουν επιχειρησιακή ικανότητα αντιμετώπισης προβλημάτων και υλοποίησης λύσεων, κυρίως σε περιβάλλοντα ψηφιακού μετασχηματισμού, αλλαγών και διαχείρισης κρίσεων
- Τη δυνατότητα των αποφοίτων να αξιολογούν, να ερμηνεύουν και να προωθούν σύγχρονες επιστημονικές έρευνες και μελέτες συναφείς με το γνωστικό τους πεδίο
- Την αξιοποίηση, εκ μέρους των αποφοίτων, λύσεων που θα αρθρώνονται επαγωγικά και με επιστημονικά τεκμηριωμένο τρόπο, στα σύνθετα προς επίλυση προβλήματα διεπιστημονικής διαθεματικής φύσης που εγείρονται στο περιβάλλον επαγγελματικής ή ερευνητικής δραστηριοποίησής τους
- Την ανάπτυξη με αυτονομία των γνώσεων και ικανοτήτων τους
- Την καλλιέργεια στους αποφοίτους εκείνων των ικανοτήτων και δεξιοτήτων που θα επιτρέπουν βελτίωση επικοινωνιακών δεξιοτήτων, δημιουργικότητας, αναλυτικής σκέψης, συνεργασιμότητας, ηγεσίας, κινητροδότησης, αυτογνωσίας, επίλυσης πολύπλοκων προβλημάτων.

Όλα τα παραπάνω καθιστούν το προτεινόμενο Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» εξαιρετικά χρήσιμο, απολύτως ενδιαφέρον και εντυπωσιακά ανταγωνιστικό σε σχέση με αντίστοιχης θεματικής κορυφαία Π.Μ.Σ. σε άλλες χώρες της Ευρωπαϊκής Ένωσης, ενώ διαφοροποιείται απολύτως από τα υπάρχοντα σχετικά συναφή Π.Μ.Σ. στη χώρα μας, αφού θα είναι το μοναδικό στην Ελλάδα που θα θεραπεύει θέματα κυβερνοασφάλειας, προστασίας δεδομένων και διακυβέρνησης σχετικών περιβαλλόντων, αμιγώς στην αγγλική γλώσσα. Κυρίως, μάλιστα, όταν η ως άνω δραστηριότητα ίδρυσης Π.Μ.Σ. στην αγγλική γλώσσα με μεταπτυχιακούς φοιτητές και φοιτήτριες από την Ελλάδα και τις άλλες χώρες εντός και εκτός της ΕΕ στοιχίζεται πλήρως με την ιδρυματική στρατηγική του Πανεπιστημίου Πειραιώς για διεθνοποίηση και ανάπτυξη καινοτόμων ανταγωνιστικών εκπαιδευτικών δράσεων στην αγγλική γλώσσα.

3.2 Μεταπτυχιακός Τίτλος Σπουδών

Το Πρόγραμμα Μεταπτυχιακών Σπουδών (Π.Μ.Σ.) απονέμει Δίπλωμα Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) στις «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» (MSc in Advanced Cybersecurity Technologies and Governance).

Το Δ.Μ.Σ. είναι δημόσιο έγγραφο. Ο τύπος του ορίζεται με απόφαση της Συγκλήτου. Το Δ.Μ.Σ. συντάσσεται και απονέμεται στην ελληνική και αγγλική γλώσσα. Τα Π.Μ.Σ. οδηγούν σε τίτλο σπουδών επιπέδου 7 σύμφωνα με το Ευρωπαϊκό Πλαίσιο Προσόντων (EQF) και το Εθνικό Πλαίσιο Προσόντων (ΕΠΠ). Το Δ.Μ.Σ. που απονέμει το Π.Μ.Σ. που διοργανώνεται από ένα Τμήμα, υπογράφεται από τον/την Πρύτανη, τον/την Πρόεδρο του Τμήματος και τον/τη Γραμματέα του Τμήματος. Ο βαθμός του Διπλώματος χαρακτηρίζεται ως εξής: από 5 έως 6.49 ΚΑΛΩΣ, από 6.50 έως 8.49 ΛΙΑΝ ΚΑΛΩΣ και από 8.50 έως 10 ΑΡΙΣΤΑ. Το βιβλίο

διπλωματούχων μεταπτυχιακών φοιτητών και φοιτητριών υπογράφεται από τον/τη Γραμματέα του Τμήματος, τον/την Πρόεδρο του Τμήματος και τον/την Πρύτανη του Πανεπιστημίου. Στο Δ.Μ.Σ. επισυνάπτεται Παράρτημα Διπλώματος στην ελληνική και αγγλική γλώσσα σύμφωνα με τις διατάξεις του άρθρου 15 του ν. 3374/2005 (Α' 189) και της υπό στοιχεία Φ5/89656/Β3/13.8.07 υπουργικής απόφασης (Β' 1466).

3.3 Δομή και Όργανα του Π.Μ.Σ.

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

α) η Σύγκλητος του Ιδρύματος

β) η Συνέλευση του Τμήματος

γ) η Συντονιστική Επιτροπή (Σ.Ε.) του Π.Μ.Σ.

δ) ο Διευθυντής του Π.Μ.Σ.

Οι αρμοδιότητες των οργάνων των Π.Μ.Σ. είναι οι εξής:

1. Η Σύγκλητος είναι το αρμόδιο όργανο για τα θέματα ακαδημαϊκού, διοικητικού, οργανωτικού χαρακτήρα των Π.Μ.Σ. Η Σύγκλητος έχει τις ακόλουθες αρμοδιότητες σχετικά με τα Π.Μ.Σ. και όσες άλλες προβλέπονται από τον Εσωτερικό Κανονισμό λειτουργίας του ιδρύματος, εφόσον αυτές δεν έχουν ανατεθεί από τον νόμο ειδικώς σε άλλα όργανα του ιδρύματος:
   - εγκρίνει την ίδρυση ή την τροποποίηση της απόφασης Ίδρυσης του Π.Μ.Σ., καθώς και το περιεχόμενο των προγραμμάτων αυτών
   - εγκρίνει ή τροποποιεί τους εσωτερικούς κανονισμούς λειτουργίας των Π.Μ.Σ.
   - εγκρίνει την παράταση της χρονικής διάρκειας της εσωτερικής λειτουργίας των Π.Μ.Σ.
   - εγκρίνει τη σύναψη συνεργασιών με ιδρύματα της ημεδαπής ή αλλοδαπής ή ερευνητικά κέντρα - ινστιτούτα και τεχνολογικούς φορείς του άρθρου 13Α του ν. 4310/2014 (ΦΕΚ 258 τ. Α') για την οργάνωση διιδρυματικών προγραμμάτων σπουδών, δεύτερου κύκλου, καθώς και τα πρωτόκολλα για ακαδημαϊκή ή ερευνητική συνεργασία με φορείς της ημεδαπής ή αλλοδαπής
   - αποφασίζει την κατάργηση των Π.Μ.Σ. που προσφέρονται από το Α.Ε.Ι.
2. Η Συνέλευση του Τμήματος είναι αρμόδια για την οργάνωση, διοίκηση και διαχείριση του Π.Μ.Σ. και ιδίως:
   - εισηγείται προς τη Σύγκλητο την έγκριση ή την τροποποίηση της απόφασης ίδρυσης του Π.Μ.Σ., καθώς και την παράταση της διάρκειας του Π.Μ.Σ.
   - ορίζει τα μέλη της Σ.Ε. του Π.Μ.Σ. του Τμήματος
   - αναθέτει το διδακτικό έργο στους διδάσκοντες και διδάσκουσες του Π.Μ.Σ.
   - συγκροτεί επιτροπές για την αξιολόγηση των αιτήσεων των υποψήφιων μεταπτυχιακών φοιτητών και φοιτητριών και εγκρίνει την εγγραφή τους στο Π.Μ.Σ.

- συγκροτεί εξεταστικές επιτροπές για την εξέταση των μεταπτυχιακών διπλωματικών εργασιών των μεταπτυχιακών φοιτητών και φοιτητριών και ορίζει τον επιβλέποντα ή επιβλέπουσα ή συνεπιβλέποντες ανά μεταπτυχιακή διπλωματική εργασία
- διαπιστώνει την επιτυχή ολοκλήρωση της φοίτησης προκειμένου να απονεμηθεί ο τίτλος του Μεταπτυχιακού Διπλώματος Ειδίκευσης
- εγκρίνει τον απολογισμό του Π.Μ.Σ., κατόπιν εισήγησης της Σ.Ε.
- ασκεί κάθε άλλη αρμοδιότητα που προβλέπεται από τις διατάξεις του Κανονισμού Λειτουργίας.

Με απόφαση της Συνέλευσης του Τμήματος οι αρμοδιότητες των περ. 4. και 5. δύναται να μεταβιβάζονται στη Σ.Ε. του Π.Μ.Σ. (παρ. 2, άρθρο 82 ν. 4957/2022).

Επίσης, δύναται να μεταβιβάζονται προς τη Σ.Ε. συγκεκριμένες αρμοδιότητες της Συνέλευσης του Τμήματος για την αποτελεσματικότερη λειτουργία του Π.Μ.Σ., κατόπιν έκδοσης σχετικής απόφασης μεταβίβασης αρμοδιοτήτων.

3. Η Σ.Ε. αποτελείται από τον Διευθυντή του Π.Μ.Σ. και τέσσερα (4) μέλη Διδακτικού Ερευνητικού Προσωπικού (Δ.Ε.Π.) του Τμήματος, που έχουν συναφές γνωστικό αντικείμενο με αυτό του Π.Μ.Σ. και αναλαμβάνουν διδακτικό έργο στο Π.Μ.Σ. Τα μέλη της Σ.Ε. καθορίζονται από τη Συνέλευση του Τμήματος για διετή θητεία, παράλληλα με τη θητεία του Διευθυντή. Στη Σ.Ε. δύναται να συμμετέχουν Ομότιμοι Καθηγητές του Τμήματος εφόσον παρέχουν διδακτικό έργο στο Π.Μ.Σ. Τα μέλη της Σ.Ε. δε δικαιούνται αμοιβής ή οιασδήποτε αποζημίωσης για την εκτέλεση των αρμοδιοτήτων που τους ανατίθενται και σχετίζεται με την εκτέλεση των καθηκόντων τους. Η Σ.Ε. είναι αρμόδια για την παρακολούθηση και τον συντονισμό της λειτουργίας του Π.Μ.Σ. και ιδίως:
   - καταρτίζει τον αρχικό ετήσιο προϋπολογισμό του Π.Μ.Σ. και τις τροποποιήσεις του, εφόσον το Π.Μ.Σ. διαθέτει πόρους (άρθρο 84 του ν. 4957/2022) και εισηγείται την έγκρισή του προς την Επιτροπή Ερευνών του Ειδικού Λογαριασμού Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.) του Πανεπιστημίου
   - καταρτίζει τον απολογισμό του προγράμματος και εισηγείται την έγκρισή του προς τη Συνέλευση του Τμήματος
   - εγκρίνει τη διενέργεια δαπανών του Π.Μ.Σ.
   - εγκρίνει τη χορήγηση υποτροφιών, ανταποδοτικών ή μη, σύμφωνα με όσα ορίζονται στην απόφαση ίδρυσης του Π.Μ.Σ. και τον Κανονισμό Μεταπτυχιακών και Διδακτορικών Σπουδών
   - εισηγείται προς τη Συνέλευση του Τμήματος την κατανομή του διδακτικού έργου, καθώς και την ανάθεση διδακτικού έργου στις κατηγορίες διδασκόντων (άρθρο 83 του ν. 4957/2022)
   - εισηγείται προς τη Συνέλευση του Τμήματος την πρόσκληση Επισκεπτών Καθηγητών και Καθηγητριών για την κάλυψη διδακτικών αναγκών του Π.Μ.Σ.
   - καταρτίζει σχέδιο για την τροποποίηση του προγράμματος σπουδών, το οποίο υποβάλλει προς τη Συνέλευση του Τμήματος,
   - εισηγείται προς τη Συνέλευση του Τμήματος την ανακατανομή των μαθημάτων μεταξύ των ακαδημαϊκών εξαμήνων, καθώς και θέματα που σχετίζονται με την ποιοτική αναβάθμιση του προγράμματος σπουδών

- ασκεί κάθε άλλη αρμοδιότητα που προβλέπεται από τις διατάξεις του Κανονισμού Λειτουργίας.

4. Ο Διευθυντής του Π.Μ.Σ. προέρχεται από τα μέλη Δ.Ε.Π. του Τμήματος κατά προτεραιότητα βαθμίδας Καθηγητή ή Αναπληρωτή Καθηγητή και ορίζεται με απόφαση της Συνέλευσης του Τμήματος για διετή θητεία, με δυνατότητα ανανέωσης χωρίς περιορισμό. Ο Διευθυντής του Π.Μ.Σ. δε δικαιούται αμοιβής ή οιασδήποτε αποζημίωσης για την εκτέλεση των αρμοδιοτήτων που του ανατίθενται και σχετίζονται με την εκτέλεση των καθηκόντων του. Ο Διευθυντής του Π.Μ.Σ. έχει τις ακόλουθες αρμοδιότητες:
    1. προεδρεύει της Σ.Ε., συντάσσει την ημερήσια διάταξη και συγκαλεί τις συνεδριάσεις της
    2. εισηγείται τα θέματα που αφορούν στην οργάνωση και λειτουργία του Π.Μ.Σ. προς τη Συνέλευση του Τμήματος
    3. εισηγείται προς τη Σ.Ε. και τα λοιπά όργανα του Π.Μ.Σ. και του Α.Ε.Ι. θέματα σχετικά με την αποτελεσματική λειτουργία του Π.Μ.Σ.
    4. είναι Επιστημονικός Υπεύθυνος του προγράμματος (άρθρο 234 του ν. 4957/2022) και ασκεί τις αντίστοιχες αρμοδιότητες
    5. παρακολουθεί την υλοποίηση των αποφάσεων των οργάνων του Π.Μ.Σ. και του Εσωτερικού Κανονισμού Μεταπτυχιακών και Διδακτορικών προγραμμάτων σπουδών, καθώς και την παρακολούθηση εκτέλεσης του προϋπολογισμού του Π.Μ.Σ.
    6. ασκεί οποιαδήποτε άλλη αρμοδιότητα, η οποία ορίζεται στην απόφαση ίδρυσης του Π.Μ.Σ.

Με απόφαση της Επιτροπής Ερευνών δύναται να ορίζεται αναπληρωτής Επιστημονικός Υπεύθυνος του έργου/προγράμματος, εφόσον αυτό κρίνεται αναγκαίο, κατόπιν απόφασης της Συνέλευσης.

Τη διοικητική και γραμματειακή υποστήριξη του Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» αναλαμβάνει η Γραμματεία του Τμήματος. Οι διοικητικοί υπάλληλοι που υποστηρίζουν τα Π.Μ.Σ. εκτός ωρών εργασίας τους στο Πανεπιστήμιο, καθώς και αυτοί στους οποίους έχει ανατεθεί έργο σχετικά με τα Π.Μ.Σ., δύνανται να αμείβονται για τις υπηρεσίες που παρέχουν.

3.4 Αριθμός και Κατηγορίες Εισακτέων

Στο Π.Μ.Σ. γίνονται δεκτοί κάτοχοι τίτλου πρώτου κύκλου σπουδών Α.Ε.Ι. της ημεδαπής ή ομοταγών ιδρυμάτων της αλλοδαπής σύμφωνα με τις διατάξεις του ν. 4957/2022 όπως ισχύει. Όλοι οι υποψήφιοι και υποψήφιες θα πρέπει να γνωρίζουν επαρκώς την αγγλική γλώσσα (γλώσσα διδασκαλίας). Τα μέλη των κατηγοριών Ε.Ε.Π., Ε.ΔΙ.Π. και Ε.Τ.Ε.Π. και διοικητικών υπαλλήλων του ιδρύματος μπορούν να υποβάλλουν αίτηση και – εφόσον γίνουν δεκτοί κατά τη διαδικασία αξιολόγησης – να θεωρηθούν υπεράριθμοι και μόνο ένας κατ' έτος σύμφωνα με τον Εσωτερικό Κανονισμό του ιδρύματος.

Πιο συγκεκριμένα, το Π.Μ.Σ. απευθύνεται σε πτυχιούχους Ανώτατων Εκπαιδευτικών Ιδρυμάτων της ημεδαπής ή αντιστοίχων ομοταγών ιδρυμάτων της αλλοδαπής. Ενδεικτικά αναφέρονται πτυχιούχοι: Τμημάτων Πληροφορικής και Επικοινωνιών, Τμημάτων Θετικών και Τεχνολογικών Επιστημών, διπλωματούχοι μηχανικοί: Πολυτεχνείων και Πολυτεχνικών Σχολών, Νομικής Σχολής, Τμημάτων Πολιτικής Επιστήμης και Δημόσιας Διοίκησης, Τμημάτων Διοίκησης και Οικονομίας. Επιπλέον, Απόφοιτοι Εθνικής Σχολής Δημόσιας Διοίκησης και Απόφοιτοι παραγωγικών Στρατιωτικών Σχολών Ενόπλων Δυνάμεων και Σωμάτων Ασφαλείας κ.ά.

Το Π.Μ.Σ. δέχεται εκατό πενήντα (150) φοιτητές και φοιτήτριες ανά ακαδημαϊκό έτος.

3.5 Κριτήρια και Διαδικασία Επιλογής Υποψηφίων για τα Π.Μ.Σ.

Η επιλογή των εισακτέων στα Π.Μ.Σ. γίνεται σύμφωνα με τις διατάξεις και τις ρυθμίσεις του Κανονισμού Μεταπτυχιακών Σπουδών.

Με απόφαση της Συνέλευσης δημοσιεύεται και αναρτάται στην ιστοσελίδα του Τμήματος και του Ιδρύματος προκήρυξη για την εισαγωγή μεταπτυχιακών φοιτητών και φοιτητριών στο Π.Μ.Σ. Στην προκήρυξη αναγράφονται όλες οι σχετικές λεπτομέρειες υποβολής. Οι σχετικές αιτήσεις μαζί με τα απαραίτητα δικαιολογητικά υποβάλλονται ηλεκτρονικά ή κατατίθενται στη 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 και υποψήφια είναι τα εξής:

1. Αίτηση εγγραφής (Παράρτημα 1: Έντυπο αίτησης υποψηφιότητας).
2. Βιογραφικό σημείωμα.
3. Αντίγραφο πτυχίου/διπλώματος ή βεβαίωση περάτωσης σπουδών.
4. Πιστοποιητικό αναλυτικής βαθμολογίας (στο οποίο αναγράφεται και ο βαθμός πτυχίου ή διπλώματος εάν οι υποψήφιοι και υποψήφιες έχουν ήδη αποφοιτήσει).
5. Δύο συστατικές επιστολές (Παράρτημα 2: Πρότυπο Συστατικής Επιστολής).
6. Αντίγραφο Πτυχιακής ή Διπλωματικής εργασίας (εάν εκπονήθηκε).
7. Δημοσιεύσεις σε επιστημονικά περιοδικά με κριτές ή επιστημονικά συνέδρια με κριτές ή άλλες δημοσιεύσεις (εάν υπάρχουν).
8. Αποδεικτικά επαγγελματικής ή ερευνητικής δραστηριότητας (εάν υπάρχουν).
9. Πιστοποιητικό καλής γνώσης αγγλικής γλώσσας.
10. Φωτοτυπία διαβατηρίου ή εθνικού εγγράφου ταυτοποίησης.
11. Μία φωτογραφία.

Η Συνέλευση του Τμήματος, με απόφασή της, δύναται να ορίσει πρόσθετα δικαιολογητικά. Η ακριβής διαδικασία περιγράφεται στην προκήρυξη.

Για τους υποψήφιους και υποψήφιες που είναι κάτοχοι τίτλου σπουδών πρώτου κύκλου από ιδρύματα της αλλοδαπής θα 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. Σε κάθε περίπτωση, τίτλοι σπουδών της αλλοδαπής υποβάλλονται και γίνονται αποδεκτοί σύμφωνα με τις κείμενες διατάξεις.

Κατ' εξαίρεση, γίνονται δεκτές αιτήσεις υποψηφίων που δε διαθέτουν κατά την καταληκτική ημερομηνία για την υποβολή υποψηφιοτήτων τίτλο σπουδών πρώτου κύκλου. Σε περίπτωση επιλογής τους, οι υποψήφιοι και υποψήφιες πρέπει να προσκομίσουν πριν την εγγραφή τους στο Π.Μ.Σ. είτε βεβαίωση ολοκλήρωσης σπουδών είτε επικυρωμένο αντίγραφο του τίτλου σπουδών τους, άλλως δεν εγγράφονται στο Π.Μ.Σ. Το αυτό ισχύει και για το πιστοποιητικό καλής γνώσης της αγγλικής γλώσσας.

Η επιλογή των εισακτέων πραγματοποιείται από επιτροπή μελών Δ.Ε.Π. (Επιτροπή Επιλογής) που συγκροτείται με απόφαση της Συνέλευσης. Η έγκριση της εγγραφής των μεταπτυχιακών φοιτητών και φοιτητριών ορίζεται από τη Συνέλευση του Τμήματος.

Τα κριτήρια επιλογής, καθώς και οι λεπτομέρειες εφαρμογής των κριτηρίων αυτών γίνονται γνωστά στους υποψηφίους με την προκήρυξη του Π.Μ.Σ. και είναι ενδεικτικά τα ακόλουθα:

- Τίτλοι σπουδών
- Βαθμολογία τίτλων σπουδών
- Βαθμολογία μαθημάτων – και ιδιαίτερα της Πτυχιακής εργασίας ή Διπλωματικής εργασίας – εφόσον είναι συναφή με το αντικείμενο του Π.Μ.Σ.
- Κατοχή δεύτερου πτυχίου/διπλώματος ή μεταπτυχιακού τίτλου σπουδών
- Πεδίο και διάρκεια εργασιακής και ερευνητικής εμπειρίας
- Συστατικές επιστολές από μέλη Δ.Ε.Π. ΑΕΙ ή/και από εργοδότη
- Συνέντευξη εξ αποστάσεως με χρήση ψηφιακών μέσων
- Πρόσθετα κριτήρια που ορίζει με απόφασή της η Συνέλευση του Τμήματος

Η Συνέλευση δύναται να συγκροτεί Επιτροπή Πρόσθετων Εσωτερικών Εξετάσεων, κατόπιν πρότασης της Επιτροπής Επιλογής, για όλους ή για μερικούς υποψηφίους. Την ύλη και τον χρόνο των εξετάσεων αυτών καθορίζει η Επιτροπή Επιλογής.

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

- Καταρτίζει πλήρη κατάλογο όσων έχουν υποβάλει αίτηση
- Απορρίπτει τους υποψηφίους που δεν πληρούν τα ελάχιστα κριτήρια σε περίπτωση που έχουν τεθεί τέτοια από τη Συνέλευση και περιλαμβάνονται στον Κανονισμό Λειτουργίας του Π.Μ.Σ. ή ο φάκελος τους είναι ελλιπής ως προς κάποιο δικαιολογητικό/έγγραφο
- Καλεί σε συνέντευξη όσους υποψηφίους αποφασισθεί να κληθούν. Η συνέντευξη διεξάγεται από τα μέλη της Επιτροπής Επιλογής εξ αποστάσεως με χρήση ψηφιακών μέσων

- Οργανώνει τυχόν εσωτερικές εξετάσεις για τους υποψηφίους που θα κριθεί απαραίτητο
- Ιεραρχεί βαθμολογικά τους υποψηφίους και υποβάλλει την πρότασή της για την τελική έγκριση στη Συνέλευση.

Οι επιτυχόντες και επιτυχούσες θα πρέπει να εγγραφούν στη Γραμματεία του Τμήματος σε προθεσμία που θα οριστεί από τη Συνέλευση του Τμήματος. Σε περίπτωση ισοβαθμίας, όλοι οι ισοβαθμήσαντες και ισοβαθμήσασες με τον τελευταίο ή τελευταία θεωρούνται επιτυχόντες και επιτυχούσες.

Σε περίπτωση μη εγγραφής ενός ή περισσοτέρων επιλεγέντων και επιλεγεισών, θα κληθούν, αν υπάρχουν, να εγγραφούν στο Πρόγραμμα ισάριθμοι επιλαχόντες και επιλαχούσες, με βάση τη σειρά τους στον εγκεκριμένο αξιολογικό πίνακα.

3.6 Αξιολόγηση των υποψηφίων

Η αξιολόγηση των υποψήφιων για το Π.Μ.Σ. γίνεται από Επιτροπή Αξιολόγησης Υποψηφίων, η οποία αποτελείται από Καθηγητές και Καθηγήτριες του Τμήματος με βάση τα κριτήρια που αναφέρονται στον Κανονισμό Λειτουργίας, καθώς και προσωπική συνέντευξη εξ αποστάσεως με χρήση ψηφιακών μέσων (π.χ. μέσω MS-Teams κ.ά.).

Η πρώτη φάση της αξιολόγησης είναι προκριματική και γίνεται με βάση στοιχεία που συνάγονται από τα υποβληθέντα απαραίτητα δικαιολογητικά.
Τα κριτήρια κατά την πρώτη φάση είναι τα εξής:

Κριτήριο	Βαρύτητα
Γνωσιολογικό υπόβαθρο	30%
Σύνολο δεξιοτήτων	30%
Αναλυτική – συνθετική ικανότητα	20%

Το σύνολο μορίων από την πρώτη φάση αξιολόγησης έχει συντελεστή βαρύτητας στην τελική βαθμολογία ίσο προς 80%.

Η δεύτερη φάση περιλαμβάνει προσωπική συνέντευξη όλων των υποψηφίων, στην οποία κρίνεται η ιδιαίτερη κλίση, η δυναμική και η γενικότερη ακαδημαϊκή προσωπικότητα καθενός και καθεμιάς. Η δεύτερη φάση έχει συντελεστή βαρύτητας 20%.

3.7 Τέλη υποβολής υποψηφιοτήτων, φοίτησης και τρόπος καταβολής τους

Για **όλους τους κύκλους λειτουργίας** του ΠΜΣ, στο πλαίσιο υποβολής υποψηφιότητας οι ενδιαφερόμενες/οι καταβάλουν τέλος υποβολής υποψηφιότητας ύψους διακοσίων (200) ευρώ. Το τέλος αυτό δεν επιστρέφεται στις υποψήφιες και στους υποψήφιους, ανεξαρτήτως του αποτελέσματος της αξιολόγησης.

Για τους **πρώτους δύο (2) κύκλους λειτουργίας του ΠΜΣ** τα τέλη φοίτησης φοιτητριών και φοιτητών **προερχομένων από χώρες της ΕΕ** καλύπτονται καθ' ολοκληρίαν από το Ευρωπαϊκό έργο EU-iNSPIRE (EU **iN**novative multi-di**S**ci**P**linary **I**ndustry-focused cybersecurity education for upskilling and **R**eskilling the EU workforce**)** που χρηματοδοτείται από το πρόγραμμα DIGITAL-2023-SKILLS-05 (Αρ. Συμβολαίου 101190054). Για φοιτητές και φοιτήτριες που **προέρχονται από χώρες εκτός της ΕΕ** τα τέλη φοίτησης είναι πέντε χιλιάδες (5.000) ευρώ.

Από τον **τρίτο (3ο) κύκλο λειτουργίας του ΠΜΣ** τα τέλη φοίτησης φοιτητριών και φοιτητών **προερχομένων από χώρες της ΕΕ** είναι πέντε χιλιάδες (5.000) ευρώ, ενώ για φοιτητές και φοιτήτριες που **προέρχονται από χώρες εκτός της ΕΕ** τα τέλη φοίτησης είναι επτά χιλιάδες (7.000) ευρώ.

Σύμφωνα με τον Κανονισμό Μεταπτυχιακών Σπουδών τα τέλη φοίτησης καταβάλλονται σε δύο ισόποσες δόσεις: η πρώτη δόση με την ανακοίνωση όσων γίνονται δεκτοί στο Π.Μ.Σ. για δέσμευση της θέσης (Σεπτέμβριος), και η δεύτερη δόση κατά την έναρξη του 2ου ακαδημαϊκού εξαμήνου.

Η καταβολή των τελών υποβολής υποψηφιότητας και φοίτησης στον Ειδικό Λογαριασμό Κονδυλίων Έρευνας του Πανεπιστημίου Πειραιώς μπορεί να γίνει και με χρήση πιστωτικής ή χρεωστικής κάρτας.

Από τον **τρίτο (3ο) κύκλο λειτουργίας του ΠΜΣ** τα θέματα ρύθμισης για την απαλλαγή των φοιτητών και φοιτητριών από τα τέλη φοίτησης θα ακολουθούν την εν ισχύι νομοθεσία. Με βάση την κείμενη νομοθεσία, αριθμός φοιτητών και φοιτητριών που δεν υπερβαίνει το 30% του συνόλου και οι οποίοι δεν είναι πολίτες τρίτων χωρών (Διευκρίνιση: Τρίτη χώρα είναι κάθε χώρα που είναι εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Οι χώρες του ΕΟΧ είναι τα 28 κράτη-μέλη της Ευρωπαϊκής Ένωσης, καθώς και η Ισλανδία, η Νορβηγία και το Λιχτενστάιν), έχει δικαίωμα να απαλλαγεί εν όλω της καταβολής των τελών φοίτησης εφόσον πληρούνται συγκεκριμένα κριτήρια (Υπουργική Απόφαση «Ρύθμιση θεμάτων απαλλαγής από τα τέλη φοίτησης φοιτητών Προγράμματος Μεταπτυχιακών Σπουδών των Ελληνικών Α.Ε.Ι.» υπ' αριθμ. 108990/Ζ1/08.09.2022 (ΦΕΚ Β' 4899) στην οποία αναφέρονται τα δικαιολογητικά, και στην Υπουργική Απόφαση «Διαπίστωση του ποσού που αντιστοιχεί στο εθνικό διάμεσο διαθέσιμο ισοδύναμο εισόδημα (το ατομικό και το εβδομήντα τοις εκατό (70%) του οικογενειακού)» υπ' αριθ. 84560/Ζ1/27.07.2023 (ΦΕΚ 4837/01.08.2023)). Προϋπόθεση για τη χορήγηση του δικαιώματος δωρεάν φοίτησης λόγω οικονομικών ή κοινωνικών κριτηρίων (άρθρο 86 του ν. 4957/2022), είναι, επιπλέον, η πλήρωση των προϋποθέσεων

αριστείας κατά τον πρώτο κύκλο σπουδών, δηλαδή κατ' ελάχιστον κατοχή βασικού πτυχίου με βαθμό ίσο ή ανώτερο του επτά μισή με άριστα το δέκα (7.5/10). Στους επιλεγέντες φοιτητές και επιλεγείσες φοιτήτριες που θα απαλλαγούν των τελών φοίτησης, τα μέχρι εκείνη τη στιγμή καταβληθέντα τέλη επιστρέφονται εν όλω. Η απαλλαγή αυτή παρέχεται αποκλειστικά για τη φοίτηση σε ένα (1) Π.Μ.Σ. που οργανώνεται από Α.Ε.Ι. της ημεδαπής.

3.8 Εγγραφές μεταπτυχιακών φοιτητών και φοιτητριών

Η εγγραφή των εισακτέων μεταπτυχιακών φοιτητών και φοιτητριών κάθε έτους γίνεται σε προθεσμίες που ανακοινώνονται από τον Διευθυντή του Π.Μ.Σ.

Ο/Η υποψήφιος/α, πριν εγγραφεί:

- λαμβάνει γνώση ότι με το νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΕΕ) 2016/679 που τέθηκε σε εφαρμογή την 25η Μαΐου 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της Ε.Ε. Στο πλαίσιο αυτό ενημερώνεται ότι, σύμφωνα με την ισχύουσα νομοθεσία για τη διαδικασία εγγραφής των επιτυχόντων σε Προγράμματα Μεταπτυχιακών Σπουδών (Π.Μ.Σ.), το Πανεπιστήμιο Πειραιώς τηρεί δεδομένα προσωπικού χαρακτήρα των μεταπτυχιακών φοιτητών και φοιτητριών του. Επίσης ενημερώνεται ότι το Πανεπιστήμιο Πειραιώς συλλέγει συμπληρωματικά στοιχεία των μεταπτυχιακών φοιτητών και φοιτητριών του, στα οποία περιλαμβάνονται δεδομένα προσωπικού χαρακτήρα. Η τήρηση και η επεξεργασία των παραπάνω δεδομένων πραγματοποιείται με στόχο την εγγραφή και στη συνέχεια την ακαδημαϊκή διαχείρισή του, την επικοινωνία του με τους οικείους του σε περιπτώσεις έκτακτης ανάγκης, καθώς επίσης και την εξασφάλιση πρόσβασής του σε παρεχόμενες ηλεκτρονικές υπηρεσίες, καθ' όλη τη διάρκεια των σπουδών του.
- παρέχει τη συγκατάθεσή του για την τήρηση και επεξεργασία των προσωπικών του δεδομένων για όλους τους προαναφερόμενους σκοπούς επεξεργασίας
- δηλώνει ότι τα στοιχεία που έχει υποβάλλει καθώς και τα δικαιολογητικά είναι ακριβή, αληθή και γνήσια αντίγραφα των πρωτοτύπων
- λαμβάνει γνώση του Κανονισμού Μεταπτυχιακών Σπουδών και δηλώνει εγγράφως ότι αποδέχεται τους κανόνες λειτουργίας του προγράμματος
- δηλώνει το email του στο οποίο επιθυμεί να λαμβάνει προσωποποιημένη αλληλογραφία.

Πληροφορίες εγγραφής αναρτώνται στην ιστοσελίδα του Π.Μ.Σ.

3.9 Χρονική Διάρκεια Φοίτησης

Η χρονική διάρκεια σπουδών του Π.Μ.Σ. για την απονομή του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) ορίζεται σε τρία (3) εξάμηνα.

Τα δύο (2) πρώτα ακαδημαϊκά εξάμηνα περιλαμβάνουν διδασκαλία μαθημάτων, ενώ το τρίτο ακαδημαϊκό εξάμηνο την εκπόνηση Μεταπτυχιακής Διπλωματικής Εργασίας. Καθ' όλη τη διάρκεια του κύκλου σπουδών οι μεταπτυχιακοί φοιτητές και φοιτήτριες θα ενημερώνονται και για διαλέξεις σεμιναριακού χαρακτήρα που θα προγραμματίζονται.

Ο ανώτατος επιτρεπόμενος χρόνος ολοκλήρωσης των σπουδών, ορίζεται στα πέντε (5) ακαδημαϊκά εξάμηνα. Συγκεκριμένα, μεταπτυχιακοί φοιτητές και φοιτήτριες δικαιούνται ένα (1) ακαδημαϊκό εξάμηνο επιπλέον της προβλεπόμενης διάρκειας φοίτησής τους προκειμένου να ολοκληρώσουν τις μεταπτυχιακές τους σπουδές. Επιπλέον, με απόφαση της Συνέλευσης του Τμήματος κατόπιν εισήγησης της Σ.Ε. του Π.Μ.Σ., μπορεί να χορηγηθεί παράταση του προβλεπόμενου χρονικού ορίου των (3+1) αυτών ακαδημαϊκών εξαμήνων, μετά από αίτηση των ενδιαφερομένων και μόνο για σοβαρούς ανυπαίτιους λόγους, όπως επαγγελματικοί λόγοι και λόγοι υγείας. Σε κάθε περίπτωση η αίτηση του ενδιαφερομένου ή ενδιαφερόμενης πρέπει να συνοδεύεται από τα σχετικά δικαιολογητικά τεκμηρίωσης του αιτήματος.

Οι μεταπτυχιακοί φοιτητές και φοιτήτριες, με αίτησή τους, μπορούν να ζητήσουν αιτιολογημένα προσωρινή αναστολή φοίτησης η οποία δεν υπερβαίνει τα δύο (2) συνεχόμενα ακαδημαϊκά εξάμηνα. Τα εξάμηνα αναστολής της φοιτητικής ιδιότητας δεν προσμετρώνται στην προβλεπόμενη ανώτατη διάρκεια κανονικής φοίτησης. Η δυνατότητα χορήγησης αναστολής φοίτησης σε μεταπτυχιακό φοιτητή ή φοιτήτρια πραγματοποιείται μετά από αίτησή τους, πρόταση της Σ.Ε. του Π.Μ.Σ. και απόφαση της Συνέλευσης του Τμήματος. Στην αίτησή του ο μεταπτυχιακός φοιτητής ή η φοιτήτρια αναφέρει υποχρεωτικώς τους λόγους, το χρονικό διάστημα της αιτούμενης αναστολής φοίτησης και επισυνάπτει τα σχετικά τυχόν δικαιολογητικά.

3.10 Ευρωπαϊκό Σύστημα Μεταφοράς Πιστωτικών Μονάδων

Το Ευρωπαϊκό Σύστημα Μεταφοράς Ακαδημαϊκών Μονάδων (European Credit Transfer System, ECTS) αποτελεί εργαλείο του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης (ΕΧΑΕ) με σκοπό τη μεγαλύτερη διαφάνεια των σπουδών και κατά συνέπεια τη βελτίωση της ποιότητας της Ανώτατης Εκπαίδευσης. Σκοπός του είναι να ενισχύσει και να διευκολύνει τις διαδικασίες ακαδημαϊκής αναγνώρισης μεταξύ συνεργαζόμενων ιδρυμάτων της Ευρώπης με διαφορετικά εθνικά συστήματα εκπαίδευσης, με τη χρήση απλών και εφαρμόσιμων μηχανισμών.

3.10.1 Πιστωτικές Μονάδες του Προγράμματος Σπουδών

Ο αριθμός πιστωτικών μονάδων του κάθε μαθήματος του Π.Μ.Σ. καταδεικνύει τον φόρτο εργασίας, τον οποίο απαιτείται να καταβάλλει κάθε μεταπτυχιακός φοιτητής και φοιτήτρια για να επιτύχει τους αντικειμενικούς στόχους μιας εκπαιδευτικής συνιστώσας, ανάλογα με τα εκάστοτε μαθησιακά αποτελέσματα και τις γνώσεις, ικανότητες και δεξιότητες που επιδιώκεται να αποκτηθούν μετά την επιτυχή ολοκλήρωσή της. Στον φόρτο εργασίας περιλαμβάνονται όλες οι προγραμματισμένες δραστηριότητες μάθησης, όπως διαλέξεις,

σεμινάρια, μελέτη, προετοιμασία εργασιών, εξετάσεις κ.λπ.

3.10.2 Φόρτος Εργασίας

Ο φόρτος εργασίας συνίσταται στον χρόνο που υπολογίζεται ότι χρειάζεται τυπικά να αφιερώσει ένας μεταπτυχιακός φοιτητής ή φοιτήτρια για να ολοκληρώσει όλες τις μαθησιακές δραστηριότητες (όπως παρακολούθηση παραδόσεων, σεμινάρια, εργασίες, ανεξάρτητη προσωπική μελέτη και εξετάσεις) που απαιτούνται για την επίτευξη των αναμενόμενων μαθησιακών αποτελεσμάτων. Αριθμός εξήντα (60) πιστωτικών μονάδων ECTS αντιστοιχούν στον φόρτο εργασίας ενός ακαδημαϊκού έτους τυπικής μάθησης πλήρους φοίτησης και τα συναφή μαθησιακά αποτελέσματα. Στην αντιστοίχιση που έχει πραγματοποιηθεί για τα μαθήματα του Π.Μ.Σ., μία πιστωτική μονάδα (ΠΜ) έχει αντιστοιχηθεί με είκοσι πέντε (25) ώρες φόρτου εργασίας.

3.10.3 Απόδοση πιστωτικών μονάδων

Για τη λήψη διπλώματος στο Π.Μ.Σ. απαιτείται η συσσώρευση 90 ΠΜ (ECTS). Ο αριθμός των πιστωτικών μονάδων που αποδίδονται σε κάθε συνιστώσα βασίζεται στη βαρύτητά της από την άποψη του φόρτου εργασίας που χρειάζονται οι μεταπτυχιακοί φοιτητές και φοιτήτριες ώστε να επιτύχουν τα μαθησιακά αποτελέσματα σε πλαίσιο τυπικής εκπαίδευσης.

3.10.4 Μεταφορά πιστωτικών μονάδων (ECTS)

Οι πιστωτικές μονάδες που απονέμονται σε ένα πρόγραμμα μπορούν να μεταφερθούν σε άλλο πρόγραμμα που προσφέρει το ίδιο ή διαφορετικό ίδρυμα. Η μεταφορά αυτή μπορεί να γίνει μόνον εάν το ίδρυμα που χορηγεί τον τίτλο σπουδών αναγνωρίζει τις πιστωτικές μονάδες και τα συνδεόμενα με αυτές μαθησιακά αποτελέσματα. Το Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» συμμορφώνεται με το Ευρωπαϊκό Σύστημα Μεταφοράς Πιστωτικών Μονάδων και εφαρμόζει πλήρη διαδικασία μεταφοράς και αναγνώρισης των ακαδημαϊκών μονάδων μαθημάτων. Το σύστημα εφαρμογής και συσσώρευσης ακαδημαϊκών μονάδων έχει θεσμοθετηθεί και εφαρμόζεται και σε κάθε περίπτωση που εκπαιδευτικές δραστηριότητες του οδηγού σπουδών του Π.Μ.Σ. είναι αντίστοιχης ύλης και ανάλογου επιπέδου με εκπαιδευτικές δραστηριότητες στις οποίες έχει εξετασθεί επιτυχώς ο μεταπτυχιακός φοιτητής ή φοιτήτρια σε προηγούμενη ολοκληρωμένη ή μη φοίτησή του.

3.11 Γλώσσα Προγράμματος

Η διδασκαλία των μαθημάτων γίνεται στην αγγλική γλώσσα. Επίσης, η βιβλιογραφία περιλαμβάνει επιστημονικά άρθρα και συγγράμματα στην αγγλική γλώσσα.

3.12 Διδακτικό Προσωπικό

Στους διδάσκοντες και διδάσκουσες του Προγράμματος Μεταπτυχιακών Σπουδών Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση περιλαμβάνονται διακεκριμένοι Καθηγητές και Καθηγήτριες Πανεπιστημίων της χώρας και της αλλοδαπής, διδάκτορες Ερευνητές και Ερευνήτριες, καθώς και προβεβλημένα στελέχη Ανεξάρτητων Αρχών, Δημοσίων Οργανισμών και Επιχειρήσεων του ιδιωτικού τομέα, όλες και όλοι με εξαιρετικές σπουδές, προερχόμενοι από τον χώρο των Τεχνολογιών Πληροφορικής και Επικοινωνιών και της Κυβερνοασφάλειας, με σημαντικές γνώσεις και ξεχωριστές εμπειρίες από διεθνώς προηγμένα επιστημονικά περιβάλλοντα.

Στο πλαίσιο του παρόντος ΠΜΣ έχουν συμφωνήσει να συμμετάσχουν στην εκπαιδευτική διαδικασία τα ακόλουθα Πανεπιστημιακά Ιδρύματα: Technical University of Munich (Γερμανία), University of Oslo (Νορβηγία), University of Malaga (Ισπανία), Open University of Cyprus (Κύπρος), ενώ το Business School της École des Ponts (Γαλλία) θα υποστηρίξει το πρόγραμμα με διακεκριμένους καθηγητές και καθηγήτριες για στοχευμένες διαλέξεις σεμιναριακού χαρακτήρα. Με την ενεργό υποστήριξη των εν λόγω πανεπιστημίων, διακεκριμένοι καθηγητές και ερευνητές θα συμβάλουν στη διδασκαλία του Π.Μ.Σ., ενισχύοντας τον διεθνή και διεπιστημονικό χαρακτήρα του.

3.12.1 Διευθυντής του Π.Μ.Σ.

Ο Καθηγητής **Κωνσταντίνος Λαμπρινουδάκης** έχει πτυχίο Ηλεκτρολόγου και Ηλεκτρονικού Μηχανικού από το Πανεπιστήμιο του Salford UK, M.Sc. σε Συστήματα Αυτομάτου Ελέγχου από το Imperial College και Ph.D. από το University of London, Queen Mary and Westfield College. Την περίοδο 1998-2009 εργάστηκε στο Πανεπιστήμιο Αιγαίου, ως μέλος ΔΕΠ του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Από τον Ιούνιο 2009 μέχρι και σήμερα υπηρετεί στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς (από το 2017 ως Καθηγητής). Από το 2015 είναι Πρόεδρος του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς και Διευθυντής του Εργαστηρίου Ασφάλειας Συστημάτων (Secure Systems Laboratory). Από το 2016 είναι Τακτικό Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Στο διάστημα 2012-2015 διατέλεσε Τακτικό Μέλος της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών. Τα τρέχοντα επιστημονικά ενδιαφέροντα του συμπεριλαμβάνουν τους τομείς της ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων και της προστασίας της ιδιωτικότητας. Είναι συγγραφέας περισσότερων των 120 ερευνητικών εργασιών σε διεθνή επιστημονικά περιοδικά, βιβλία και πρακτικά συνεδρίων στους τομείς ενδιαφέροντός του. Επίσης συμμετέχει στην Επιστημονική Επιτροπή Προγράμματος (Program Committee) σε περισσότερα από 200 διεθνή επιστημονικά συνέδρια,

ενώ σε 15 από αυτά είναι Πρόεδρος της Επιστημονικής Επιτροπής. Επίσης είναι μέλος της συντακτικής επιτροπής και κριτής ερευνητικών εργασιών σε περισσότερα από 35 διεθνή επιστημονικά περιοδικά Έχει συμμετάσχει σε πλήθος χρηματοδοτούμενων ερευνητικών, μελετητικών και αναπτυξιακών έργων, τόσο στην Ελλάδα όσο και στην Ευρώπη (https://www.ds.unipi.gr/faculty/clam/).

3.12.2 Διδάσκοντες και Διδάσκουσες

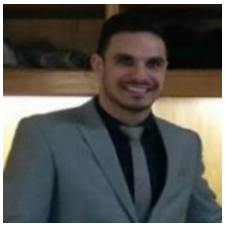
Ο **Στέφανος Γκρίτζαλης** είναι Καθηγητής Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς (6.2019+) και διατελεί Διευθυντής του Προγράμματος Μεταπτυχιακών Σπουδών "Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών (MSc in Law and ICT)" (06.2020+). Είναι Μέλος της Ανεξάρτητης Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) (12.2020+). Είναι Μέλος της Εθνικής Επιτροπής για τα Δικαιώματα του Ανθρώπου (ΕΕΔΑ) (09.2024+). Διετέλεσε Πρύτανης στο Πανεπιστήμιο Αιγαίου (09.2014-08.2018). Διετέλεσε Ειδικός Γραμματέας στο Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης (11.2009-10.2012). Νωρίτερα ήταν Καθηγητής στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων της Πολυτεχνικής Σχολής του Πανεπιστημίου Αιγαίου (2002-2019), Πρόεδρος του Τμήματος (2005-2009), Αναπληρωτής Προέδρου του Τμήματος (2012-2014) και Διευθυντής του Εργαστηρίου Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων (2005-2009). Έχει δραστηριοποιηθεί επί 30 και πλέον χρόνια σε σειρά διεθνών και εθνικών έργων Έρευνας και Ανάπτυξης (Horizon 2020, IST FP7/FP6/FP5, DGXIII Telematics / ETS-II / ETS-I / Telematics for Administration / Value II / Healthcare Telematics, DG XVI Feder, GSRT κ.λπ.). Σύμφωνα με την κατάταξη "2023 World's Top 2% Scientists", από ερευνητές του Stanford που δημοσίευσε η Elsevier τον Σεπτέμβριο 2024, περιλαμβάνεται, για μία ακόμη χρονιά, στο 2% των κορυφαίων επιστημόνων σε όλο τον κόσμο, με κριτήριο αξιολόγησης τις αναφορές που έλαβε το συνολικό ερευνητικό έργο του κατά τη διάρκεια της τριακονταετούς καριέρας του. Έχει συγγράψει ή επιμεληθεί 14 Βιβλία, έχει επιμεληθεί τα Πρακτικά 35 και πλέον Διεθνών Συνεδρίων (IEEE, ACM, Springer κ.α.), έχει συγγράψει 37 Κεφάλαια Βιβλίων, έχει δημοσιεύσει 336 επιστημονικά άρθρα (151 άρθρα σε διεθνή Επιστημονικά Περιοδικά και 185 σε Πρακτικά Διεθνών Συνεδρίων με έκδοση Πρακτικών). Διατελεί Area Editor στο κορυφαίο περιοδικό IEEE Communications Surveys and Tutorials (ImpactFactor=46.7 (Clarivate JCR Report), No. 1 στα 120 περιοδικά για Τηλεπικοινωνίες και No. 1 στα 259 περιοδικά για την Επιστήμη των Υπολογιστών και Πληροφοριακά Συστήματα). Είναι Μέλος

Συντακτικής Επιτροπής (Editorial Board Member) σε 35 περιοδικά, Κριτής (Reviewer) σε 80 διεθνή Επιστημονικά Περιοδικά και έχει διατελέσει Προσκεκλημένος Εκδότης (Guest Editor) 35 φορές σε Επιστημονικά Περιοδικά. Έχει διατελέσει Πρόεδρος Συνεδρίου (General Chair) ή Πρόεδρος Επιτροπής Προγράμματος (PC Chair) σε 50 διεθνή συνέδρια, Μέλος Επιτροπής Προγράμματος (PC Member) σε περισσότερα από 600 διεθνή συνέδρια και έχουν καταγραφεί περισσότερες από 11.000 Αναφορές (citations) στο έργο του με h-index=55, i-10 index=178 κατά Google Scholar. Έχει επιβλέψει την εκπόνηση 17 διδακτορικών διατριβών που έχουν περατωθεί επιτυχώς. Οι επιστήμονες αυτοί έχουν σημαντική ακαδημαϊκή και επαγγελματική εξέλιξη στην Ελλάδα και το εξωτερικό (π.χ. TU Delft, University of the Aegean, University of Crete, ENISA, European Commission JRC, Volvo group, Hellenic Ministry of Digital Governance, TEIRESIAS SA, Hellenic Statistical Authority, Hellenic Civil Aviation Authority, Hellenic Ministry of Education κ.λπ.). Επιπλέον, έχει διατελέσει μέλος επιτροπής αξιολόγησης / εξωτερικός αξιολογητής 60 και πλέον υποψηφίων διδακτόρων στην Ελλάδα, τη Γερμανία, την Ιταλία, την Ισπανία, το Πακιστάν και την Ινδία. Έχει επιβλέψει περισσότερες από 150 Μεταπτυχιακές Διπλωματικές Εργασίες και 300 Πτυχιακές Εργασίες. Έχει οριστεί εμπειρογνώμονας για την αξιολόγηση προτάσεων έργων και υποψηφιοτήτων από πλήθος ελληνικών και διεθνών φορέων: ERC European Research Council, Swiss National Science Foundation, Italian Ministry of University and Research, The Netherlands Organisation for Scientific Research, Belgian Fund for Scientific Research, Czech Science Foundation, FFG Austrian Research Promotion Agency, ETH Zurich Research Commission, Croatian Ministry of Science and Education, Slovenian Research Agency, South Africa's National Research Foundation, Qatar Foundation National Research Fund, Cyprus Research Promotion Foundation, The University of Nicosia Research Foundation Cyprus, Hellenic Foundation for Research and Innovation, Hellenic General Secretariat for Research and Technology, Hellenic State Scholarship Foundation, Hellenic Ministry of Economy and Development ESF Operational Programme "HR Development Education and Life Long Learning". Έχει διατελέσει Αξιολογητής σε διαγωνισμούς μεγάλων έργων Πληροφορικής και Τηλεπικοινωνιών του Δημόσιου Τομέα, ενώ έχει οριστεί Εμπειρογνώμονας για την Ελληνική Δικαιοσύνη σε θέματα Ασφάλειας Επικοινωνιών και Προστασίας της Ιδιωτικότητας. (https://www.ds.unipi.gr/faculty/sgritz/).

Ο Δρ. Χρήστος Καλλονιάτης είναι κάτοχος πτυχίου Μηχανικού Πληροφορικής από το ΑΤΕΙ Αθήνας, μεταπτυχιακού διπλώματος από το Τμήμα Πληροφορικής του Πανεπιστημίου του Essex και διδακτορικού διπλώματος από το Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας του Πανεπιστημίου Αιγαίου. Σήμερα υπηρετεί ως Καθηγητής στο Τμήμα Πολιτισμικής Τεχνολογίας και Επικοινωνίας του Πανεπιστημίου Αιγαίου και είναι διευθυντής του εργαστηρίου PrivaSI «Τεχνολογίες Προστασίας της Ιδιωτικότητας και Εφαρμογές Πληροφορικής στις Κοινωνικές Επιστήμες». Υπηρέτησε ως Πρόεδρος του Τμήματος από το 2020-2024 και ως αναπληρωτής προέδρου από το 2017 έως το 2020 στο ίδιο τμήμα. Είναι τακτικό μέλος της ολομέλειας της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ενώ έχει υπηρετήσει και ως μέλος της ολομέλειας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν την ανάλυση και μοντελοποίηση απαιτήσεων ασφάλειας και ιδιωτικότητας σε παραδοσιακά πληροφοριακά συστήματα καθώς και σε περιβάλλοντα νεφοϋπολογιστικής, και τεχνητής νοημοσύνης, τις τεχνολογίες προστασίας της ιδιωτικότητας καθώς και τα ζητήματα που αφορούν την ασφάλεια και προστασία της ιδιωτικότητας σε πολιτισμικά πληροφοριακά συστήματα. Είναι συγγραφέας σε πάνω από 150 άρθρα σε διεθνή περιοδικά και συνέδρια με κριτές και επισκέπτης καθηγητής σε ευρωπαϊκά πανεπιστήμια. Πριν ξεκινήσει την ακαδημαϊκή του καρίερα, ο Δρ. Χρήστος Καλλονιάτης υπηρέτησε σε διάφορες θέσεις στη δημόσια διοίκηση, όπως στην Περιφέρεια Βορείου Αιγαίου και το Υπουργείο Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης. Είναι συνεργάτης του εργαστηρίου Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου καθώς και του Εργαστηρίου Ασφαλών Συστημάτων του Πανεπιστημίου Πειραιώς. Έχει συμμετάσχει σε πλήθος ερευνητικών και αναπτυξιακών προγραμμάτων. (https://kalloniatis.aegean.gr/).

Ο **Χαράλαμπος Βρασίδας** είναι Καθηγητής με γνωστικό αντικείμενο την Εκπαιδευτική Τεχνολογία και Καινοτομία και Αναπληρωτής Κοσμήτορας για την εξ αποστάσεως εκπαίδευση στο Πανεπιστήμιο Λευκωσίας. Είναι συνιδρυτής και Εκτελεστικός Διευθυντής του CARDET (Center for the Advancement of Research and Development in Educational Technology (Κέντρο για την Προώθηση της Έρευνας και Ανάπτυξης στην Εκπαιδευτική Τεχνολογία), ενός μη κυβερνητικού, μη κερδοσκοπικού ερευνητικού και αναπτυξιακού κέντρου με έδρα την Κύπρο και συνεργάτες σε όλο τον κόσμο. Αποφοίτησε από την Παιδαγωγική Ακαδημία Κύπρου (ΠΑΚ) τον Ιούνιο του 1989. Η ΠΑΚ ήταν η επίσημη σχολή εκπαίδευσης δασκάλων για τα δημοτικά

σχολεία και πλέον έχει γίνει το Πανεπιστήμιο Κύπρου. Τον Σεπτέμβριο του 1991 διορίστηκε ως δάσκαλος δημοτικής εκπαίδευσης. Μετά από ένα χρόνο υπηρεσίας, έλαβε μία υποτροφία Φουλμπράιτ για να σπουδάσει στις Ηνωμένες Πολιτείες. Εκεί απέκτησε πτυχίο σε Φωτογραφία/Πολυμέσα με δευτερεύον αντικείμενο τον Κινηματογράφο από το Πανεπιστήμιο του Δυτικού Ιλινόι (Western Illinois University - WIU). Στη συνέχεια συνέχισε με Μεταπτυχιακές Σπουδές στην Εκπαίδευση με έμφαση στην Εκπαιδευτική Τεχνολογία και τις Τηλεπικοινωνίες, επίσης στο WIU. Τον Αύγουστο του 1996 εντάχθηκε στο διδακτορικό πρόγραμμα στα Εκπαιδευτικά Μέσα και Υπολογιστές στο Πανεπιστήμιο της Πολιτείας της Αριζόνα (Arizona State University) και έλαβε το διδακτορικό του τον Μάιο του 1999. (https://www.unic.ac.cy/el/vrasidas-charalambos/).



Ο Δρ. **Μαρίνος Παπαϊωακείμ** είναι ερευνητής με ειδίκευση στις διεθνείς σχέσεις, τη διπλωματία, και την άμυνα και ασφάλεια, με ιδιαίτερη έμφαση στον ρόλο των μικρών κρατών στη διακυβέρνηση της ασφάλειας και τη διπλωματία άμυνας. Είναι κάτοχος διδακτορικού (PhD) στη Διπλωματία και Διεθνείς Σχέσεις από το Πανεπιστήμιο Κύπρου, όπου η διδακτορική του διατριβή εξέτασε τη χρήση της διπλωματίας άμυνας από μικρά κράτη σε παρατεταμένες συγκρούσεις. Τα ερευνητικά του ενδιαφέροντα περιλαμβάνουν, μεταξύ άλλων, την ασφάλεια, τη στρατιωτική και αμυντική διπλωματία, τις υβριδικές απειλές, την πολιτική και την "ήπια ισχύ" (soft power). Ο Δρ. Παπαϊωακείμ απέκτησε το μεταπτυχιακό του δίπλωμα (MA) στη Διπλωματία και Εξωτερική Πολιτική από το Πανεπιστήμιο του Λάνκαστερ (Lancaster University) (Ηνωμένο Βασίλειο), ενώ προηγήθηκε το πτυχίο του (BA) στην Ιστορία από το Πανεπιστήμιο Κύπρου. Έχει εργαστεί ως Ερευνητικός Συνεργάτης στη Νομική Σχολή του Πανεπιστημίου Λευκωσίας και έχει διατελέσει Διευθυντής της Βασιλικής Κοινότητας της Κοινοπολιτείας στην Κύπρο (Royal Commonwealth Society Cyprus). Επιπλέον, έχει διατελέσει Βοηθητικό Διδακτικό και Ερευνητικό Προσωπικό στο Τμήμα Κοινωνικών και Πολιτικών Επιστημών του Πανεπιστημίου Κύπρου, αναλαμβάνοντας διδακτικά και ερευνητικά καθήκοντα. Παράλληλα, έχει διατελέσει λέκτορας και καθηγητής σε διάφορα ακαδημαϊκά ιδρύματα, σε θέματα όπως η διπλωματία, οι διεθνείς σχέσεις, οι συγκρούσεις, η ασφάλεια και η άμυνα. Εργάζεται επί του παρόντος στο CARDET ως Έμπειρος Ερευνητής, Διαχειριστής Έργων και Επικεφαλής Τμήματος, με αρμοδιότητα τη διαχείριση πολλών έργων, κυρίως στον τομέα της ασφάλειας. Παράλληλα, υπηρετεί ως Ερευνητικός Συνεργάτης στην Διπλωματική Ακαδημία του Πανεπιστημίου Λευκωσίας και στο Ινστιτούτο Πολιτικής και Δημοκρατίας. (https://ucy.academia.edu/MarinosPapaioakeim).

Ο Δρ. **Mohammad Hamad** ηγείται της ερευνητικής ομάδας «Ασφάλεια για το Διαδίκτυο των Πραγμάτων (IoT) και Αυτόνομα Συστήματα» στην ομάδα Ενσωματωμένων Συστημάτων και Διαδικτύου των Πραγμάτων της Σχολής Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Πληροφορικής του Τεχνικού Πανεπιστημίου Μονάχου (Technical University of Munich - TUM). Πριν από αυτό, ο Δρ Hamad έλαβε το διδακτορικό του στην Μηχανική Υπολογιστών από το Τεχνικό Πανεπιστήμιο του Μπράουνσβαϊγκ (TU Braunschweig) το 2020. (https://www.ce.cit.tum.de/en/esi/staff/hamad/).

Ο **Audun Jøsang** είναι Καθηγητής Κυβερνοασφάλειας στο Πανεπιστήμιο του Όσλο (University of Oslo), καθώς και Επισκέπτης Καθηγητής στο Πανεπιστήμιο Τεχνολογίας του Κουίνσλαντ (Queensland University of Technology - QUT) στην Αυστραλία. Ο Καθ. Jøsang είναι ευρέως γνωστός για την έρευνά του στους τομείς των συστημάτων εμπιστοσύνης και φήμης σε ψηφιακά περιβάλλοντα, όπως ηλεκτρονικές αγορές και μέσα κοινωνικής δικτύωσης. Μία από τις βασικές του συνεισφορές είναι η ανάπτυξη της Υποκειμενικής Λογικής (Subjective Logic), ενός μαθηματικού πλαισίου για συλλογιστική υπό αβεβαιότητα, το οποίο έχει εφαρμογές σε τομείς όπως η εκτίμηση κινδύνου, η λήψη αποφάσεων, η τεχνητή νοημοσύνη και η ανάλυση εμπιστοσύνης σε κοινωνικά δίκτυα. Το έργο αυτό χρησιμοποιείται ευρέως τόσο στην ακαδημαϊκή κοινότητα όσο και στη βιομηχανία. Ο Καθ. Jøsang είναι κάτοχος μεταπτυχιακού τίτλου (MSc) στην Ασφάλεια Πληροφοριών από το Βασιλικό Κολλέγιο του Χόλογουεϊ του Πανεπιστημίου του Λονδίνου (Royal Holloway College, University of London), καθώς και μεταπτυχιακού τίτλου στις Τηλεπικοινωνίες από το Νορβηγικό Πανεπιστήμιο Επιστημών και Τεχνολογίας (Norwegian University of Science and Technology - NTNU), όπου απέκτησε επίσης και το διδακτορικό του. Ανάμεσα στα βιβλία που έχει συγγράψει περιλαμβάνονται τα: Subjective Logic: A Formalism for Reasoning Under Uncertainty και Cybersecurity: Technology and Governance. (https://www.mn.uio.no/ifi/english/people/aca/josang/).

Ο **László Erdődi** ζει στο Όσλο της Νορβηγίας, όπου είναι Επίκουρος Καθηγητής στο Πανεπιστήμιο του Όσλο (University Oslo - UiO), καθώς και στο Τμήμα Ασφάλειας Πληροφοριών και Τεχνολογίας Επικοινωνιών του Νορβηγικού Πανεπιστημίου Επιστημών και Τεχνολογίας (Norwegian University of Science and Technology - NTNU). Ο László Erdődi διαθέτει πάνω από 15 χρόνια εμπειρίας στον τομέα της ασφάλειας πληροφοριακών συστημάτων, με πληθώρα έργων ηθικού hacking, που περιλαμβάνουν εξειδικευμένες εργασίες όπως ανάπτυξη μεθόδων εκμετάλλευσης ευπαθειών (exploit) και

επιθέσεις σε δίκτυα ηλεκτρικής ενέργειας. Τα κύρια ερευνητικά του πεδία είναι οι επιθέσεις στον κυβερνοχώρο με τη βοήθεια ενισχυτικής μάθησης (reinforcement learning) και η ασφάλεια των ηλεκτρικών δικτύων. Είναι επίσης επικεφαλής προπονητής της νορβηγικής φοιτητικής ομάδας. (https://www.mn.uio.no/ifi/english/people/aca/laszloe/index.html).

Η Δρ. Cristina Alcaraz είναι Επίκουρη Καθηγήτρια στο Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου της Μάλαγα (University of Malaga - UMA). Απέκτησε το διδακτορικό της στην Επιστήμη Υπολογιστών από το ίδιο πανεπιστήμιο το 2011 και μεταπτυχιακό δίπλωμα στην Επιστήμη Υπολογιστών επίσης από το UMA το 2006. Έλαβε δύο εξαιρετικά ανταγωνιστικές μεταδιδακτορικές υποτροφίες: την υποτροφία Marie-Curie το 2012 μέσω του προγράμματος COFUND και την υποτροφία Ramón-y-Cajal το 2015. Υπήρξε φιλοξενούμενη ερευνήτρια στο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST) (ΗΠΑ, 2011–2012), ενώ ακολούθως επισκέφθηκε το Royal Holloway (2012–2014 μέσω της μεταδιδακτορικής υποτροφίας Marie-Curie Confund), το UCBM (Ρώμη, 2017) και την εταιρεία Neurosoft (Αθήνα, 2019 και 2022). Η Δρ. Alcaraz, κατατάσσεται μεταξύ του κορυφαίου 2% των επιστημόνων παγκοσμίως από το 2020 έως σήμερα, έχει δημοσιεύσει πάνω από 95 επιστημονικά άρθρα (εκ των οποίων 40 είναι καταχωρημένα στη βάση JCR – 20 σε περιοδικά Q1, 15 σε Q2 και 5 σε Q3). Τα ερευνητικά της ενδιαφέροντα επικεντρώνονται στην ασφάλεια κυβερνο-φυσικών συστημάτων, τη Βιομηχανία 5.0/4.0, το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), τα ψηφιακά διδύμα και τα δίκτυα αεροδιαστημικής, με έμφαση στην επίγνωση της κατάστασης (situational awareness), την προηγμένη ανίχνευση και την ανθεκτικότητα. Είναι Επιμελήτρια του Τμήματος Τεχνολογίας Λειτουργιών (OT) στο IEEE, και Επίκουρη Συντάκτρια σε περισσότερα από 7 κορυφαία επιστημονικά περιοδικά στον τομέα της ασφάλειας, όπως τα: IEEE Transactions on Industrial Informatics, IEEE Transactions on Dependable and Secure Computing, International Journal of Critical Infrastructure Protection, International Journal of Information Security, Distributed Ledger Technologies (ACM), IEEE Networking Letters, μεταξύ άλλων. Σε ακαδημαϊκό επίπεδο διδάσκει τακτικά κυβερνοασφάλεια σε σχέση με την ασφάλεια δικτύων και τη βιομηχανική ασφάλεια, τόσο σε προπτυχιακό όσο και σε μεταπτυχιακό επίπεδο. Αξιοσημείωτο είναι ότι τιμήθηκε με την «Ειδική Μνεία για την Ποιότητα Διδασκαλίας» (Special Mention for Teaching Quality) και το «Βραβείο Αριστείας στη Διδασκαλία» (Teaching Excellence) από το Διεθνές Πανεπιστήμιο της Ανδαλουσίας (International University of Andalusia) το 2023 και 2024 αντίστοιχα. Το 2021 της απονεμήθηκε η διάκριση «Γυναίκες στην Εθνική Ασφάλεια»

(Women in Homeland Security) από την Τεχνική Επιτροπή του IEEE της Κοινωνίας Συστημάτων Ανθρώπου και Κυβερνητικής στην Εθνική Ασφάλεια (IEEE SMC TC on Homeland Security), ενώ είναι Αντιπρόεδρος της Ομάδας Ειδικού Ενδιαφέροντος (SIG) του IEEE ComSoc για τα Πράσινα Δίκτυα Ψηφιακών Διδύμων (Green Digital Twin Network). (https://www.nics.uma.es/cristina-alcaraz/).

Ο Καθηγητής **Σταύρος Σταύρου** κατέχει διδακτορικό τίτλο σπουδών στις Τηλεπικοινωνίες από το Πανεπιστήμιο του Surrey (Μεγάλη Βρετανία) και η περιοχή εμπειρογνωμοσύνης του επικεντρώνεται στην Κυβερνοασφάλεια, στα Συστήματα / Δίκτυα Τηλεπικοινωνιών και σε συνυφασμένα θέματα ασφάλειας. Τα ερευνητικά του ενδιαφέροντα εντοπίζονται μεταξύ του πρώτου (physical) και τρίτου (network) επίπεδου (OSI layer stack). Έχει δημοσιεύσει εκτενώς σε έγκριτα διεθνή περιοδικά και συνέδρια και έχει επιβλέψει διδακτορικούς φοιτητές στα πιο πάνω θέματα των ερευνητικών του ενδιαφερόντων. Έχει συγγράψει και διαχειρισθεί μεγάλο αριθμό ερευνητικών προτάσεων για σκοπούς βασικής και εφαρμοσμένης έρευνας και για σκοπούς ανάπτυξης επιχειρησιακών πλατφόρμων. Ο Καθηγητής Σταύρου έχει συνεργαστεί με ευρωπαϊκούς και εθνικούς ερευνητικούς, κυβερνητικούς και άλλους οργανισμούς. Είναι κριτής σε επιστημονικά περιοδικά και κάτοχος διπλώματος ευρεσιτεχνίας ενός παρεμβολέα ασύρματων συστημάτων. Είναι Fellow της Ανώτερης Ακαδημίας Τριτοβάθμιας Εκπαίδευσης της Μεγάλης Βρετανίας, ο πρώτος εκλεγμένος πρόεδρος του σχηματισμού Κυβερνοασφάλειας του Ευρωπαϊκού Κολλεγίου Άμυνας και Ασφάλειας (European Security and Defense College - ESDC), μέλος του εκτελεστικού Ακαδημαϊκού Συμβουλίου του ESDC, το οποίο δραστηριοποιείται στον τομέα της κοινής Ευρωπαϊκής πολιτικής άμυνας και ασφάλειας, καθώς και μέλος του Συμβουλίου του Φορέα Διασφάλισης και Πιστοποίησης της Ποιότητας της Ανώτερης Εκπαίδευσης (ΔΙΠΑΕ). (https://www.ouc.ac.cy/index.php/el/profiles/stavros-stavrou).

Η Δρ. **Ιλιάνα Σταύρου** σπούδασε στο Πανεπιστήμιο Κύπρου όπου έλαβε διδακτορικό τίτλο στην Επιστήμη της Πληροφορικής (Κυβερνοασφάλεια) και είναι κάτοχος Μεταπτυχιακού τίτλου σε Προηγμένες Τεχνολογίες Πληροφορικής από το ίδιο Πανεπιστήμιο. Τα ερευνητικά της ενδιαφέροντα επικεντρώνονται στον τομέα της εκπαίδευσης σε θέματα κυβερνοασφάλειας και στις προκλήσεις που σχετίζονται με την ανάπτυξη δεξιοτήτων. Μέσα από τις ερευνητικές της δραστηριότητες, η Δρ. Σταύρου διεξάγει εφαρμοσμένη έρευνα, αναπτύσσοντας εξειδικευμένα προγράμματα εκπαίδευσης και κατάρτισης με τη χρήση σύγχρονων εκπαιδευτικών μεθόδων και τεχνολογιών για αποτελεσματική μάθηση και αναβάθμιση

δεξιοτήτων κυβερνοασφάλειας. Συγκεκριμένα, η έρευνά της επικεντρώνεται στην καλλιέργεια δεξιοτήτων ανθεκτικότητας (cyber resilience) μέσω της προώθησης μιας κουλτούρας επίγνωσης της κατάστασης στον κυβερνοχώρο ('cyber situational awareness'). Στο πλαίσιο ανάπτυξης μιας τέτοιας κουλτούρας, διερευνά και καθορίζει το προφίλ κυβερνοαπειλών σε διαφορετικά περιβάλλοντα, π.χ. ΜΜΕ, κρίσιμα συστήματα πληροφορικής, κλπ., το οποίο μπορεί να χρησιμοποιηθεί για την ασφαλή διαμόρφωση των συστημάτων και για την καθοδήγηση του σχεδιασμού εξειδικευμένων προγραμμάτων εκπαίδευσης και κατάρτισης. Κύριες πηγές πληροφοριών για απειλές που ενημερώνουν τις έρευνές της περιλαμβάνουν industrial πλαίσια κυβερνοασφάλειας, όπως οι MITRE ATT&CK πίνακες, και threat intelligence πληροφορίες, οι οποίες κοινοποιούνται από την κοινότητα της κυβερνοασφάλειας. Επιπρόσθετα, η Δρ. Σταύρου διερευνά λύσεις για ανάδειξη της διεπιστημονικής φύσης της κυβερνοασφάλειας και της προσέλκυσης επαγγελματιών, οι οποίοι προέρχονται από διαφορετικούς κλάδους, ώστε να γεφυρωθεί η έλλειψη δεξιοτήτων στην κυβερνοασφάλεια. Πέρα από την αναβάθμιση των δεξιοτήτων του ανθρώπινου δυναμικού, έχει ιδιαίτερο ενδιαφέρον για τη βελτίωση των δεξιοτήτων κυβερνοασφάλειας των πολιτών. Για τον σκοπό αυτό έχει αναπτύξει εκπαιδευτικό περιεχόμενο και πρακτικές δραστηριότητες για βελτίωση της επίγνωσης της κατάστασης στον κυβερνοχώρο και προώθηση κουλτούρας καλών πρακτικών, ξεκινώντας από νεαρή ηλικία. Στα ερευνητικά της ενδιαφέροντα είναι οι προκλήσεις ασφάλειας που σχετίζονται με το Διαδίκτυο των Πραγμάτων (IoT) και αναπτύσσει λύσεις για την ασφαλή διαμόρφωση του οικοσυστήματος IoT. Είναι μέλος πολλών ομάδων εργασίας και συμβουλευτικών επιτροπών που σχετίζονται με την ανάπτυξη ικανοτήτων κυβερνοασφάλειας, την έρευνα και την καινοτομία και δημοσιεύει σε κορυφαία διεθνή περιοδικά και συνέδρια. Έχει συγγράψει προτάσεις και έχει συντονίσει πολλά ερευνητικά και αναπτυξιακά έργα σχετικά με κυβερνοασφάλεια και τις ICT τεχνολογίες, τα οποία χρηματοδοτήθηκαν από εθνικά, ευρωπαϊκά και διεθνή προγράμματα. (https://www.ouc.ac.cy/index.php/el/profiles/98-eliana-stavrou).

Η Δρ. **Αδαμαντίνη Περατικού** είναι κάτοχος διδακτορικού τίτλου στον τομέα Αλγόριθμων Παράλληλης Επεξεργασίας και Βελτιστοποίησης, κατέχει πτυχίο Πληροφορικής από το Πανεπιστήμιο του Πόρτσμουθ του Ηνωμένου Βασίλειου και Postgraduate Certificate στην Τεχνολογία. Είναι μέλος του Ερευνητικού Εργαστηρίου Κυβερνοασφάλειας και Τηλεπικοινωνιών του Ανοικτού Πανεπιστημίου Κύπρου. Εργάζεται σε διάφορα χρηματοδοτούμενα έργα στον τομέα της ασφάλειας στον κυβερνοχώρο και της δικτύωσης. Κατά την τελευταία τετραετία μέρος της ερευνητικής της δραστηριότητας σχετίζεται με τα Cyber Ranges και την εκπαίδευση σε θέματα κυβερνοασφάλειας. Έχει δημοσιεύσει άρθρα σε διεθνή επιστημονικά συνέδρια και περιοδικά στους τομείς της Αρχιτεκτονικής Διασύνδεσης, των Δικτύων, των Ασύρματων Δικτύων και των Cyber Ranges και έχει υπηρετήσει ως κριτής σε διεθνή συνέδρια. Συμμετέχει στην επιτροπή τεχνικού προγράμματος για τα συμπόσια IEEE-ICC GCSN, IEEE-CIT και IEEE Greencom τα τελευταία επτά χρόνια. Έχει εμπειρία στη διδασκαλία σε προπτυχιακό και μεταπτυχιακό επίπεδο.. (https://www.ouc.ac.cy/index.php/el/profiles/99-adamantini-peratikou).

3.13 Επαγγελματική αποκατάσταση αποφοίτων

Κατά τη διάρκεια φοίτησης στο Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση», οι φοιτήτριες και οι φοιτητές αποκτούν γνώση και πρακτική εμπειρία που διευκολύνουν την επαγγελματική τους αποκατάσταση σε πολλούς τομείς εργασίας. Συγκεκριμένα, αποκτούν υψηλής εξειδίκευσης γνώσεις και δεξιότητες, που ανταποκρίνονται στις αυξανόμενες ανάγκες του δημόσιου και ιδιωτικού τομέα για θέματα κυβερνοασφάλειας, προστασίας δεδομένων και διακυβέρνησης σχετικών περιβαλλόντων.

Το World Economic Forum, τον Ιανουάριο 2023, ανακοίνωσε τους μεγαλύτερους κινδύνους / διακινδυνεύσεις (risks) για την ανθρωπότητα, κατηγοριοποιημένους σε Περιβαλλοντικούς, Γεωπολιτικούς, Κοινωνικούς και Τεχνολογικούς. Με βάση τη μελέτη αυτή, ο σημαντικότερος τεχνολογικός κίνδυνος θεωρήθηκε ότι είναι η διάδοση του κυβερνοεγκλήματος και η απουσία κυβερνοασφάλειας. Σε αντίστοιχη μελέτη του, το World Economic Forum, τον Ιανουάριο του 2024, ανακοίνωσε ότι ο 5ος μεγαλύτερος κίνδυνος στην ανθρωπότητα είναι οι κυβερνοεπιθέσεις, ενώ μόλις πρόσφατα, τον Ιανουάριο του 2025, περιέγραψε ότι στους σημαντικότερους τεχνολογικούς κινδύνους, παγκοσμίως, περιλαμβάνονται οι ψηφιακές επιθέσεις, η ψηφιακή παρακολούθηση και η κατασκοπεία στο Διαδίκτυο.

Με βάση στοιχεία της European Commission, Digital EU, Security Union και σχετική επεξεργασία από την PriceWaterhouseCoopers το 2020, το ετήσιο κόστος του κυβερνοεγκλήματος υπολογιζόταν σε €5.5 τρις., ποσό διπλάσιο από εκείνο του 2015. Και μάλιστα, το ποσό αυτό υπερέβαινε τα εκτιμώμενα έσοδα από την εμπορία ναρκωτικών ουσιών, ενώ αν οι κυβερνοεγκληματίες αναπαριστούσαν κράτος, τότε αυτό θα

συγκαταλέγονταν στους G20 με το 13ο μεγαλύτερο ΑΕΠ παγκοσμίως. Για το έτος 2025, η Cybersecurity Ventures αναμένει διαρκώς ετήσια αύξηση του κόστους του κυβερνοεγκλήματος κατά 15%, εκτιμώντας ότι στο τέλος του 2025 θα έχει φτάσει σε €10.5 τρις. Ουσιαστικά, το κυβερνοέγκλημα θεωρείται πλέον ως η τρίτη μεγαλύτερη οικονομία στον κόσμο μετά τις ΗΠΑ και την Κίνα (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/)

Στη χώρα μας, μελέτη της Allianze Global Corporate το 2023, είχε καταγράψει ότι τα περιστατικά κυβερνοασφάλειας αποτελούν τον τρίτο μεγαλύτερο κίνδυνο για τη χώρα, μετά την ενεργειακή κρίση και την αδυναμία επίτευξης διατηρήσιμης μακροοικονομικής ανάπτυξης. Με βάση στοιχεία της Eurostat, ποσοστό 22.2% των επιχειρήσεων (18% στην Ελλάδα), αντελήφθησαν και έχουν αντιμετωπίσει ποικίλα περιστατικά ασφάλειας. Επιπλέον, με βάση στοιχεία του ευρωπαϊκού οργανισμού για την ασφάλεια ENISA European Union Agency for Cybersecurity, το ποσοστό της δαπάνης για κυβερνοασφάλεια από οντότητες του δημόσιου και του ιδιωτικού τομέα, σε σχέση με τις δαπάνες τους για τεχνολογίες πληροφορικής και επικοινωνιών, είναι της τάξεως του 7%.

Όσον αφορά την κατάσταση της αγοράς εργασίας στην Ελλάδα και διεθνώς, τόσο για Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ) γενικά, όσο και ειδικά για θέματα κυβερνοασφάλειας, τα στοιχεία είναι γνωστά και χαρακτηριστικά. Στις ΗΠΑ ο Πρόεδρος Joe Biden, τον Αύγουστο του 2021, σε ξεχωριστή συνέντευξη τύπου δήλωνε εμφατικά ότι "…half a million cybersecurity jobs are unfilled" (https://www.reuters.com/world/us/cyber-threats-top-agenda-white-house-meeting-with-big-tech-finance-executives-2021-08-25/). Στην ΕΕ, με βάση μελέτη με τίτλο "Women in Cybersecurity", ανακοινώθηκε ότι: "The Cybersecurity field is suffering from a massive skills shortage. The gap, predicted to hit 1.8 million globally by 2022 and 350.000 in Europe alone. The gap is exacerbated by lack of female representation – with women comprising only 11% of the workforce, according to the "Women in Cybersecurity" research. For Europe the percentage is even lower – 7%. The involvement of women is an untapped resource. It is unlikely that we will close this gap without better gender balance" (https://www.iamcybersafe.org/s/). Επιπλέον, εξειδικευμένες έγκυρες μελέτες αποτυπώνουν επιμέρους πεδία κυβερνοασφάλειας, τα οποία απαιτείται κατά προτεραιότητα να γνωρίζουν στελέχη από επιχειρήσεις και οργανισμούς του ιδιωτικού και δημόσιου τομέα.

Στην Ελλάδα, το ποσοστό των επιστημόνων που ασχολούνται γενικά με ΤΠΕ είναι μακράν το μικρότερο στην Ευρώπη, αντιπροσωπεύοντας μόλις 2.5% των εργαζομένων, όταν ο μέσος όρος στην Ευρώπη είναι 4.6%. Πιο συγκεκριμένα, με βάση έρευνα που διεξήγαγε το 2024 η Deloitte για λογαριασμό του Συνδέσμου Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδος (ΣΕΠΕ), έδειξε ότι η ελληνική αγορά έως το 2030 θα χρειαστεί συνολικά 300.000 πτυχιούχους του κλάδου ΤΠΕ που θα συμβάλλουν στον ψηφιακό μετασχηματισμό της χώρας. Για την περίοδο 2023-2030 αναμένεται, επιπρόσθετη της σημερινής, σωρευτική ζήτηση για 120.000-140.000 ειδικούς ΤΠΕ, δηλαδή υπάρχει ανάγκη για επιπλέον 15.000-16.000 ειδικούς του κλάδου ΤΠΕ ετησίως μέχρι τότε. Η προσφορά από αποφοίτους πανεπιστημίων σήμερα είναι 8.000-8.500 ετησίως. Άρα καταγράφεται κενό πτυχιούχων του κλάδου ΤΠΕ, μεταξύ ζήτησης και προσφοράς, 7.000-7.500 αποφοίτων ετησίως, επιπλέον αυτών που θεωρείται ότι θα αποφοιτήσουν από τα πανεπιστήμια της χώρας.

Και όλα αυτά, για τη χώρα μας, σε περιβάλλον έκρηξης της ηλεκτρονικής απάτης τα τελευταία χρόνια. Μόλις πρόσφατα, η Εθνική Αρχή Κυβερνοασφάλειας, νεοσυσταθέν αρμόδιο ΝΠΔΔ για συναφή θέματα, δια του Προέδρου της, τόνισε επισήμως την αδυναμία εύρεσης και προσέλκυσης επιστημόνων με κατάλληλες γνώσεις και δεξιότητες σε θέματα κυβερνοασφάλειας και προστασίας δεδομένων.

Με βάση τα ανωτέρω, καθίσταται σαφές ότι η αγορά εργασίας στην Ελλάδα και στην ΕΕ, τόσο στον ιδιωτικό τομέα όσο και στον δημόσιο τομέα, συνεχίζει να αναζητά εναγωνίως επιστήμονες με γνώσεις και δεξιότητες σε θέματα κυβερνοασφάλειας και προστασίας δεδομένων και η τάση είναι διαρκώς αυξητική. Κατά συνέπεια, οι προοπτικές απασχόλησης των αποφοίτων του παρόντος ΠΜΣ «**Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση»,** τόσο κυρίως στην Ελλάδα όσο όμως και στην ΕΕ εν γένει, είναι εντυπωσιακά θετικές. Επιπροσθέτως, δια μέσου της εφαρμογής σύγχρονων διδακτικών μεθόδων και μελετών περίπτωσης, οι απόφοιτοι αποκτούν κρίσιμες «οριζόντιες» δεξιότητες (soft skills) αποτελεσματικής επικοινωνίας, επίλυσης προβλημάτων, εργασίας σε ομάδες, διαχείρισης χρόνου, προσαρμοστικότητας σε νέες καταστάσεις και κριτικής σκέψης.

3.14 Ακαδημαϊκό ημερολόγιο

Το ακαδημαϊκό ημερολόγιο αναρτάται στην ιστοσελίδα του Π.Μ.Σ. κάθε αρχή του ακαδημαϊκού έτους και ανανεώνεται όποτε υπάρξουν αλλαγές.

3.15 Πρόγραμμα Σπουδών

Το Π.Μ.Σ. ξεκινά το χειμερινό ακαδημαϊκό εξάμηνο εκάστου ακαδημαϊκού έτους (Σεπτέμβριος). Για την απόκτηση Διπλώματος Μεταπτυχιακών Σπουδών απαιτούνται συνολικά ενενήντα (90) πιστωτικές μονάδες (ECTS). Κατά τη διάρκεια των σπουδών, οι μεταπτυχιακοί φοιτητές και φοιτήτριες υποχρεούνται σε παρακολούθηση και επιτυχή εξέταση μεταπτυχιακών μαθημάτων, ερευνητική απασχόληση ή/και πρακτική άσκηση κ.ά., καθώς και σε εκπόνηση Μεταπτυχιακής Διπλωματικής Εργασίας.

Η οργάνωση της εκπαιδευτικής διαδικασίας του Π.Μ.Σ. πραγματοποιείται με χρήση μεθόδων σύγχρονης και ασύγχρονης εξ' αποστάσεως εκπαίδευσης:

- **Σύγχρονη εξ αποστάσεως εκπαίδευση**, είναι η εκπαιδευτική μέθοδος μέσω τεχνολογικής διαμεσολάβησης (περιβάλλον τηλεδιάσκεψης) όπου διδάσκων και διδασκόμενοι αλληλεπιδρούν σε διαφορετικό χώρο, αλλά στον ίδιο χρόνο με δυνατότητα αμφίδρομης επικοινωνίας και διαμοίρασης πολυτροπικού περιεχομένου (διαφάνειες, video κ.λπ.) σε πραγματικό χρόνο. **Το ποσοστό των σύγχρονων εξ αποστάσεως εκπαιδευτικών δραστηριοτήτων του Π.Μ.Σ. είναι 30,4% των συνολικών ECTS των μαθημάτων**.
- **Ασύγχρονη εξ αποστάσεως εκπαίδευση**, είναι η εκπαιδευτική μέθοδος μέσω ενός ολοκληρωμένου τεχνολογικού περιβάλλοντος (πλατφόρμα) ασύγχρονης

εκπαίδευσης, όπου διδάσκων και διδασκόμενοι αλληλεπιδρούν σε διαφορετικό χώρο και σε διαφορετικό χρόνο. Ειδικότερα πραγματοποιείται αλληλεπίδραση μεταξύ: α. διδάσκοντα - διδασκόμενου, β. διδασκόμενου - εκπαιδευτικού υλικού, γ. διδασκομένων. **Το ποσοστό των ασύγχρονων εξ αποστάσεως εκπαιδευτικών δραστηριοτήτων του Π.Μ.Σ. είναι 20,0% των συνολικών ECTS των μαθημάτων.**

Εκπαιδευτικές δραστηριότητες μη-καθοδηγούμενες από διδακτικό προσωπικό, ατομικής ή/και ομαδικής μελέτης και εξάσκησης των φοιτητών και φοιτητριών στα επιμέρους μαθήματα, γίνεται μέσω της εξ αποστάσεως πρόσβασής τους στις κατάλληλες υπηρεσίες του συστήματος ασύγχρονης εξ αποστάσεως εκπαίδευσης e-Class και στις ψηφιακές υπηρεσίες της Βιβλιοθήκης του Ιδρύματος. **Το ποσοστό των μη-καθοδηγούμενων εκπαιδευτικών δραστηριοτήτων του Π.Μ.Σ. είναι 49,6% των συνολικών ECTS των μαθημάτων.**

Τα μαθήματα οργανώνονται σε ακαδημαϊκά εξάμηνα, πραγματοποιούνται σε εβδομαδιαία βάση και διεξάγονται στην αγγλική γλώσσα.

3.15.1 Κατάλογος μαθημάτων ανά ακαδημαϊκό εξάμηνο

Τα μαθήματα που προσφέρονται ανά ακαδημαϊκό εξάμηνο περιγράφονται παρακάτω. Επιπροσθέτως, οι φοιτήτριες και οι φοιτητές θα ενημερώνονται εγκαίρως και για διαλέξεις σεμιναριακού χαρακτήρα που θα προγραμματίζονται.

3.15.1.1 Ακαδημαϊκό Εξάμηνο 1

Κωδικός Μαθήματος	Τίτλος Μαθήματος	Τύπος	ECTS
ΨΣ-ΠΤΚΔ-001	Ιδιωτικότητα και Προστασία Δεδομένων (Privacy and Data Protection)	Υποχρεωτικό	7,5
ΨΣ-ΠΤΚΔ-002	Διακυβέρνηση Κυβερνοασφάλειας (Cybersecurity Governance)	Υποχρεωτικό	7,5
ΨΣ-ΠΤΚΔ-003	Ασφάλεια Δικτύων (Network Security)	Υποχρεωτικό	7,5
ΨΣ-ΠΤΚΔ-004	Ασφάλεια Διαδικτύου των Πραγμάτων (IoT Security)	Υποχρεωτικό	7,5
	Σύνολο		**30**

3.15.1.2 Ακαδημαϊκό Εξάμηνο 2

Στο 2ο εξάμηνο οι φοιτητές θα πρέπει να παρακολουθήσουν τα δύο υποχρεωτικά μαθήματα και να επιλέξουν να παρακολουθήσουν άλλα δύο από τα πέντε μαθήματα επιλογής που προσφέρονται.

Κωδικός Μαθήματος	Τίτλος Μαθήματος	Τύπος	ECTS
ΨΣ-ΠΤΚΔ-005	Ψηφιακή Ευημερία στον Κυβερνοχώρο (Digital Wellbeing in Cyber-space)	Υποχρεωτικό	7,5
ΨΣ-ΠΤΚΔ-006	Τεχνικές Δοκιμαστικών Επιθέσεων (Offensive Security)	Υποχρεωτικό	7,5
ΨΣ-ΠΤΚΔ-007	Ψηφιακή Δικανική (Forensics)	Επιλογής	7,5
ΨΣ-ΠΤΚΔ-008	Ασφαλή Αυτόνομα Συστήματα (Secure Autonomous Systems)	Επιλογής	7,5
ΨΣ-ΠΤΚΔ-009	Κυβερνοασφάλεια: Λειτουργικές πρακτικές στον εντοπισμό και αντιμετώπιση επιθέσεων (Cybersecurity: Attack, Defence, and Operational Practice)	Επιλογής	7,5
ΨΣ-ΠΤΚΔ-010	Κυβερνοασφάλεια σε Βιομηχανικά Περιβάλλοντα (Cybersecurity in Industrial Scenarios)	Επιλογής	7,5
ΨΣ-ΠΤΚΔ-011	Κυβερνοασφάλεια στον Πολιτικό Τομέα: Εσωτερικές και Εξωτερικές Διαστάσεις (Cybersecurity in the Political Domain: Internal and External Dimensions)	Επιλογής	7,5
	Σύνολο (δύο υποχρεωτικά μαθήματα και δύο μαθήματα επιλογής)		**30**

3.15.1.3 Ακαδημαϊκό Εξάμηνο 3

Κωδικός Μαθήματος	Τίτλος Μαθήματος	Τύπος	ECTS
ΨΣ-ΠΤΚΔ-012	Μεταπτυχιακή Διπλωματική Εργασία (MSc Thesis)	Υποχρεωτικό	30

3.15.2 Περιγραφή μαθημάτων ανά ακαδημαϊκό εξάμηνο

3.15.2.1 Ακαδημαϊκό Εξάμηνο 1

3.15.2.1.1 Ιδιωτικότητα και Προστασία Δεδομένων (Privacy and Data Protection)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην Ιδιωτικότητα και τις Αρχές του ΓΚΠΔ
- Νομικό και Ρυθμιστικό Πλαίσιο
- Μοντέλο Διακυβέρνησης Ιδιωτικότητας
- Απαιτήσεις Συμμόρφωσης με τον ΓΚΠΔ
- Πολιτικές Ιδιωτικότητας
- Εκτίμηση και Διαχείριση Κινδύνων
- Εκτίμηση Αντικτύπου Προστασίας Δεδομένων (DPIA)
- Προστασία Δεδομένων από τον Σχεδιασμό και εξ Ορισμού (Privacy by Design & Default)
- Τεχνητή Νοημοσύνη και Προσωπικά Δεδομένα
- Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (PETs)
- Ευαισθητοποίηση/Εκπαίδευση για την Ιδιωτικότητα
- Ασφάλιση Κυβερνοκινδύνων και Προσωπικά Δεδομένα
- Διαδικτυακό Μάρκετινγκ και Διαφήμιση, Cookies και Τεχνολογίες Ιχνηλάτησης

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Acquisti, A., Gritzalis, S., Lambrinoudakis, C., di Vimercati, S. (2007) Digital Privacy, Theory, Technologies and Practices.
  - Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles.
- Συναφή επιστημονικά περιοδικά:
  - Journal of Information Privacy and Security, Taylor & Francis
  - Information and Computer Security, Emerald
  - International Journal of Information Security, Springer
  - Computer Law & Security Review, Elsevier
  - IEEE Security and Privacy Magazine, IEEE
  - Computers and Security, Elsevier
  - Requirements Engineering, Springer
  - IEEE Transactions on Software Engineering, IEEE
  - Security and Communication Networks, Wiley
  - Information Management and Computer Security, Emerald
  - International Journal on Advances in Security, IARIA
  - Journal of Information Security and Applications, Elsevier

3.15.2.1.2 Διακυβέρνηση Κυβερνοασφάλειας (Cybersecurity Governance)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Έννοιες Κυβερνοασφάλειας
- Προστασία Δεδομένων, Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) και Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA)
- Ο Ρόλος του Υπεύθυνου Ασφάλειας Πληροφοριών (CISO - Chief Information Security Officer)
- Ετοιμότητα για Κυβερνοαπειλές (Cyber Readiness)
- Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) και διαχείριση κυβερνοασφάλειας
- Διαχείριση και Αξιολόγηση Κινδύνων Κυβερνοασφάλειας
- Κανονιστικό Πλαίσιο και Συμμόρφωση
- Επιχειρήσεις Κυβερνοασφάλειας και Κυβερνοπόλεμος

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Jøsang, Audun. Cybersecurity: Technology and Governance. Springer (2024).
  - Tran, Dinh Uy; Jøsang, Audun. Business Language for Information Security. Human Aspects of Information Security and Assurance (HAISA 2023).
  - Tran, Dinh Uy; Jøsang, Audun. Information Security Posture to Organize and Communicate the Information Security Governance Program. European Conference on Management, Leadership & Governance (2022).
  - OECD Digital Economy Papers: New Perspectives on Measuring Cybersecurity, OECD Publishing, June 2024, no. 366.
- Συναφή επιστημονικά περιοδικά:
  - Computers & Security (Elsevier)
  - Journal of Cybersecurity (Oxford University Press)
  - Journal of Information Security and Applications (JISA) (Elsevier)
  - IEEE Security & Privacy
  - International Journal of Critical Infrastructure Protection (Elsevier)
  - Information and Computer Security (Emerald)
  - Information Security Journal: A Global Perspective (Taylor & Francis)

3.15.2.1.3 Ασφάλεια Δικτύων (Network Security)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην Ασφάλεια Δικτύων
  - Βασικές αρχές και στοιχεία δικτύου

- Εγγενή πρωτόκολλα TCP/IP και κύρια ζητήματα ασφάλειας αυτών
- Επισκόπηση επιθέσεων σε επίπεδο δικτύου

- Κύριες επιθέσεις και εργαλεία δικτύου
  - Επιθέσεις στην εμπιστευτικότητα
  - Επιθέσεις στην ακεραιότητα
  - Επιθέσεις στη διαθεσιμότητα
  - Άλλες συναφείς επιθέσεις
- Πρωτόκολλα ασφάλειας στο TCP/IP
  - Ασφάλεια σε επίπεδο ζεύξης
  - Ασφάλεια σε επίπεδο δικτύου
  - Ασφάλεια σε επίπεδο μεταφοράς
  - Ασφάλεια σε επίπεδο εφαρμογής
- Ασφαλής παραμετροποίηση δικτύου
  - Θωράκιση μεταγωγέων (switches) και δρομολογητών (routers)
  - Εικονικά ιδιωτικά δίκτυα (VPNs)
  - Τείχος προστασίας (firewall) και 'αποστρατιωτικοποιημένη ζώνη' (DMZ) δικτύου
  - Ανίχνευση, πρόληψη και εξαπάτηση
  - Θωράκιση τερματικών συσκευών (Linux, Windows)

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Computer Networking Hacking: Ultimate Guide To Ethical Hacking, Wireless Network, Cybersecurity With Practical Penetration Test On Kali Linux And System Security Practices (Computer Networking Easy). Ramon Base (autor), ISBN: 978-1083056832, 2019.
  - Implementing and Administering Cisco Solutions: 200-301 CCNA Exam Guide: Begin a successful career in networking with 200-301 CCNA certification. Glen D. Singh (autor), Packt, ISBN: 978-1800208094, 2020.
  - Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Donald A. Tevault (autor), Packt, ISBN: 978-1788620307, 2018.
  - Network Security Strategies. Aditya Mukherjee (autor), Packt, ISBN:9781789806298, 2020.
  - Security Engineering: A Guide to Building Dependable Distributed Systems. Ross Anderson (autor), Wiley, ISBN: 978-1119642787, 2020.
  - pfSense Essentials: The Complete Reference to the pfSense Internet Gateway and Firewall. Jeremy C. Reed (autor), ISBN: 978-1937516048, 2019.
- Συναφή επιστημονικά περιοδικά:
  - IEEE Network
  - IEEE Computer Networks
  - IEEE Communications Surveys & Tutorials
  - IEEE Transactions on Secure and Dependable Computing

- IEEE Transactions on Information Forensics and Security
- Computers and Security, Elsevier
- IEEE Security & Privacy
- ACM Transactions on Privacy and Security, μεταξύ άλλων

- Συναφή επιστημονικά συνέδρια:
  - BlackHat
  - ESORICS
  - Usenix Security
  - ACM Conference on Computer and Communications Security
  - IEEE International Conference on Cyber Security and Resilience, μεταξύ άλλων συναφών συνεδρίων

3.15.2.1.4 Ασφάλεια Διαδικτύου των Πραγμάτων (IoT Security)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Βασικές Έννοιες IoT: Το μάθημα ξεκινά με μια επισκόπηση των συνηθέστερων IoT συστημάτων και αρχιτεκτονικών, της διάκρισης μεταξύ IoT και παραδοσιακών IT συστημάτων, σημαντικών επιθέσεων σε IoT συσκευές καθώς και των τρεχουσών θεμάτων που άπτονται της προστασίας βιομηχανικών IoT (IIoT).
- Μοντελοποίηση Απειλών (Threat Modelling): Παρουσιάζεται το απαραίτητο θεωρητικό υπόβαθρο για τη μοντελοποίηση απειλών και περιουσιακών στοιχείων σε συστήματα IoT. Η ενότητα περιλαμβάνει ορολογία, τον Ασφαλή Κύκλο Ζωής Λογισμικού IoT, τα πρότυπα ISO 21424 και ISO/IEC 18045, σχήματα κατηγοριοποίησης επιτιθέμενων (Adversary Classification), τη βιβλιοθήκη απειλών της Intel (Intel Threat Agent Library), την ταξινόμηση περιουσιακών στοιχείων (Asset Taxonomy), OCTAVE, τις βασικές αρχές και στόχους ασφάλειας στο πλαίσιο του IoT, STRIDE, επιθέσεις ενδιάμεσου (MITM) και εισαγωγή σε τεχνικές αντιμετώπισης των επιθέσεων (mitigations) σε IoT.
- Βασικοί κρυπτογραφικοί μηχανισμοί στο IoT: Παρουσιάζεται το θεωρητικό υπόβαθρο των βασικών κρυπτογραφικών μηχανισμών που χρησιμοποιούνται σε συνήθη IoT συστήματα, όπως κλασικά κρυπτογραφήματα (π.χ. μονοαλφαβητικά, πολυαλφαβητικά, υποκατάστασης, μεταθετικά), συμμετρική κρυπτογραφία (με έμφαση στοον αλγόριθμο AES και τους τρόπους λειτουργίας του), ασύμμετρη κρυπτογραφία (με έμφαση στον αλγόριθμο RSA) και σχήματα ψηφιακής υπογραφής (MAC, HMAC, βασισμένα στον αλγόριθμο RSA).
- Κρυπτανάλυση (Cryptanalysis): Εξετάζονται γνωστοί περιορισμοί των παραπάνω βασικών κρυπτογραφικών μηχανισμών στο πλαίσιο του IoT, όπως επιθέσεις τύπου padding oracle, επιθέσεις επιλεγμένου απλού κειμένου (plaintext), παραγοντοποίηση ακεραίων (integer factorization) κ.ά. Επιπλέον, παρουσιάζονται πραγματικά παραδείγματα τέτοιων επιθέσεων σε διάφορους τομείς IoT όπως τα συστήματα αυτοκινήτων.
- Μοτίβα Επικοινωνίας και Ασφάλειας συγκεκριμένα στο IoT: Εξετάζονται, στο πλαίσιο της κυβερνοασφάλειας, τα κυριότερα πρωτόκολλα επικοινωνίας στο IoT. Γίνεται ανάλυση των MQTT, XMPP, CoAP, HTTPS, του Request/Response Pattern, των

Ασύγχρονων Μηνυμάτων (Asynchronous Messaging), των Ουρών Μηνυμάτων (Message Queues), του Μοτίβου Εκδότη/Συνδρομητή (Publisher/Subscriber Pattern).

- Πρωτόκολλα Ανταλλαγής Κλειδιών: Εξετάζεται το ζήτημα του κοινού διαμοιρασμού/ανταλλαγής/διαπραγμάτευσης κρυπτογραφικών κλειδιών για τη διασφάλιση ασφαλούς επικοινωνίας μεταξύ διαφορετικών συσκευών IoT. Παρουσιάζονται θέματα όπως οι μηχανισμοί μεταφοράς και ανταλλαγής κλειδιών και οι περιορισμοί τους, η έννοια των Κέντρων Διανομής Κλειδιών (Key Distribution Centers), η (επαληθευμένη) Ανταλλαγή Κλειδιών Diffie-Hellman, καθώς και τα Πιστοποιητικά και οι αντίστοιχες μεθοδολογίες Υποδομής Δημοσίου Κλειδιού (PKI).
- Ασφάλεια Ιστού και Δικτύου στο πλαίσιο του IoT: Δεδομένου ότι τα τυπικά IoT συστήματα είναι έντονα διασυνδεδεμένα, εξετάζονται θεωρητικά και πρακτικά ζητήματα ασφάλειας σε δικτυωμένα συστήματα. Συγκεκριμένα θα παρουσιαστούν μεθόδοι αναγνώρισης (reconnaissance) με χρήση του nmap και συναφών εργαλείων, Τεχνικές Απαρίθμησης (Enumeration) σε web-based IoT συσκευές, Μεθοδολογίες Εκτίμησης Ευπαθειών, το OWASP Top 10 και οι αντίστοιχες κοινές στρατηγικές εκμετάλλευσης (π.χ. SQL injection, XSS), καθώς και εργαλειοθήκες για τον έλεγχο διείσδυσης (penetration testing) τέτοιων εφαρμογών.
- Μηχανισμοί Προστασίας: Παρουσιάζονται εναλλακτικοί μηχανισμοί προστασίας IoT συστημάτων. Περιλαμβάνονται μεθοδολογίες και μοτίβα Ελέγχου Πρόσβασης (Access Control) για IoT, Μηχανισμοί Αυθεντικοποίησης, καθώς και οι περιορισμοί και προκλήσεις των εν λόγω μέτρων.
- Σύγχρονη Έρευνα, Κενά και Κατευθύνσεις: Καθ' όλη τη διάρκεια του μαθήματος δίνεται έμφαση στις τρέχουσες επιστημονικές εξελίξεις που αφορούν τόσο επιθέσεις όσο και νέους μηχανισμούς προστασίας σε IoT. Στόχος είναι η ενίσχυση των δεξιοτήτων κριτικής ανάλυσης των φοιτητών στο πλαίσιο των σύγχρονων ερευνητικών τάσεων.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Adam Shostack, "Threat Modeling: Designing for Security", (https://ieeexplore.ieee.org/book/9932141)
  - ENISA Report, "Good Practices for Security of IoT - Secure Software Development Lifecycle" (https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1)
  - ENISA Report, "Baseline Security Recommendations for IoT" (https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot)
  - Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source Code in C" (https://www.schneier.com/books/applied-cryptography/)
  - Dan Boneh, Victor Shoup, "A Graduate Course in Applied Cryptography" (https://toc.cryptobook.us/book.pdf)
  - Nitesh Dhanjani, "Abusing the Internet of Things" (https://www.oreilly.com/library/view/abusing-the-internet/9781491902899/)
  - Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook, 2nd Edition" (https://www.oreilly.com/library/view/the-web-application/9781118026472/)

- Συναφή επιστημονικά περιοδικά:
  - IEEE Internet of Things Journal
  - ACM Transactions on Internet Technology
  - IEEE Transactions on Dependable and Secure Computing

3.15.2.2 Ακαδημαϊκό Εξάμηνο 2

3.15.2.2.1 Ψηφιακή Ευημερία στον Κυβερνοχώρο (Digital Wellbeing in Cyber-space)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην Ψηφιακή Ευημερία και στην Κυβερνοασφάλεια: Εξερεύνηση των βασικών ορισμών, θεματικών περιοχών και συσχετίσεων μεταξύ ψηφιακής ευημερίας και κυβερνοασφάλειας. Διερεύνηση της αυξανόμενης σημασίας τους σε έναν υπερσυνδεδεμένο κόσμο σε ατομικό, οργανωσιακό και κοινωνικό επίπεδο.
- Βασικά στοιχεία κυβερνοασφάλειας για προσωπική προστασία: Απόκτηση θεμελιωδών γνώσεων κυβερνοασφάλειας, συμπεριλαμβανομένης της διαχείρισης κωδικών πρόσβασης, των ελέγχων ταυτότητας δύο παραγόντων (2FA), της αναγνώρισης επιθέσεων τύπου phishing και της ψηφιακής υγιεινής στην καθημερινή ζωή.
- Απειλές για την Ψηφιακή Ευημερία: Διερεύνηση απειλών όπως ο κυβερνοεκφοβισμός, η διαδικτυακή παρενόχληση και η ψηφιακή κόπωση. Ανάλυση του τρόπου με τον οποίο αυτές επηρεάζουν την ψυχική και συναισθηματική ευημερία και εκμάθηση προληπτικών μέτρων.
- Κοινωνική ευημερία στον κυβερνοχώρο: Διερεύνηση του τρόπου με τον οποίο οι διαδικτυακές κακόβουλες συμπεριφορές (κυβερνοεκφοβισμός, επιθέσεις τύπου phishing, επιθέσεις κοινωνικής μηχανικής) επηρεάζουν την κοινωνική και συναισθηματική υγεία. Ανάπτυξη ψηφιακής παιδείας και ενθάρρυνση συμμετοχής σε διαδικτυακές κοινότητες για την αντιμετώπιση τέτοιου είδους συμπεριφορών.
- Ψηφιακοί εθισμοί και αλγοριθμική χειραγώγηση: Ανάλυση των χαρακτηριστικών σχεδιασμού με έμφαση στην αλληλεπίδραση και των αλγοριθμικών συστημάτων των ψηφιακών πλατφορμών. Εξέταση του τρόπου με τον οποίο επηρεάζουν τη συμπεριφορά των χρηστών, ενισχύουν την ψηφιακή εξάρτηση και εγείρουν ηθικά ζητήματα.
- Ψυχική υγεία, εξουθένωση και κουλτούρα συνεχούς διαθεσιμότητας: Διερεύνηση των ψυχολογικών επιπτώσεων της συνεχούς συνδεσιμότητας, μελέτη του τεχνολογικού άγχους, της επαγγελματικής εξουθένωσης και του αντίκτυπου της πληροφοριακής υπερφόρτωσης στην ψυχική υγεία. Επιπλέον, εξοικείωση με στρατηγικές ανθεκτικότητας και τεχνικές ψηφιακής αυτοφροντίδας.
- Σχεδιασμός για την Ασφάλεια και την Ευημερία: Κατανόηση του τρόπου με τον οποίο ο ανθρωποκεντρικός σχεδιασμός UX/UI μπορεί να προωθήσει τόσο την ασφάλεια των συστημάτων όσο και την ψηφιακή ευημερία. Εξέταση πραγματικών τεχνολογικών παραδειγμάτων και βέλτιστων πρακτικών σχεδιασμού.
- Κοινωνικά Μέσα, Παραπληροφόρηση και Συναισθηματική Ανθεκτικότητα: Αξιολόγηση του αντίκτυπου της παραπληροφόρησης, της διαδικτυακής τοξικότητας και των αλγοριθμικών φουσκών φιλτραρίσματος. Εξοικείωση με πρακτικές ενδυνάμωσης της

συναισθηματικής ανθεκτικότητας και κριτικής προσέγγισης του ψηφιακού περιεχομένου.

- Ο ρόλος του ανθρώπινου παράγοντα στην κυβερνοασφάλεια: Εξέταση της συμπεριφορικής διάστασης του κυβερνοκινδύνου, κατανόηση του πώς ψυχολογικοί παράγοντες, γνωστικές μεροληψίες και ανθρώπινα λάθη επηρεάζουν την ασφάλεια, καθώς και διερεύνηση εργαλείων όπως οι συμπεριφορικές ωθήσεις (nudging) και η παιχνιδοποίηση (gamification)
- Ηθικές Προοπτικές του Μέλλοντος - Τεχνητή Νοημοσύνη (ΤΝ), Ηλεκτρονική παρακολούθηση και ο Ανθρώπινος Νους: Συζήτηση του πώς η τεχνητή νοημοσύνη και τα συστήματα επιτήρησης επηρεάζουν την ιδιωτικότητα, την αυτονομία και την ψυχική υγεία των ανθρώπων. Εξέταση των ηθικών διλημμάτων που σχετίζονται με την ψηφιακή χειραγώγηση και τη διακυβέρνηση των δεδομένων.
- Οργανωσιακή κυβερνοασφάλεια και ευημερία των εργαζομένων: Διερεύνηση του αντίκτυπου των εταιρικών πολιτικών κυβερνοασφάλειας στην ψυχική ευεξία και στην παραγωγικότητα του προσωπικού, μέσα από ανάλυση πραγματικών περιπτώσεων που αναδεικνύουν ηθικές και ισορροπημένες πρακτικές ψηφιακής ασφάλειας.
- Εκπόνηση προσωπικού πλάνου ψηφιακής ευημερίας και αναστοχασμός: Αναστοχασμός στις γνώσεις και δεξιότητες που αποκτήθηκαν κατά τη διάρκεια του μαθήματος και κατάρτιση προσωπικού σχεδίου δράσης για την ψηφιακή ευημερία και την κυβερνοασφάλεια. Συζήτηση των μελλοντικών επιπτώσεων και διαμόρφωση στρατηγικών για βιώσιμες ψηφιακές συνήθειες.
- Εργαστήριο σχεδιασμού παρεμβάσεων: Εφαρμογή των εννοιών του μαθήματος μέσω συνεργατικού σχεδιασμού μιας πρακτικής παρέμβασης που ενσωματώνει αρχές κυβερνοασφάλειας και ψηφιακής ευημερίας. Περιλαμβάνει συνεδρία αξιολόγησης μεταξύ των εκπαιδευόμενων και παροχής ανατροφοδότησης.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Bauman, S., Cross, D., & Walker, J. (Eds.). (2013). Principles of cyberbullying research: Definitions, measures, and methodology. Routledge.
  - Brewer, J. (2017). The craving mind: From cigarettes to smartphones to love—Why we get hooked and how we can break bad habits. Yale University Press.
  - Büchi, M. (2022). Digital well-being: Conceptualizations, implications, and open questions. New Media & Society, 24(2), 337–355.
  - Cecchinato, M. E., Rooksby, J., Hiniker, A., Munson, S., Lukoff, K., Ciolfi, L., ... & Harrison, D. (2019, May). Designing for digital wellbeing: A research & practice agenda. In Extended abstracts of the 2019 CHI conference on human factors in computing systems (pp. 1–8). ACM.
  - Crouch, A. (2017). The tech-wise family: Everyday steps for putting technology in its proper place. Baker Books.
  - Filep, S., Kondja, A., Wong, C. C. K., Weber, K., Moyle, B. D., & Skavronskaya, L. (2023). The role of technology in users' wellbeing: Conceptualizing digital wellbeing in hospitality and future research directions. Journal of Sustainable Tourism, 31(5), 583–601.

- Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206–221.
- Hinduja, S., & Patchin, J. W. (2024). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (3rd ed.). Corwin Press.
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137.
- Krause, C. (2024). Digital wellbeing: Empowering connection with wonder and imagination in the age of AI. Wiley.
- Monge Roffarello, A., & De Russis, L. (2019, May). The race towards digital wellbeing: Issues and opportunities. In Proceedings of the 2019 CHI conference on human factors in computing systems (pp. 1–14). ACM.
- Patchin, J. W., & Hinduja, S. (2014). Words wound: Delete cyberbullying and make kindness go viral. Free Spirit Publishing.
- Patchin, J. W., & Hinduja, S. (2016). Bullying today: Bullet points and best practices. Corwin Press.
- Regehr, K. (2025). Smartphone nation: Digital addiction and how to break free. Bloomsbury Academic.
- Roffarello, A. M., & De Russis, L. (2023). Achieving digital wellbeing through digital self-control tools: A systematic review and meta-analysis. ACM Transactions on Computer-Human Interaction, 30(4), 1–66.
- Schlyakhto, E., Ilin, I., Devezas, T., Correia Leitão, J. C., & Cubico, S. (2024). Innovations for healthcare and wellbeing: Digital technologies, ecosystems and entrepreneurship. Springer.
- Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26–32.
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277–287.
- Turkle, S. (2015). Reclaiming conversation: The power of talk in a digital age. Penguin Press.
- Vanden Abeele, M. M. P. (2021). Digital wellbeing as a dynamic construct. Communication Theory, 31(4), 932–955.
- Willard, N. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Research Press.
- Wong, B. L. H., Maaß, L., Vodden, A., van Kessel, R., Sorbello, S., Buttigieg, S. C., & Odone, A. (2022). From digital health to digital well-being: A systematic scoping review. Journal of Medical Internet Research, 24, Article e33787.

- Συναφή επιστημονικά περιοδικά:
  - **<u>Digital Wellbeing, Cyberpsychology & Human Behavior</u>**
    - **Journal of Cybersecurity**
      - Focus: Cybersecurity policy, technical, and human dimensions

        - Publisher: Oxford University Press
        - https://academic.oup.com/cybersecurity
    - **Cyberpsychology: Journal of Psychosocial Research on Cyberspace**
        - Focus: Online behavior, cyberbullying, digital wellbeing, and psychosocial research
        - Publisher: Masaryk University
        - https://cyberpsychology.eu/
    - **Computers in Human Behavior**
        - Focus: Human interaction with digital technologies, including mental health and screen time
        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/computers-in-human-behavior
    - **Journal of Medical Internet Research (JMIR)**
        - Focus: Digital health, eHealth, digital wellbeing
        - Publisher: JMIR Publications
        - https://www.jmir.org/
    - **Communication Theory**
        - Focus: Theoretical and empirical research in communication, including digital wellbeing
        - Publisher: Oxford University Press
        - https://academic.oup.com/ct
    - **Journal of Computer-Mediated Communication (JCMC)**
        - Focus: Social and interpersonal communication in digital media
        - Publisher: Oxford University Press
        - https://academic.oup.com/jcmc
    - **New Media & Society**
        - Focus: Socio-cultural impacts of new media and technology, including wellbeing
        - Publisher: SAGE
        - https://journals.sagepub.com/home/nms
    - **Technology in Society**
        - Focus: Social impacts of emerging technologies, ethics, and behavior
        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/technology-in-society
    - **Information, Communication & Society**
        - Focus: Intersection of technology, communication, and society
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/rics20
- **Human–Computer Interaction (HCI) & UX**
    - **ACM Transactions on Computer-Human Interaction (TOCHI)**

        - Focus: Interaction design, user experience, digital self-control tools
        - Publisher: ACM
        - https://dl.acm.org/journal/tochi
    - **International Journal of Human-Computer Studies**
        - Focus: HCI, UX design, and digital behavior
        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/international-journal-of-human-computer-studies
    - **Behaviour & Information Technology**
        - Focus: Human interaction with technology and design for wellbeing
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/tbit20
- **Psychological and Media Effects**
    - **Media Psychology**
        - Focus: Media influence on emotions, cognition, addiction, and wellbeing
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/hmep20

3.15.2.2.2 Τεχνικές Δοκιμαστικών Επιθέσεων (Offensive Security)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Ανάκτηση πληροφοριών από Ανοικτές Πηγές (Open-Source Intelligence-OSINT): Εισαγωγή στις τεχνικές συλλογής γενικών και τεχνικών πληροφοριών στόχου (π.χ. Google hacking), άντληση δεδομένων από μέσα κοινωνικής δικτύωσης και διαδικτυακά αρχεία, συλλογή δεδομένων τεχνικής φύσεως, αναζήτηση στοιχείων ονόματος χώρου και ιδιοκτητών, έρευνα διευθύνσεων IP, ταυτοποίηση και απαρίθμηση δικτυακών περιοχών (network ranges).
- Αναγνώριση Δικτύου: Χαρτογράφηση δικτύου με διάφορες τεχνικές, χρήση του εργαλείου nmap, χρήση του εργαλείου hping με διαφορετικές παραμέτρους.
- Εξοικείωση με Υπηρεσίες: Αναγνώριση και εκδήλωση κυβερνοεπιθέσεων σε διάφορες υπηρεσίες, εντοπισμός διαρροής πληροφοριών και προεπιλεγμένων ρυθμίσεων, επιθέσεις εξαντλητικής αναζήτησης (brute-force), γενική κατανόηση εκμεταλλεύσεων (exploits), μοναδικές τεχνικές εκμετάλλευσης ειδικές ανά υπηρεσία.
- Χάκινγκ Διαδικτυακών Εφαρμογών: Επιθέσεις εξαντλητικής αναζήτησης (brute-force), επιθέσεις χειραγώγησης και παραποίησης προσανατολισμένες στον χρήστη (client-side manipulation and tampering attacks), επιθέσεις τύπου XSS, επιθέσεις πλαστογράφησης αιτήσεων μεταξύ ιστοτόπων (CSRF), επιθέσεις διακομιστή, εκμετάλλευση συνεδριών (session-related exploitations), επιθέσεις ενσωμάτωσης αρχείων, επιθέσεις έγχυσης SQL (SQL injection), επιθέσεις έγχυσης XPath (XPath injection), επιθέσεις έγχυσης προτύπου διακομιστή (SSTI), εκμεταλλεύσεις εξωτερικών οντοτήτων XML (XXE).
- Εκμετάλλευση Δυαδικών Αρχείων: Κατανόηση δυαδικών αρχείων και αρχιτεκτονιών CPU, εικονικοί χώροι διευθύνσεων και διάταξη μνήμης, αποσφαλμάτωση (debugging),

κατανόηση στοίβας, υπερχείλιση στοίβας (stack overflow), τεχνική επιστροφής στη libc (return-to-libc), προγραμματισμός κατευθυνόμενης επιστροφής (ROP), ευπάθειες σωρού (heap), τεχνικές χρήση μετά την αποδέσμευση (use-after-free), τεχνικές 'ψεκασμού' σωρού (heap spraying)

- Κοινωνική Μηχανική (Social Engineering): Κατανόηση ανθρώπινης συμπεριφοράς, τεχνικές ηλεκτρονικού ψαρέματος (phishing), άλλες τεχνικές κοινωνικής μηχανικής.
- Χάκινγκ Εσωτερικών Δικτύων: Πρόσβαση και επιθέσεις εντός εσωτερικών εταιρικών δικτύων, με στόχευση σε πρωτόκολλα της Microsoft, εφαρμογή επιθέσεων τύπου MITM, ARP poisoning και εκμετάλλευση εσωτερικής υποδομής.
- Ηθικό Χάκινγκ και Κρυπτογραφία: Ανάλυση τεχνικών αποκάλυψης κωδικών πρόσβασης (password cracking), με έμφαση στο πλαίσιο της ηθικής και της νομικής δεοντολογίας.
- Ασφάλεια Ασύρματων Δικτύων: Επισκόπηση πρωτοκόλλων WEP και WPA2, καταγραφή χειραψίας Wi-Fi (Wi-Fi handshake), Παραβίαση πρωτοκόλλου WPA2 (cracking WPA2).

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Στις διαφάνειες των διαλέξεων θα παρέχεται ενημερωμένη βιβλιογραφία
- Συναφή επιστημονικά περιοδικά:
  - Journal of Cybersecurity (Oxford University Press)
  - IEEE Security & Privacy
  - Cybersecurity (SpringerOpen)

3.15.2.2.3 Ψηφιακή Δικανική (Forensics)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην Ψηφιακή Δικανική / Εγκληματολογία: Αλυσίδα επιμέλειας (chain of custody), κύκλος ζωής αποδεικτικών στοιχείων (evidence lifecycle), ρόλοι στην εγκληματολογική διερεύνηση
- Συλλογή Αρχείων, Δεδομένων, και Μεταδεδομένων: Τεχνικές δημιουργίας εγκληματολογικού αντιγράφου ενός δίσκου, ανάλυση συστημάτων αρχείων, εξαγωγή μεταδεδομένων και ιχνών, συναρτήσεις κατακερματισμού κ.ά.
- Εγγενή Ίχνη των Windows 1: Prefetch, Μητρώο Καταγραφής (Registry) κ.ά.
- Εγγενή Ίχνη των Windows 2: Καταγραφές Συμβάντων (Event Logs), LNK, Jumplist κ.ά.
- Δεδομένα Περιήγησης στο Διαδίκτυο: Ίχνη από τους φυλλομετρητές Chrome και Firefox: Ιστορικό Περιήγησης, Λήψεις, Σελιδοδείκτες κ.ά.
- Προηγμένα Θέματα Ψηφιακής Εγκληματολογίας: Υπολογιστικό Νέφος, Κινητές Συσκευές, Διαδίκτυο των Πραγμάτων (IoT) κ.ά.
- Βασικές Αρχές SOC: Δομή SOC, αρμοδιότητες επιπέδων L1–L3, επισκόπηση εργαλείων
- Λειτουργία SIEM και Αρχική Διαλογή Ειδοποιήσεων: Αρχιτεκτονική SIEM, συλλογή και επξεργασία αρχείων καταγραφής, αρχικός χειρισμός ειδοποιήσεων
- Απόκριση σε Περιστατικά (Incident Response) 1: Κύκλος ζωής απόκρισης σε περιστατικά,

Συλλογή και Ανάλυση Εγκληματολογικού Αντιγράφου Διαλογής (Triage Image).

- Απόκριση σε Περιστατικά (Incident Response) 2: Συλλογή και Ανάλυση Μνήμης RAM.
- Πληροφορίες για Απειλές και Πληροφορίες για Απειλές Κυβερνοχώρου (CTI): Κύκλος ζωής CTI, MISP, προφίλ δραστών απειλών
- Ανίχνευση Απειλών (Threat Hunting) και Μηχανική Ανίχνευσης (Detection Engineering): Ανίχνευση βάσει υποθέσεων, αντιστοίχιση στο πλαίσιο MITTE ATT&CK, ανάπτυξη κανόνων ανίχνευσης
- Τεχνητή Νοημοσύνη στην Κυβερνοάμυνα και Αυτοματοποίηση SOC: ΤΝ για αρχική διαλογή ειδοποιήσεων, αυτοματοποιημένη ανάλυση αρχείων καταγραφής, ανίχνευση phishing κ.ά.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - William Oettinger, Learn Computer Forensics – 2nd edition: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence , Second Edition (2022)
  - Anson, S. (2020). Applied incident response. Wiley.
  - Murdoch, D. (2019). Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A condensed guide for the security operations team and threat hunter. Independently published.
- Συναφή επιστημονικά περιοδικά:
  - Digital Investigation (Elsevier)
  - Journal of Cybersecurity (Oxford University Press)
  - Journal of Forensics Sciences (Wiley)

3.15.2.2.4 Ασφαλή Αυτόνομα Συστήματα (Secure Autonomous Systems)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγικό θεωρητικό υπόβαθρο για τα αυτόνομα συστήματα: Το μάθημα ξεκινά με τη μελέτη του θεωρητικού υποβάθρου των τυπικών αυτόνομων συστημάτων, καλύπτοντας τις συνήθεις αρχιτεκτονικές και τα λειτουργικά υποσυστήματα των αυτόνομων οχημάτων και των drones, με έμφαση στην πολυεπίπεδη δομή, στα περιβάλλοντα προσομοίωσης για end-to-end δοκιμές, σε αξιοσημείωτα παραδείγματα πραγματικών επιθέσεων κατά αυτόνομων οχημάτων, καθώς και στην τρέχουσα κατάσταση της έρευνας ασφάλειας στον συγκεκριμένο τομέα.
- Μοντελοποίηση απειλών: Ως βάση για περαιτέρω συζήτηση, το μάθημα καλύπτει σημαντικές μεθοδολογίες κατηγοριοποίησης απειλών και πόρων σε αυτόνομα συστήματα (π.χ. EVITA), καθώς και τον τρόπο εφαρμογής τους.
- Ροή επεξεργασίας δεδομένων αισθητήρων καμερών: Το μάθημα αναλύει τις επικρατέστερες τεχνολογίες αισθητήρων καμερών και το σχετικό πλαίσιο ασφάλειας. Η ενότητα περιλαμβάνει τα στάδια (προ)επεξεργασίας δεδομένων, τη ροή επεξεργασίας από τον αισθητήρα έως το επίπεδο αντίληψης, τα βασικά δομικά στοιχεία του επιπέδου αντίληψης, τις επιπτώσεις ασφάλειας που προκύπτουν από την επεξεργασία, καθώς και

την τρέχουσα ερευνητική δραστηριότητα στον τομέα των συστημάτων αντίληψης που βασίζονται σε κάμερες.

- Ροή επεξεργασίας δεδομένων αισθητήρα LiDAR: Η ενότητα αυτή εξετάζει τις αλυσίδες επεξεργασίας δεδομένων από αισθητήρες LiDAR, ως τη δεύτερη κρίσιμη τεχνολογία αντίληψης στα αυτόνομα οχήματα. Όπως και στην περίπτωση των καμερών, παρουσιάζονται τα τυπικά βήματα (προ)επεξεργασίας δεδομένων, η ροή δεδομένων μεταξύ αισθητήρα και επιπέδου αντίληψης, τα βασικά δομικά στοιχεία του επιπέδου αντίληψης (perception layer), καθώς και οι σχετικές επιπτώσεις ασφάλειας. Ειδική αναφορά γίνεται στις τρέχουσες ερευνητικές εξελίξεις, τόσο ως προς τις επιθετικές όσο και τις αμυντικές τεχνικές σε εφαρμογές αυτόνομων συστημάτων βασισμένων σε LiDAR.
- Ενοποίηση δεδομένων αισθητήρων, Συνεργατική αντίληψη και Συστήματα πραγματικού χρόνου: Αφού παρουσιαστεί το θεωρητικό υπόβαθρο για τα συστήματα που βασίζονται σε κάμερα και LiDAR, το μάθημα επικεντρώνεται σε συνήθεις προσεγγίσεις συγχώνευσης αισθητήρων (sensor fusion), στις οποίες συνδυάζονται οι δύο τεχνολογίες. Παρουσιάζονται πολυτροπικά μοντέλα αντίληψης, ερευνητικές κατευθύνσεις και συναφή ζητήματα ασφάλειας. Επιπλέον, εξετάζονται εφαρμογές συνεργατικής αντίληψης μεταξύ πολλών συστημάτων και οι αντίστοιχες επιπτώσεις στην ασφάλεια. Δεδομένου ότι τα αυτόνομα συστήματα βασίζονται σε μεθοδολογίες πραγματικού χρόνου, καλύπτεται το θεωρητικό τους υπόβαθρο, καθώς και χαρακτηριστικές επιθέσεις και τεχνικές προστασίας.
- Ενσύρματες και ασύρματες επικοινωνίες σε περιβάλλοντα αυτόνομων οχημάτων: Η ενότητα αναδεικνύει το πλαίσιο ασφάλειας των επικρατέστερων ενσύρματων και ασύρματων αρχιτεκτονικών επικοινωνίας και των σχετικών πρωτοκόλλων που συναντώνται σε αυτόνομα οχήματα. Για να αποκτήσουν όλοι οι φοιτητές (ανεξάρτητα από το τεχνικό υπόβαθρό τους) τη δυνατότητα να μελετούν αυτά τα συστήματα και το περιβάλλον τους, παρέχεται εισαγωγή στη φυσική ραδιοσυχνοτήτων (RF) και στη χρήση συστημάτων ραδιοεπικοινωνίας οριζόμενης από λογισμικό (SDR) με εργαλεία ανοιχτού κώδικα όπως το GNUradio. Παράλληλα, καλύπτεται το θεωρητικό πλαίσιο για την ενσύρματη ενδο-οχηματική επικοινωνία (π.χ. CAN, LIN), καθώς και οι επιπτώσεις ασφάλειας και οι σύγχρονες ερευνητικές τάσεις γύρω από τα αντίστοιχα πρωτόκολλα επικοινωνίας.
- Μηχανισμοί ανίχνευσης απειλών και προστασίας από επιθέσεις: Η τελευταία ενότητα επικεντρώνεται στα συνήθως προτεινόμενα μέτρα προστασίας για την προστασία από τις ευπάθειες που συζητήθηκαν στις προηγούμενες θεματικές. Περιλαμβάνει τόσο αντιδραστικά μέτρα (π.χ. συστήματα ανίχνευσης εισβολών για οχήματα-automotive IDS), όσο και προληπτικά μέτρα (π.χ. δοκιμές μέσω προσομοιώσεων και τεχνικές fuzzing). Δίνεται έμφαση στις πρόσφατες ερευνητικές εξελίξεις, ενώ ταυτόχρονα αναλύονται κριτικά τα υφιστάμενα κενά και οι περιορισμοί των προτεινόμενων τεχνικών.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- Bruce Schneier, “Applied Cryptography Protocols, Algorithms, and Source Code in C” (https://www.schneier.com/books/applied-cryptography/)
- Dr. Charlie Miller, Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle” (https://illmatics.com/Remote%20Car%20Hacking.pdf)
- Craig Smith, “The Car Hacker’s Handbook” (https://nostarch.com/carhacking)

- Συναφή επιστημονικά περιοδικά:
  - USENIX Symposium on Vehicle Security and Privacy (VehicleSec)
  - Network and Distributed System Security Symposium (NDSS)
  - ACM Conference on Embedded Networked Sensor Systems (SenSys)

3.15.2.2.5 Κυβερνοασφάλεια: Λειτουργικές πρακτικές στον εντοπισμό και αντιμετώπιση επιθέσεων (Cybersecurity: Attack, Defence, and Operational Practice)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή: Παρουσιάζεται το τοπίο της κυβερνοασφάλειας, οι βασικές πηγές απειλών και η ηθική οπτική του hacking και της προστασίας. Οι φοιτητές και φοιτήτριες μελετούν γνωστά περιστατικά παραβίασης της ασφάλειας ενός συστήματος και δημιουργούν ένα εικονικό εργαστηριακό περιβάλλον για πρακτική εξάσκηση.
- Συλλογή Πληροφοριών (OSINT): Παρουσιάζονται τεχνικές παθητικής και ενεργητικής συλλογής πληροφοριών από επιτιθέμενους. Οι φοιτητές και φοιτήτριες μαθαίνουν να χρησιμοποιούν εργαλεία OSINT για αποτύπωση στόχων (footprinting) και συλλογή πληροφοριών.
- Σάρωση & Απαρίθμηση: Αναλύονται τεχνικές σάρωσης δικτύων και απαρίθμησης υπηρεσιών, χρηστών και πληροφοριών συστημάτων. Στο εργαστήριο γίνεται χρήση εργαλείων όπως το Nmap για την αποτύπωση επιφανειών επίθεσης (attack surface) και τον εντοπισμό ευπαθειών.
- Τεχνικές Εκμετάλλευσης: Παρουσιάζεται ο τρόπος εκμετάλλευσης γνωστών ευπαθειών σε web εφαρμογές, συστήματα και υπηρεσίες. Οι φοιτητές και φοιτήτριες εξασκούνται σε περιβάλλον εργαστηρίου με εργαλεία όπως το Metasploit.
- Ενέργειες μετά την Εκμετάλλευση Ευπαθειών (Post-Exploitation) & Πλευρική Κίνηση (Lateral Movement): Εξετάζονται μέθοδοι που χρησιμοποιούν οι επιτιθέμενοι μετά την αρχική πρόσβαση, όπως κλιμάκωση προνομίων, διατήρηση πρόσβασης και πλευρική κίνηση στο δίκτυο. Οι φοιτητές και φοιτήτριες εκτελούν σχετικές ενέργειες σε προσομοιωμένα σενάρια.
- Μηχανισμοί Προστασίας: Παρουσιάζονται οι αρχές της πολυεπίπεδης προστασίας (defense-in-depth) και βασικές τεχνολογίες όπως firewalls, antivirus και IDS/IPS. Οι φοιτητές και φοιτήτριες εξασκούνται στην παραμετροποίηση των εργαλείων αυτών.
- Παρακολούθηση Ασφαλείας & Καταγραφή: Περιγράφονται τρόποι για τον εντοπισμό επιθέσεων μέσω ανάλυσης αρχείων καταγραφής (logs). Οι φοιτητές και φοιτήτριες θα αξιοποιήσουν εργαλεία SIEM για να αναγνωρίσουν παραβιάσεις και να συσχετίσουν γεγονότα.
- Αντιμετώπιση Περιστατικών (Incident Response): Παρουσιάζεται ο κύκλος ζωής της

διαχείρισης/αντιμετώπισης περισαταικών: προετοιμασία, ανίχνευση, περιορισμός, εξάλειψη, αποκατάσταση και εξαγωγή συμπερασμάτων.

- Πληροφορίες για Απειλές (Threat Intelligence): Εξετάζονται οι τύποι CTI, η δημιουργία προφίλ επιτιθέμενων και οι πηγές πληροφοριών. Οι φοιτητές και φοιτήτριες μαθαίνουν να παράγουν και να χρησιμοποιούν πληροφορίες για την ενίσχυση της ανίχνευσης και της προστασίας.
- Κέντρα Επιχειρήσεων Ασφάλειας (SOC): Παρουσιάζεται η λειτουργία, τα εργαλεία και οι διαδικασίες ενός SOC. Οι φοιτητές και φοιτήτριες προσομοιώνουν εργασία σε περιβάλλον SOC, διαχειριζόμενοι ειδοποιήσεις, εκτελώντας διαλογή (triage) και καταγράφοντας ενέργειες αντιμετώπισης.
- Ανάλυση Κακόβουλου Λογισμικού & Αντίστροφη Μηχανική (Reverse Engineering): Καλύπτονται βασικοί τύποι κακόβουλου λογισμικού, στατική και δυναμική ανάλυση, καθώς και η χρήση απομονωμένων περιβαλλόντων (sandbox). Οι φοιτητές και φοιτήτριες εξετάζουν με ασφάλεια δείγματα malware για να κατανοήσουν τη συμπεριφορά τους.
- Διαχείριση Ταυτοτήτων, Πρόσβασης & Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης (Zero Trust): Παρουσιάζονται οι αρχές ασφαλούς ταυτοποίησης και εξουσιοδότησης, στη διαχείρηση ταυτοτήτων και στα μοντέλα Μηδενικής Εμπιστοσύνης (Zero Trust). Αναλύεται η χρήση πολυπαραγοντικής ταυτοποίησης (MFA), συστήματα ενιαίας πρόσβασης (SSO) και αδυναμίες των μηχανισμών ελέγχου πρόσβασης.
- Εφαρμογή & Αξιολόγηση: Οι φοιτητές και φοιτήτριες εφαρμόζουν τις γνώσεις τους σε τελική παρουσίαση και/ή πρακτική επίδειξη, βασισμένη σε σενάριο επίθεσης-άμυνας ή λειτουργικής ασφάλειας από τον πραγματικό κόσμο.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Alsmadi, I. (2023). The NICE cyber security framework: Cyber security intelligence and analytics. Springer. https://doi.org/10.1007/978-3-031-21651-0
  - Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity – Attack and defense strategies: Red and blue team tactics for security professionals (3rd ed.). Packt Publishing.
- Συναφή επιστημονικά περιοδικά:
  - Journal of Cybersecurity (Oxford University Press)
  - IEEE Security & Privacy
  - International Journal of Critical Infrastructure Protection (Elsevier)
  - Cybersecurity (SpringerOpen)

3.15.2.2.6 Κυβερνοασφάλεια σε Βιομηχανικά Περιβάλλοντα (Cybersecurity in Industrial Scenarios)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Βιομηχανικά περιβάλλοντα και έξυπνες τεχνολογίες
  - Βιομηχανικά περιβάλλοντα

- Κυβερνοφυσικά Συστήματα (CPS) - Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) και άλλες τεχνολογίες σε βιομηχανικά περιβάλλοντα
- Βιομηχανικά πρωτόκολλα επικοινωνίας

- Απειλές κυβερνοασφάλειας για βιομηχανικά περιβάλλοντα
  - Κύρια ζητήματα κυβερνοασφάλειας σε βιομηχανικά περιβάλλοντα
  - Ταξινόμιση απειλών και πραγματικές περιπτώσεις
- Βασικές δυνατότητες κυβερνοασφάλειας για βιομηχανικά περιβάλλοντα
  - Αρχές μηδενικής εμπιστοσύνης (zero-trust) και πολυεπίπεδης προστασίας (defense in-depth)
  - Κανονιστικά πλαίσια, πρότυπα και συστάσεις
  - Ασφάλεια περιμέτρου στον βιομηχανικό χώρο
  - Ασφαλής συνδεσιμότητα και προσβασιμότητα
- Προηγμένες δυνατότητες κυβερνοασφάλειας για βιομηχανικά περιβάλλοντα
  - Προληπτική και ενεργή προστασία
  - Συνεχής παρακολούθηση και αξιολόγηση
  - Προσομοίωση για προστασία, εκπαίδευση και δοκιμές
  - Εμπιστοσύνη και ιδιωτικότητα

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - Shinde, A., Lokegaonkar, B. (2024). Industrial Cybersecurity: A Practical Approach to OT Protection. (n.p.): CyberAuthor.
  - Ackerman, P. (2021). Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment. Alemanya: Packt Publishing.
  - Shinde, A., Lokegaonkar, B. (2024). Industrial Cybersecurity: A Practical Approach to OT Protection. (n.p.): CyberAuthor.
  - Knapp, E. D. (2024). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Estats Units d'Amèrica: Syngress
- Συναφή επιστημονικά περιοδικά:
  - IEEE Transactions on Industrial Informatics
  - IEEE Transactions on Industrial Cyber-Physical Systems
  - ACM Transactions on Cyber-Physical Systems
  - IEEE Communications Surveys & Tutorials
  - IEEE Transactions on Secure and Dependable Computing
  - IEEE Transactions on Information Forensics and Security
  - Computers and Security, Elsevier
  - IEEE Security & Privacy
  - ACM Transactions on Privacy and Security, μεταξύ άλλων
- Συναφή επιστημονικά συνέδρια:

- BlackHat
- ESORICS
- Usenix Security
- ACM Conference on Computer and Communications Security
- IEEE International Conference on Cyber Security and Resilience, μεταξύ άλλων συναφών συνεδρίων

3.15.2.2.7 Κυβερνοασφάλεια στον Πολιτικό Τομέα: Εσωτερικές και Εξωτερικές Διαστάσεις (Cybersecurity in the Political Domain: Internal and External Dimensions)

ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στις Κυβερνοαπειλές, την Κυβερνοανθεκτικότητα και την Κυβερνοπολιτική: Η εισαγωγή αυτή θέτει τα θεμέλια παρουσιάζοντας βασικές έννοιες της κυβερνοασφάλειας, της κυβερνοανθεκτικότητας και της κυβερνοπολιτικής στο πλαίσιο των διεθνών σχέσεων. Οι φοιτητές και φοιτήτριες θα εξερευνήσουν πώς οι κυβερνοαπειλές έχουν εξελιχθεί σε πολιτικά ζητήματα τόσο στο εσωτερικό των κρατών όσο και σε διεθνές επίπεδο.
- Κυβερνοαπειλές κατά της Δημοκρατίας - Θεσμούς, Παραπληροφόρηση και Κοινωνικός Αντίκτυπος: Παρουσιάζεται ο τρόπος με τον οποίο οι κυβερνοαπειλές υπονομεύουν τους δημοκρατικούς θεσμούς και τις πολιτικές διαδικασίες. Θέματα που καλύπτονται περιλαμβάνουν την παρέμβαση σε εκλογές, επιχειρήσεις παραπληροφόρησης και την πόλωση στο διαδίκτυο. Μέσα από περιπτωσιολογικές μελέτες, οι φοιτητές και φοιτήτριες θα αξιολογήσουν τη διάβρωση της δημόσιας εμπιστοσύνης και θα εξετάσουν τρόπους ενίσχυσης της δημοκρατικής ανθεκτικότητας, όπως η ψηφιακή παιδεία, η πολιτική τεχνολογία και οι ρυθμιστικές παρεμβάσεις.
- Κρατικοί και Μη Κρατικοί Φορείς στον Κυβερνοχώρο: Οι φοιτητές και φοιτήτριες θα αναλύσουν το φάσμα των δρώντων που δραστηριοποιούνται στον κυβερνοχώρο – εθνικά κράτη, εντεταλμένες ομάδες (proxy groups), κυβερνοεγκληματίες, ακτιβιστές χάκερ (hacktivists) και ιδιωτικές εταιρείες κυβερνοασφάλειας. Η ενότητα εστιάζει στα κίνητρα, τις τακτικές και την πολυπλοκότητα της απόδοσης ευθύνης (attribution), καθώς και στη στρατηγική χρήση μη κρατικών φορέων σε συγκρούσεις υβριδικού χαρακτήρα.
- Κυβερνοαπειλές στις Κοινωνικές και Πολιτισμικές Διαστάσεις: Εξετάζεται ο τρόπος με τον οποίο οι κυβερνοαπειλές επηρεάζουν την ανθρώπινη συμπεριφορά, τη δημόσια εμπιστοσύνη και τον ψηφιακό πολιτισμό. Οι φοιτητές και φοιτήτριες θα αξιολογήσουν τις διαπολιτισμικές αντιλήψεις για την κυβερνοασφάλεια και θα αναλύσουν ζητήματα όπως η κοινωνική μηχανική (social engineering), η διαδικτυακή χειραγώγηση και οι ψυχολογικές επιπτώσεις του κυβερνοεγκλήματος και της παραπληροφόρησης.
- Κυβερνοασφάλεια στη Διεθνή Πολιτική - Γεωπολιτική και Εθνικές Στρατηγικές: Παρουσιάζεται ο τρόπος με τον οποίο η κυβερνοασφάλεια έχει καταστεί καθοριστικός παράγοντας στην παγκόσμια πολιτική και γεωπολιτική, επηρεάζοντας ουσιαστικά τις διεθνείς σχέσεις και τις εθνικές στρατηγικές ασφάλειας. Η κυβερνοασφάλεια προβάλλεται ως εργαλείο επίτευξης εθνικών συμφερόντων, ενώ οι κυβερνοαπειλές αντιμετωπίζονται όλο και περισσότερο ως ζήτημα διπλωματίας και πολιτικής.

- Κυβερνοασφάλεια και Θεωρίες Διεθνών Σχέσεων: Οι φοιτητές και φοιτήτριες θα εφαρμόσουν κλασικές και σύγχρονες θεωρίες των Διεθνών Σχέσεων (όπως ο ρεαλισμός, ο φιλελευθερισμός, ο εποικοδομητισμός και οι κριτικές θεωρίες) για να αναλύσουν προκλήσεις σχετικές με τον κυβερνοχώρο. Μέσα από αυτές τις θεωρητικές οπτικές, θα εξετάσουν πώς τα κράτη και οι μη κρατικοί φορείς δρουν στον κυβερνοχώρο, πώς εκδηλώνονται η ισχύς και η συνεργασία στο ψηφιακό πεδίο, και πώς οι ιδεολογικοί παράγοντες επηρεάζουν τον πολιτικές και τον διάλογο για την κυβερνοασφάλεια. Δίνεται έμφαση στη χρησιμότητα της θεωρίας για την κατανόηση της στρατηγικής συμπεριφοράς, της ανάπτυξης κανόνων και της παγκόσμιας διακυβέρνησης του κυβερνοχώρου.
- Επιπτώσεις των Κυβερνοαπειλών και Κυβερνοεπιθέσεων (Μέρος Α') – Διαστάσεις σε Στρατιωτικές Εφαρμογές και στην Εθνική Ασφάλεια: Αυτή την εβδομάδΕεξετάζεται ο αντίκτυπος των κυβερνοαπειλών και επιθέσεων στον στρατιωτικό τομέα και στον τομέα της εθνικής ασφάλειας. Οι φοιτητές και φοιτήτριες θα μελετήσουν τη χρήση κυβερνοεπιθέσεων για σκοπούς κατασκοπείας, κυβερνοπολέμου, τρομοκρατίας και διατάραξης στρατιωτικών επιχειρήσεων. Η ενότητα αναλύει ευπάθειες σε στρατιωτικά συστήματα, δίκτυα πληροφοριών και υποδομές διοίκησης και ελέγχου. Κεντρικά θέματα περιλαμβάνουν τον κίνδυνο κλιμάκωσης, τη σύγχυση ανάμεσα σε πολιτικούς και στρατιωτικούς στόχους, καθώς και τον ρόλο των κυβερνοδυνατοτήτων στον υβριδικό πόλεμο και την αποτροπή.
- Επιπτώσεις των Κυβερνοαπειλών και Κυβερνοεπιθέσεων (Μέρος Β') - Διπλωματικές και Πολιτικές Διαστάσεις: Σε συνέχεια της προηγούμενης θεματικής σχετικά με στρατιωτικές εφαρμογές και εθνική ασφάλεια, αυτή η ενότητα εξετάζει πώς οι κυβερνοαπειλές και επιθέσεις επηρεάζουν τη διπλωματία και τις πολιτικές σχέσεις μεταξύ κρατών. Οι φοιτητές και φοιτήτριες θα διερευνήσουν πώς περιστατικά υψηλού προφίλ στον κυβερνοχώρο μπορούν να διαβρώσουν την εμπιστοσύνη μεταξύ κρατών, να ασκήσουν πίεση στις συμμαχίες και να περιπλέξουν τις παραδοσιακές διπλωματικές διαδικασίες. Αυτή η ενότητα αναφέρεται στις προκλήσεις της απόδοσης ευθύνης (attribution) στον κυβερνοχώρο, συμπεριλαμβανομένης της τεχνικής αβεβαιότητας και τις πολιτικές συνέπειες, και λαμβάνει υπόψη το πως κράτη αντιδρούν μέσα από κυρώσεις, δημόσιες αποδώσεις ευθύνης ή νομικές διώξεις. Ιδιαίτερη έμφαση δίνεται στην δυσκολία διατήρησης διαλόγου κατά τη διάρκεια και μετά από κυβερνοκρίσεις, η χρήση μηχανισμών επικοινωνίας σε περιόδους κρίσης και ο ρόλος των διεθνών κανόνων και του δικαίου στη ρύθμιση της κρατικής συμπεριφοράς. Επιπλέον, αναλύονται οι συνέπειες των υβριδικών επιχειρήσεων που συνδυάζουν κυβερνοεπιθέσεις με εκστρατείες παραπληροφόρησης, δυσχεραίνοντας περαιτέρω τη διπλωματική ανταπόκριση και την ειρηνική επίλυση συγκρούσεων.
- Επιπτώσεις των Κυβερνοαπειλών και Κυβερνοεπιθέσεων (Μέρος Γ') - Οικονομικές Διαστάσεις: Η συνεδρία αυτή επικεντρώνεται στον οικονομικό αντίκτυπο των κυβερνοαπειλών, ιδίως όσον αφορά διαταραχές σε χρηματοοικονομικά συστήματα, κλοπή πνευματικής ιδιοκτησίας και επιθέσεις σε κρίσιμες υποδομές. Οι φοιτητές και φοιτήτριες θα μελετήσουν πως περιστατικά όπως επιθέσεις λυτρισμικού (ransomware), βιομηχανική κατασκοπεία και παραβιάσεις στην εφοδιαστική αλυσίδα, μπορούν να προκαλέσουν σημαντικές οικονομικές ζημίες, να υπονομεύσουν την εμπιστοσύνη των επενδυτών και να απειλήσουν την εθνική οικονομική σταθερότητα. Επιπλέον,

εξετάζονται οι μακροπρόθεσμες επιπτώσεις των επίμονων κυβερνοαπειλών στην οικονομική ανθεκτικότητα, την ανταγωνιστικότητα και την ψηφιακή μεταρρύθμιση κρίσιμων τομέων.

- Διεθνές Δίκαιο και Ηθική στον Κυβερνοχώρο: Η ενότητα αυτή εξετάζει τις νομικές και ηθικές διαστάσεις της κρατικής και μη κρατικής δραστηριότητας στον κυβερνοχώρο. Οι φοιτητές και φοιτήτριες θα μελετήσουν βασικά νομικά πλαίσια, όπως το Εγχειρίδιο του Ταλλίν και τη Σύμβαση της Βουδαπέστης, και θα αναλύσουν κριτικά θεμελιώδεις αρχές όπως η κυριαρχία, η επιμέλεια (due diligence) και η αναλογικότητα στο πλαίσιο των κυβερνοεπιχειρήσεων. Η συζήτηση θα επεκταθεί σε ηθικά διλήμματα που σχετίζονται με την ιδιωτικότητα, την επιτήρηση, την κρατική καταστολή και τα ψηφιακά δικαιώματα. Η ενότητα ενθαρρύνει τους φοιτητές να αξιολογήσουν τα όρια και τις δυνατότητες των υπαρχόντων νομικών εργαλείων και των προσπαθειών ανάπτυξης διεθνών προτύπων διακυβέρνησης του κυβερνοχώρου.
- Αναδυόμενες Τεχνολογίες, Τεχνητή Νοημοσύνη και το Μέλλον των Κυβερνοσυγκρούσεων: Η συγκεκριμένη συνεδρία έχει στραμμένο το βλέμμα στο μέλλον και εξετάζει τον μετασχηματιστικό ρόλο των αναδυόμενων τεχνολογιών στο τοπίο των κυβερνοαπειλών. Οι φοιτητές και φοιτήτριες θα αναλύσουν πώς η τεχνητή νοημοσύνη, η κβαντική υπολογιστική και τα αυτόνομα συστήματα μεταβάλλουν δραστικά τόσο τις επιθετικές όσο και τις αμυντικές κυβερνοδυνατότητες. Σημαντικά θέματα περιλαμβάνουν την παραπληροφόρηση που βασίζεται σε AI, τις αυτοματοποιημένες κυβερνοεπιχειρήσεις και τα ηθικά διλήμματα που εγείρονται από αλγοριθμικές αποφάσεις σε πολεμικά και κατασκοπευτικά συστήματα. Τονίζεται η αυξανόμενη πολυπλοκότητα στην πρόβλεψη, την απόδοση ευθύνης και την αντίδραση σε απειλές, ενόψει της ταχύτατης τεχνολογικής εξέλιξης.
- Στρατηγικές Αντιμετώπισης και Ενίσχυση Ικανοτήτων για την Κυβερνοανθεκτικότητα: Παρουσιάζονται στρατηγικές ενίσχυσης της κυβερνοανθεκτικότητας σε εθνικό και διεθνές επίπεδο. Οι φοιτητές και φοιτήτριες θα αναλύσουν τον ρόλο των συμπράξεων δημόσιου και ιδιωτικού τομέα, της εκπαίδευσης και κατάρτισης στην κυβερνοασφάλεια, της προστασίας κρίσιμων υποδομών και των πρωτοβουλιών οικοδόμησης ικανοτήτων για την ενίσχυση της κοινωνικής ανθεκτικότητας σε κυβερνοαπειλές. Έμφαση δίνεται στη διατομεακή συνεργασία, την θεσμική ετοιμότητα, και την συνοχή της πολιτικής σε τεχνικούς, νομικούς και πολιτικούς τομείς.
- Προσομοίωση Κυβερνοκρίσης - Στρατηγική Αντίδραση και Διπλωματία στην Πράξη: Σε αυτή την κορυφαία εκπαιδευτική προσομοίωση, οι φοιτητές και φοιτήτριες καλούνται να εφαρμόσουν τις αποκτηθείσες γνώσεις σε ένα δυναμικό σενάριο κυβερνοκρίσης πραγματικού χρόνου, το οποίο περιλαμβάνει μια επίθεση πολλαπλών σταδίων σε κρίσιμη υποδομή. Οι συμμετέχοντες οργανώνονται σε ομάδες με ρόλους που προσομοιώνουν κυβερνήσεις, διεθνείς οργανισμούς, μέσα ενημέρωσης και ιδιωτικές τεχνολογικές εταιρείες, με σκοπό να σχεδιάσουν και να εφαρμόσουν συντονισμένες στρατηγικές αντίδρασης. Η προσομοίωση περιλαμβάνει διαδικασίες λήψης αποφάσεων, νομική και ηθική αξιολόγηση, δημόσια επικοινωνία και διπλωματική διαπραγμάτευση. Ολοκληρώνεται με μια δομημένη απενημέρωση, όπου επισημαίνονται τα διδάγματα, τα στρατηγικά λάθη και η πολυπλοκότητα της διακυβέρνησης του κυβερνοχώρου υπό συνθήκες έντασης και κρίσης.

ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:
  - **Βιβλία**
    - Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
    - Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.
    - Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
    - Nye, J. S. (2011). The future of power. PublicAffairs.
    - Rid, T. (2013). Cyber war will not take place. Oxford University Press.
    - Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
    - Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
    - Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
    - Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.
    - Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.
  - **Άρθρα Επιστημονικών Περιοδικών**
    - Bradshaw, S., & Howard, P. N. (2019). The global disinformation order. Oxford Internet Institute Working Paper, 2019(3).
    - Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.
    - Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. American Journal of International Law, 110(3), 425–479.
    - Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40.
    - Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. Philosophy & Technology, 31(2)
- Συναφή επιστημονικά περιοδικά:
  - **International Security**
    - Published by MIT Press, this journal features foundational work on cyber conflict, deterrence, and cyber-enabled statecraft.
    - International Security. (n.d.). MIT Press. https://direct.mit.edu/isec
  - **Journal of Strategic Studies**
    - Covers strategic theory and national security, including cyberwarfare and defense planning.
    - Journal of Strategic Studies. (n.d.). Taylor & Francis. https://www.tandfonline.com/journals/fjss20

- **European Journal of International Security**
  - Explores international security issues through critical, constructivist, and strategic lenses—including cyberspace as a security domain.
  - European Journal of International Security. (n.d.). Cambridge University Press. https://www.cambridge.org/core/journals/european-journal-of-international-security
- **Security Dialogue**
  - A key journal in critical security studies, publishing on the politics and discourse of cybersecurity, digital surveillance, and hybrid threats.
  - Security Dialogue. (n.d.). SAGE Publications. https://journals.sagepub.com/home/sdi
- **International Affairs**
  - One of the oldest IR journals, covering cyber diplomacy, global norms, and state responses to digital threats.
  - International Affairs. (n.d.). Chatham House / Oxford University Press. https://academic.oup.com/ia
- **Review of International Studies**
  - Publishes theoretical and empirical work on global politics, including cybersecurity as an emerging topic in global governance.
  - Review of International Studies. (n.d.). Cambridge University Press. https://www.cambridge.org/core/journals/review-of-international-studies
- **Foreign Policy Analysis**
  - Focuses on decision-making, strategic culture, and how state actors navigate issues like cyber threats.
  - Foreign Policy Analysis. (n.d.). Oxford University Press. https://academic.oup.com/fpa
- **Global Studies Quarterly**
  - Publishes cutting-edge work on digital geopolitics, cyber cooperation, and IR theory in the age of AI and big data.
  - Global Studies Quarterly. (n.d.). International Studies Association. https://academic.oup.com/isagsq
- **Politics & Governance**
  - Open-access journal that frequently publishes thematic issues on digital authoritarianism, cyber diplomacy, and governance of emerging technologies.
  - Politics & Governance. (n.d.). Cogitatio Press. https://www.cogitatiopress.com/politicsandgovernance
- **Contemporary Security Policy**
  - Publishes empirical and conceptual studies on international security, including cyber strategy, resilience, and cyber-enabled warfare.
  - Contemporary Security Policy. (n.d.). Taylor & Francis. https://www.tandfonline.com/journals/fcsp20

3.15.2.3 Ακαδημαϊκό Εξάμηνο 3

3.15.2.3.1 Μεταπτυχιακή Διπλωματική Εργασία (MSc Thesis)

Πλαίσιο εκπόνησης

Η Μεταπτυχιακή Διπλωματική Εργασία εκπονείται κατά μόνας ή από ομάδες φοιτητών και φοιτητριών, υπό την επίβλεψη Διδάσκοντος ή Διδάσκουσας στο Π.Μ.Σ. (Επιβλέπων ή Επιβλέπουσα), στο πλαίσιο των προβλέψεων της κείμενης νομοθεσίας και αφορά σε γνωστικό αντικείμενο που επιστημονικά εντάσσεται στο Π.Μ.Σ..

Κάθε Μεταπτυχιακή Διπλωματική Εργασία πρέπει να αποδεικνύει προηγμένες θεωρητικές γνώσεις, κριτική σκέψη, ικανότητα στην ανάλυση και σύνθεση προβλημάτων και είναι επιθυμητό να τεκμηριώνει ερευνητική ικανότητα του μεταπτυχιακού φοιτητή ή φοιτήτριας για παραγωγή νέας γνώσης.

Η Μεταπτυχιακή Διπλωματική Εργασία μπορεί να αναφέρεται σε θεωρητικά ή εφαρμοσμένα θέματα, ενώ είναι επιτρεπτό να πραγματοποιείται σε συνεργασία με ιδιωτικό ή δημόσιο φορέα που δραστηριοποιείται ή παρουσιάζει ενδιαφέρον σε συναφή αντικείμενα με εκείνα που πραγματεύεται και θεραπεύει το Π.Μ.Σ., στο πλαίσιο των προβλέψεων της κείμενης νομοθεσίας.

Αξιολόγηση και κριτήρια βαθμολόγησης

Οι Μεταπτυχιακές Διπλωματικές Εργασίες αποτιμώνται με κριτήρια την άρτια επιλογή βιβλιογραφικών πηγών, την επιστημονική ορθότητα της ανάλυσης της υπάρχουσας γνώσης, την εμβάθυνση στο πεδίο, το εύρος κάλυψης του θέματος, την ακρίβεια κατά την περιγραφή, τη συνεκτική δομή και εναργή αποτύπωση των επιχειρημάτων, τα στοιχεία ερευνητικής συνεισφοράς και παραγωγής νέας γνώσης στο επιστημονικό πεδίο, τη συνολική επιστημονική ωριμότητα του πονήματος, τη συμμόρφωση της εμφάνισης και των περιεχομένων της εργασίας με τις σχετικές οδηγίες, καθώς και την πληρότητα και ωριμότητα κατά την προφορική παρουσίαση, τη συνέπεια στον διαθέσιμο χρόνο και την επιστημονικά ορθή ανταπόκριση του μεταπτυχιακού φοιτητή ή της φοιτήτριας σε ερωτήματα της Εξεταστικής Επιτροπής.

Λοιπά στοιχεία για τις ακολουθητέες διαδικασίες και το συνολικό πλαίσιο υποβολής αίτησης, επίβλεψης κατά την εκπόνηση, συγγραφής, παρουσίασης και αξιολόγησης αρμοδίως, περιλαμβάνονται στον οικείο Κανονισμό Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας (Παράρτημα 7: Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας).

3.16 Μαθησιακά Αποτελέσματα

3.16.1 Γνώσεις

Στα πλαίσια του Π.Μ.Σ., οι βασικοί πυλώνες γνώσεων που αποκτούν οι μεταπτυχιακοί φοιτητές και φοιτήτριες είναι:

- **Αρχές και ρυθμιστικό πλαίσιο προστασίας δεδομένων**: Κατανόηση βασικών εννοιών ιδιωτικότητας, φιλοσοφικών και νομικών θεμελίων, του Γενικού Κανονισμού Προστασίας Δεδομένων και συγκριτική ανάλυση με άλλα διεθνή πλαίσια.
- **Συμμόρφωση και διακυβέρνηση**: Εφαρμογή μηχανισμών συγκατάθεσης, νομικών βάσεων, τήρηση αρχείων, διαδικασίες σε περίπτωση παραβιάσεων, ρόλοι υπευθύνου επεξεργασίας, υπευθύνου προστασίας δεδομένων, λογοδοσία και ετοιμότητα για έλεγχο.
- **Αξιολόγηση κινδύνων και εκτίμηση αντικτύπου**: Διενέργεια εκτιμήσεων κινδύνου και αντικτύπου, ερμηνεία αποτελεσμάτων και στρατηγικές μετριασμού.
- **Προστασία ιδιωτικότητας από τον σχεδιασμό και τεχνολογίες ενίσχυσης ιδιωτικότητας**: Ενσωμάτωση προστασίας δεδομένων στον σχεδιασμό, χρήση τεχνικών ανωνυμοποίησης, διαφορικής ιδιωτικότητας και κρυπτογράφησης.
- **Ανάλυση τεχνολογιών και ηθικών ζητημάτων**: Επιπτώσεις της τεχνητής νοημοσύνης στην προστασία δεδομένων, κατάρτιση προφίλ, μεροληψία, έλλειψη διαφάνειας και θεσμικές ή ηθικές απαντήσεις.
- **Κυβερνοασφάλεια και διαχείριση κινδύνων**: Βασικές αρχές, νομοθεσία και πρότυπα, κουλτούρα ασφάλειας, ρόλος διοίκησης, σχεδιασμός και λειτουργία συστημάτων διαχείρισης ασφάλειας πληροφοριών.
- **Ασφάλεια δικτύων και διαδικτύου των πραγμάτων**: Σχεδίαση ασφαλών υποδομών, προστασία από απειλές σε πρωτόκολλα επικοινωνίας, ασφάλεια συσκευών και διενέργεια ελέγχων διείσδυσης και ανάλυσης απειλών.
- **Ψηφιακή ευημερία και ανθρώπινοι παράγοντες κινδύνου**: Αντιμετώπιση τεχνολογικού άγχους, επαγγελματικής εξουθένωσης, διαδικτυακού εκφοβισμού, χειραγώγησης μέσω αλγορίθμων και επιδράσεων κοινωνικών δικτύων.
- **Δοκιμές ασφάλειας και ηθική διείσδυση συστημάτων**: Συλλογή πληροφοριών από ανοικτές πηγές, αναγνώριση δικτύου, επιθέσεις σε υπηρεσίες, κοινωνική μηχανική, έλεγχοι διείσδυσης και αξιολόγηση ευπαθειών.
- **Κέντρα επιχειρήσεων ασφάλειας και διαχείριση περιστατικών**: Οργάνωση και λειτουργία, ανίχνευση απειλών, ανάπτυξη κανόνων ανίχνευσης, διαδικασίες περιορισμού και αποκατάστασης, αναζήτηση απειλών και σύνταξη τεχνικών αναφορών.
- **Εξειδικευμένες εφαρμογές ασφάλειας**: Προστασία αυτόνομων οχημάτων, βιομηχανικών εγκαταστάσεων και κρίσιμων υποδομών.
- **Προηγμένες τεχνολογίες προστασίας**: Ενεργητική κυβερνοάμυνα, πληροφορίες απειλών, εικονικά δίδυμα, κατανεμημένα μητρώα δεδομένων, τεχνητή νοημοσύνη και μηχανική μάθηση.

- **Κυβερνοπολιτική και διεθνείς σχέσεις**: Επιπτώσεις κυβερνοεπιχειρήσεων στην εθνική ασφάλεια, δημοκρατικούς θεσμούς, διεθνή διπλωματία και παγκόσμια διακυβέρνηση.
- **Κυβερνοανθεκτικότητα και νέες απειλές**: Προσαρμογή σε νέες τεχνολογίες, όπως οι κβαντικοί υπολογιστές, και ενίσχυση εμπιστοσύνης στα σύγχρονα περιβάλλοντα.

3.16.2 Δεξιότητες

Το πρόγραμμα είναι δομημένο με τρόπο ώστε να συναντώνται οι σύγχρονες διεπιστημονικές γνώσεις, με το πλαίσιο αποτελεσματικής και αποδοτικής εφαρμογής τους, με σκοπό να εφοδιαστούν οι μεταπτυχιακοί φοιτητές και φοιτήτριες με δεξιότητες απαραίτητες για τη σύγχρονη αγορά εργασίας στην Ελλάδα και διεθνώς και κατ' αποτέλεσμα να ενισχυθεί η δυνατότητα επαγγελματικής τους αποκατάστασης.

Με βάση τα ανωτέρω, ολοκληρώνοντας το πρόγραμμα, οι μεταπτυχιακοί φοιτητές και φοιτήτριες αναμένεται να δύνανται να:

- Διενεργούν μελέτες εκτίμησης αντικτύπου για την προστασία δεδομένων και εφαρμογή των ευρημάτων σε διακυβέρνηση και συμμόρφωση.
- Σχεδιάζουν διαδικασίες συγκατάθεσης, γνωστοποίησης και κοινοποίησης παραβιάσεων.
- Επιλέγουν και να χρησιμοποιούν τεχνολογίες ενίσχυσης ιδιωτικότητας, όπως ανωνυμοποίηση και κρυπτογράφηση.
- Αντιμετωπίζουν ευπάθειες σε δίκτυα και συστήματα και να διαχειρίζονται παραμέτρους ασφάλειας πρωτοκόλλων και μηχανισμών προστασίας.
- Μοντελοποιούν απειλές και να και εκτελούν ελέγχους διείσδυσης σε συστήματα και εφαρμογές, συμπεριλαμβανομένων των συστημάτων διαδικτύου των πραγμάτων.
- Συλλέγουν και να αναλύουν ψηφιακά αποδεικτικά και να συντάσσουν τεκμηριωμένες εγκληματολογικές αναφορές.
- Σχεδιάζουν και να υλοποιούν στρατηγικές βελτίωσης της ψηφιακής ευημερίας και αλλαγής συμπεριφοράς των χρηστών.
- Ενισχύουν την ασφάλεια αυτόνομων, βιομηχανικών και κρίσιμων υποδομών μέσω εγκατάστασης και ρύθμισης μηχανισμών προστασίας.
- Αναλύουν κυβερνοσυμβάντα με τεχνικές, νομικές και διπλωματικές παραμέτρους και να συμμετέχουν σε ασκήσεις κυβερνοκρίσεων.

3.16.3 Ικανότητες

Οι μεταπτυχιακοί φοιτητές και φοιτήτριες θα είναι σε θέση να:

- Εποπτεύουν τη διακυβέρνηση της ιδιωτικότητας και να ηγούνται προγραμμάτων προστασίας δεδομένων.
- Εξισορροπούν νομικές, ηθικές και επιχειρηματικές απαιτήσεις και να ενσωματώνουν την προστασία δεδομένων από τον σχεδιασμό σε συστήματα και προϊόντα.

- Αξιολογούν αναδυόμενες τεχνολογίες και να διαμορφώνουν πολιτικές θέσεις για τον οργανισμό.
- Καθοδηγούν διεπιστημονικές ομάδες και να καλλιεργούν κουλτούρα ιδιωτικότητας και ασφάλειας.
- Εποπτεύουν στρατηγικές κυβερνοασφάλειας, να συντονίζουν φόρουμ διακυβέρνησης και να διαχειρίζονται κινδύνους από τρίτα μέρη.
- Σχεδιάζουν ανθεκτικές αρχιτεκτονικές δικτύων, να αντιμετωπίζουν τρωτά σημεία και να υλοποιούν μηχανισμούς προστασίας.
- Ηγούνται επιχειρήσεων προστασίας, ασκήσεων ετοιμότητας και ερευνών περιστατικών.
- Ενσωματώνουν την ασφάλεια και την ψηφιακή ευημερία στην οργανωσιακή στρατηγική και στον σχεδιασμό υπηρεσιών.
- Προωθούν την ηθική υιοθέτηση τεχνολογιών και να αξιολογούν ψυχοκοινωνικούς κινδύνους.
- Επικοινωνούν αποτελεσματικά τεχνικά ευρήματα και να συνεργάζονται με φορείς και κέντρα αντιμετώπισης περιστατικών.

3.17 Εκπόνηση εργασιών

Οι μεταπτυχιακοί φοιτητές και φοιτήτριες σύμφωνα με τα προβλεπόμενα στον Κανονισμό και στον Οδηγό Σπουδών του Π.Μ.Σ. δύνανται να εκπονούν εργασίες στο πλαίσιο της εξέτασης του μαθήματος.

Για περισσότερες πληροφορίες σχετικά με την εκπόνηση εργασίας ανατρέξτε στο Παράρτημα 6: Κανονισμός Εκπόνησης Εργασιών .

3.18 Εκπόνηση Μεταπτυχιακής Διπλωματικής Εργασίας μέσω Erasmus

Στους μεταπτυχιακούς φοιτητές και φοιτήτριες παρέχεται η δυνατότητα εκπόνησης της Μεταπτυχιακής Διπλωματικής Εργασίας τους μέσω του προγράμματος LLP Erasmus σε χώρες της Ευρωπαϊκής Ένωσης ή σε τρίτες χώρες: [α] είτε σε συνεργασία με Πανεπιστήμια ή Ερευνητικά Ιδρύματα, [β] είτε μέσω του προγράμματος Πρακτικής Άσκησης σε ιδιωτικές ή δημόσιες επιχειρήσεις και οργανισμούς.

Για περισσότερες πληροφορίες σχετικά με την εκπόνηση της Μεταπτυχιακής Διπλωματικής Εργασίας ανατρέξτε στο Παράρτημα 7: Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας.

3.19 Ηλεκτρονικές Υπηρεσίες

3.19.1 Ηλεκτρονικές Υπηρεσίες Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση»

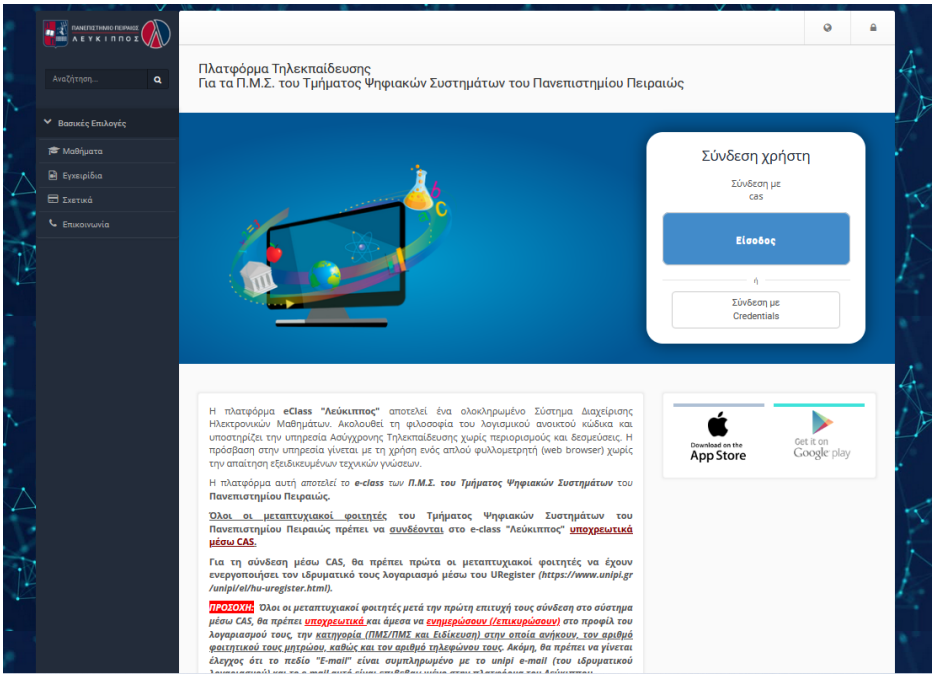
Το Π.Μ.Σ. «Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση» παρέχει στους μεταπτυχιακούς φοιτητές και φοιτήτριές του ένα σύνολο ηλεκτρονικών υπηρεσιών για την εξυπηρέτηση των ακαδημαϊκών τους δραστηριοτήτων.

3.19.1.1 Ιστοσελίδες Π.Μ.Σ., Τμήματος Ψηφιακών Συστημάτων, Πανεπιστημίου Πειραιώς

Κεντρικό σημείο ενημέρωσης και ανάρτησης ανακοινώσεων είναι η ιστοσελίδα του Π.Μ.Σ. (Αρχική - Π.Μ.Σ. Προηγμένες Τεχνολογίες Κυβερνοασφάλειας και Διακυβέρνηση), η ιστοσελίδα του Τμήματος Ψηφιακών Συστημάτων (http://www.ds.unipi.gr/) και η ιστοσελίδα του Πανεπιστημίου Πειραιώς (http://www.unipi.gr/).

3.19.1.2 Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων «ΛΕΥΚΙΠΠΟΣ» (Open eClass)

Το Π.Μ.Σ. παρέχει στους μεταπτυχιακούς φοιτητές και φοιτήτριές του την πλατφόρμα ασύγχρονης τηλεκπαίδευσης «Λεύκιππος» (Open eClass) μέσω της διεύθυνσης https://lefkippos.ds.unipi.gr/.



Εικόνα 1: Αρχική ιστοσελίδα πλατφόρμας ασύγχρονης διδασκαλίας «Λεύκιππος» (https://lefkippos.ds.unipi.gr/)

Η πλατφόρμα eClass «Λεύκιππος» (https://lefkippos.ds.unipi.gr/) αποτελεί ένα ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων. Ακολουθεί τη φιλοσοφία του λογισμικού ανοικτού κώδικα και υποστηρίζει την υπηρεσία Ασύγχρονης Τηλεκπαίδευσης χωρίς περιορισμούς και δεσμεύσεις. Η πρόσβαση στην υπηρεσία γίνεται με τη χρήση ενός απλού φυλλομετρητή (web browser) χωρίς την απαίτηση εξειδικευμένων τεχνικών γνώσεων. Η πλατφόρμα αυτή αποτελεί το e-class των Π.Μ.Σ. του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Όλοι οι μεταπτυχιακοί φοιτητές και φοιτήτριες του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς πρέπει να συνδέονται στο e-class «Λεύκιππος» υποχρεωτικά μέσω CAS Central Authentication Service. Για τη σύνδεση μέσω CAS, θα πρέπει πρώτα οι μεταπτυχιακοί φοιτητές και φοιτήτριες να έχουν ενεργοποιήσει τον ιδρυματικό τους λογαριασμό μέσω του URegister (https://www.unipi.gr/unipi/el/hu-uregister.html).

Όλοι οι μεταπτυχιακοί φοιτητές και φοιτήτριες μετά την πρώτη επιτυχή τους σύνδεση στο σύστημα μέσω CAS, θα πρέπει υποχρεωτικά και άμεσα να ενημερώσουν (/επικυρώσουν) στο προφίλ του λογαριασμού τους, την κατηγορία (Π.Μ.Σ./Π.Μ.Σ. και Ειδίκευση) στην οποία ανήκουν, τον αριθμό φοιτητικού τους μητρώου, καθώς και τον αριθμό τηλεφώνου τους. Ακόμη, θα πρέπει να γίνεται έλεγχος ότι το πεδίο «E-mail» είναι συμπληρωμένο με το unipi e-mail (του ιδρυματικού λογαριασμού) και το e-mail αυτό είναι επιβεβαιωμένο στην πλατφόρμα του Λεύκιππου.

Για πληροφορίες και υποστήριξη επικοινωνείτε με τους διαχειριστές της πλατφόρμας μέσω της επιλογής «Επικοινωνία».

3.19.1.3 Εικονικό Campus

Το Π.Μ.Σ. επιπροσθέτως των υποδομών εξ αποστάσεως εκπαίδευσης του Ιδρύματος, θα αξιοποιήσει το **πανευρωπαϊκό ψηφιακό και δια-πανεπιστημιακό campus** που έχει αναπτυχθεί στο πλαίσιο του Ευρωπαϊκού έργου **EU-iNSPIRE** στο οποίο συμμετέχει και συντονίζει. Το συγκεκριμένο ***Εικονικό Campus (Virtual Campus)*** επικεντρώνεται στην ανάπτυξη προηγμένων γνώσεων και δεξιοτήτων για την κυβερνοασφάλεια και αποτελεί το **κεντρικό επιχειρησιακό περιβάλλον** μέσω του οποίου θα υλοποιούνται οι εκπαιδευτικές δραστηριότητες αλλά και οι δραστηριότητες κατάρτισης που συνδέονται με το Π.Μ.Σ..

Το Εικονικό Campus λειτουργεί ως ένα **ενιαίο, ευέλικτο και προσβάσιμο ψηφιακό περιβάλλον μάθησης**, το οποίο ενσωματώνει διαφορετικές ψηφιακές ενότητες και τεχνολογίες, μπορεί να λειτουργήσει συνδυαστικά με τα υφιστάμενα ψηφιακά περιβάλλοντα του Ιδρύματος, και είναι ικανό να υποστηρίξει εξ' αποστάσεως εκπαίδευση, εικονική κινητικότητα και συνεργασία μεταξύ πολλαπλών εταίρων σε ευρωπαϊκό επίπεδο.

Το Εικονικό Campus:

- υποστηρίζει δομημένες και ιχνηλάσιμες διαδικασίες εισαγωγής και onboarding,
- παρέχει ευέλικτη, δεξιοκεντρική εκπαιδευτική παράδοση προσανατολισμένη

στις ανάγκες της αγοράς,
- διασφαλίζει προσβασιμότητα και συμπερίληψη σε γλωσσικό, κοινωνικό και φυσικό επίπεδο,
- και παράγει επαληθεύσιμα τεκμήρια συμμετοχής, αξιολόγησης και πιστοποίησης, σύμφωνα με τις απαιτήσεις της ευρωπαϊκής χρηματοδότησης.

Ιδιαίτερη έμφαση δίνεται στην **ανάπτυξη δεξιοτήτων**, περιλαμβάνοντας πρακτικές, hands-on μαθησιακές δραστηριότητες, αξιολόγηση ικανοτήτων και δομημένες διαδρομές πιστοποίησης. Ως εκ τούτου, το Εικονικό Campus υποστηρίζει όχι μόνο την παροχή περιεχομένου, αλλά και τη μετρήσιμη απόκτηση και επαλήθευση δεξιοτήτων.

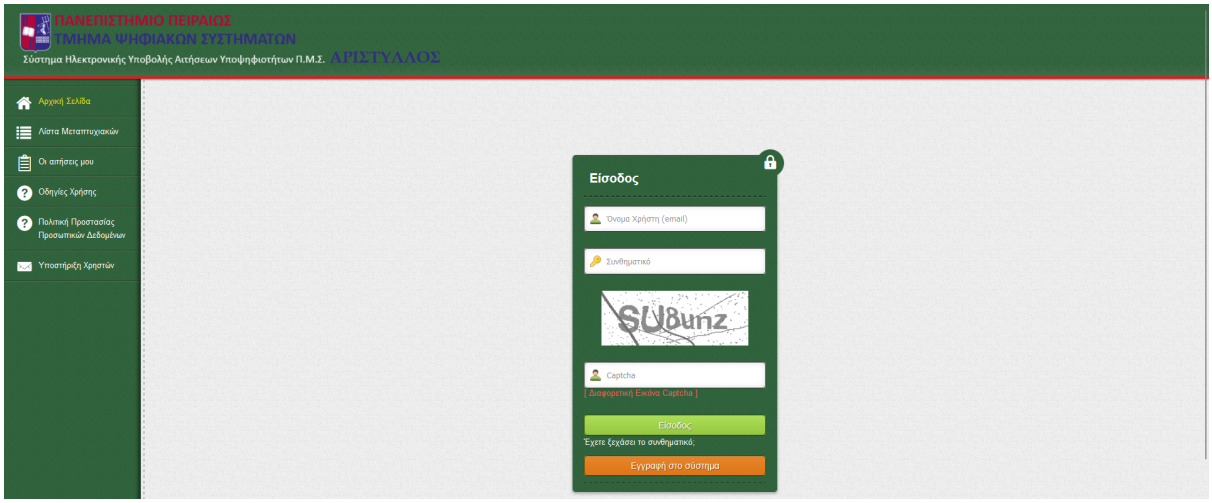
Επιπρόσθετα, υποστηρίζει διαδικασίες **επιλογής και εγγραφής** που συμμορφώνονται με αρχές **ισότητας φύλων και κοινωνικής συμπερίληψης**, καθώς και με **οδηγίες ασφάλειας, ιδιωτικότητας και προστασίας δεδομένων**.

Τέλος, ικανοποιούνται οι γενικές υποχρεώσεις για τήρηση αρχείων, τεκμηρίωση και αναφορά, γεγονός που σημαίνει ότι το Εικονικό Campus λειτουργεί ως αξιόπιστη πηγή αποδεικτικών στοιχείων για την υλοποίηση και τα αποτελέσματα της εκπαιδευτικής διαδικασίας.

Κάθε στάδιο υποστηρίζεται από συγκεκριμένη πλατφόρμα:
- το **DreamApply** για την εισαγωγή και το onboarding (Πλήρης Οδηγός Χρήσης),
- το **LearnWorlds** για την παροχή εκπαίδευσης, την αξιολόγηση και την πιστοποίηση (Learnwords),
- το **Weglot** για την πολυγλωσσική πρόσβαση,
- και το **accessiBe** για την προσβασιμότητα και τη συμπερίληψη.

3.19.1.4 Σύστημα Ηλεκτρονικής Υποβολής Αιτήσεων Π.Μ.Σ. «ΑΡΙΣΤΥΛΛΟΣ»

Το Π.Μ.Σ. παρέχει στους υποψήφιους μεταπτυχιακούς φοιτητές και φοιτήτριές του το πληροφοριακό σύστημα ηλεκτρονικής υποβολής αιτήσεων υποψηφιοτήτων «Αρίστυλλος» μέσω της διεύθυνσης https://aristyllos.ds.unipi.gr/web/.



Εικόνα 2: Αρχική ιστοσελίδα «Αρίστυλλος»

Το Σύστημα Ηλεκτρονικής Υποβολής Αιτήσεων Υποψηφιοτήτων Π.Μ.Σ. **«Αρίστυλλος»** (https://aristyllos.ds.unipi.gr/web/) δημιουργήθηκε με στόχο να παρέχει τη δυνατότητα ηλεκτρονικής υποβολής των αιτήσεων για τους υποψηφίους των Π.Μ.Σ. του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Η εγγραφή στο Π.Σ. «Αρίστυλλος» γίνεται από την αρχική σελίδα https://aristyllos.ds.unipi.gr/web/index.php. Μετά την ενεργοποίηση του λογαριασμού και την επιτυχή είσοδο στο σύστημα, υποβάλλεται αίτηση υποψηφιότητας στο Π.Μ.Σ..

3.19.1.5 Σύστημα Φοιτητολογίου & Ακαδημαϊκής Αξιολόγησης Π.Μ.Σ. «SIS-PORTAL»

Η παρακολούθηση της ακαδημαϊκής πορείας πραγματοποιείται μέσω της Πύλης του Φοιτητολογίου (υπηρεσία ηλεκτρονικής γραμματείας) στη διεύθυνση https://sis-portal.unipi.gr/.

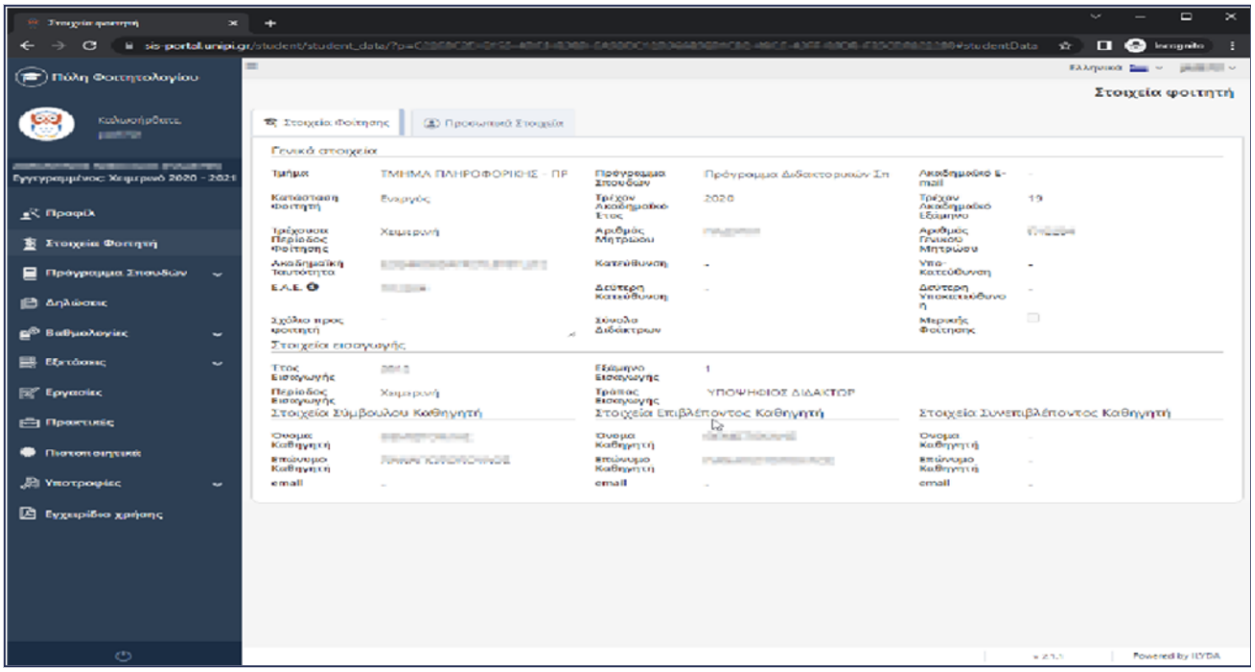
Από την εφαρμογή αυτή οι φοιτητές και φοιτήτριες έχουν τη δυνατότητα:

- να ενημερώνονται για τα μαθήματα του προγράμματος σπουδών,
- τους διδάσκοντες, τα προτεινόμενα συγγράμματα
- καθώς και τις ανακοινώσεις που εκδίδει η Γραμματεία και οι διδάσκοντες και διδάσκουσες
- να ενημερώνονται για τη βαθμολογία στα μαθήματα που έχουν εξεταστεί
- να λαμβάνουν άμεσα και σε ηλεκτρονική μορφή βεβαιώσεις φοίτησης
- να υποβάλουν αιτήσεις για χορήγηση ειδικών βεβαιώσεων ή πιστοποιητικών

Η πρόσβαση στην εφαρμογή αυτή γίνεται μέσω του προσωπικού λογαριασμού κάθε φοιτητή ή φοιτήτριας.

Μέσω της Πύλης του Φοιτητολογίου πραγματοποιείται αξιολόγηση κάθε μαθήματος, κάθε

διδάσκοντος και διδάσκουσας καθώς και των υποδομών του Π.Μ.Σ. με εμπιστευτική συμπλήρωση ερωτηματολογίων αξιολόγησης.



Εικόνα 3: Αρχική ιστοσελίδα υπηρεσίας ηλεκτρονικής γραμματείας (https://sis-portal.unipi.gr)

3.19.1.6 Σύστημα σύγχρονης διδασκαλίας (Microsoft Teams)

Για τη διεξαγωγή σύγχρονης διδασκαλίας (https://www.unipi.gr/unipi/el/hu-hlektronikh-eks-apostasews-ekpaideush.html), το Πανεπιστήμιο Πειραιώς έχει εγκαταστήσει την πλατφόρμα Microsoft Teams, η οποία είναι η κεντρικά υποστηριζόμενη λύση. Η πλατφόρμα Microsoft Teams μπορεί να υποστηρίξει σύγχρονη διδασκαλία σε κοινό έως και 250 ατόμων σε πραγματικό χρόνο, μέσω της λειτουργίας Microsoft Teams Meetings. Επίσης, το Πανεπιστήμιο διαθέτει περιορισμένο αριθμό κοινόχρηστων αδειών για το υποσύστημα Microsoft Live Events, μέσω του οποίου υποστηρίζεται μετάδοση μαθήματος σε μεγάλο κοινό σε σχεδόν πραγματικό χρόνο.

Για την έγκαιρη προετοιμασία και συμμετοχή διδασκόντων και διδασκουσών και μεταπτυχιακών φοιτητών και φοιτητριών στην εξ αποστάσεως σύγχρονη διδασκαλία, απαιτείται εγγραφή στην υπηρεσία ΔΗΛΟΣ365 (https://delos365.grnet.gr) (Ενότητα 3.19.4.2) με τον ιδρυματικό τους λογαριασμό (Ενότητα 3.19.3).

3.19.1.7 Πανεπιστημιακά Εργαστήρια

Το Π.Μ.Σ. αξιοποιεί το εργαστήριο της «Ασφάλειας Συστημάτων» το οποίο παρέχεται και υποστηρίζεται από το ίδρυμα και το Τμήμα Ψηφιακών Συστημάτων και βρίσκεται σε κτίριο

του Πανεπιστημίου στη διεύθυνση οδός Ανδρούτσου 150, στον Πειραιά.

3.19.1.8 Απόφοιτοι Π.Μ.Σ.: Ηλεκτρονική Εγγραφή στο Club Alumni

Στο πλαίσιο διατήρησης της σχέσης του Π.Μ.Σ. με τους/τις αποφοίτους του, καθώς και διερεύνησης της συμβολής των μεταπτυχιακών σπουδών στη μετέπειτα σταδιοδρομία των αποφοίτων, το Π.Μ.Σ. παροτρύνει την ηλεκτρονική εγγραφή τους στο Club Alumni (https://docs.google.com/forms/d/e/1FAIpQLScTD7N7rEUjDZsDnF7rZJHyklo9gpRX-xfymu9Y6aTS9Wbiog/viewform).

3.19.2 Ηλεκτρονικές Υπηρεσίες Ακαδημαϊκής Μονάδας

Στο Πανεπιστήμιο λειτουργούν, μεταξύ άλλων, συστήματα ασύγχρονης και σύγχρονης τηλεκπαίδευσης, υπηρεσία διανομής ακαδημαϊκού λογισμικού, υπηρεσία αιτήσεων σίτισης και στέγασης, υπηρεσία τεχνικής υποστήριξης κ.λπ. Επίσης, στους μεταπτυχιακούς φοιτητές και φοιτήτριες είναι διαθέσιμες και υπηρεσίες εξωτερικών φορέων.

3.19.2.1 Ιστοσελίδα Πανεπιστημίου Πειραιώς

Όλες οι ανακοινώσεις των υπηρεσιών του Πανεπιστημίου αναρτώνται στην κεντρική ιστοσελίδα του Πανεπιστημίου https://www.unipi.gr, ενώ πρόσθετες πληροφορίες αναρτώνται και στην ιστοσελίδα του Τμήματος και του Π.Μ.Σ.. Όλες οι πληροφορίες για τις ηλεκτρονικές υπηρεσίες οι οποίες είναι διαθέσιμες προς τη φοιτητική κοινότητα βρίσκονται αναρτημένες στην ενότητα Υπηρεσίες-Παροχές -> Ηλεκτρονικές Υπηρεσίες (https://www.unipi.gr/genikes-plhrofories/).

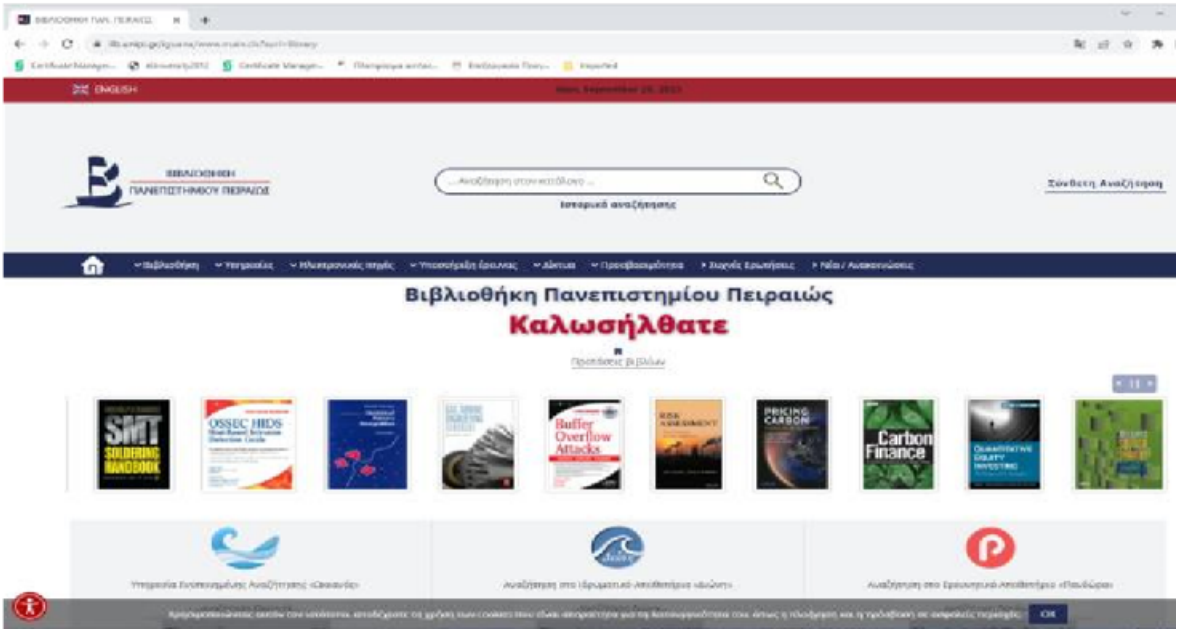
3.19.2.2 Σίτιση μεταπτυχιακών φοιτητών και φοιτητριών

Οι μεταπτυχιακοί φοιτητές και φοιτήτριες που δικαιούνται δωρεάν σίτιση μέσω του τμήματος Φοιτητικής Μέριμνας, μπορούν να υποβάλουν αίτηση για σίτιση στην ηλεκτρονική πλατφόρμα του Πανεπιστημίου https://merimna.unipi.gr/, όπου ο ενδιαφερόμενος μπορεί να καταχωρίσει την αίτησή του και να επισυνάψει τα προβλεπόμενα δικαιολογητικά, μετά την ενεργοποίηση του ιδρυματικού του λογαριασμού. Από την ίδια πλατφόρμα, οι μεταπτυχιακοί φοιτητές και φοιτήτριες που πληρούν τα αναγκαία κριτήρια μπορούν να υποβάλουν αίτηση για στέγαση σε φοιτητική εστία. Οι οδηγίες αναρτώνται στη σελίδα του τμήματος Φοιτητικής Μέριμνας (https://www.unipi.gr/unipi/el/ppf-foithtikh-merimna.html). Το Φοιτητικό Εστιατόριο λειτουργεί, όπως προαναφέρθηκε, στο κτίριο επί της οδού Τσαμαδού 78.

Εικόνα 4: Αρχική ιστοσελίδα Εφαρμογής Φοιτητικής Μέριμνας (https://merimna.unipi.gr/)

3.19.2.3 Βιβλιοθήκη Πανεπιστήμιου Πειραιώς

Η Βιβλιοθήκη (ώρες λειτουργίας: 8.00 - 20.00) του Πανεπιστημίου Πειραιώς προσφέρει ευρύ φάσμα υπηρεσιών μέσω της κεντρικής της ιστοσελίδας https://www.lib.unipi.gr/.



Εικόνα 5: Αρχική ιστοσελίδα βιβλιοθήκης Πανεπιστημίου Πειραιώς (https://www.lib.unipi.gr)

Στον ηλεκτρονικό κατάλογο της βιβλιοθήκης υπάρχουν βιβλία, λεξικά, περιοδικά, ειδικές εκδόσεις για τα μαθήματα, για τις εργασίες των μεταπτυχιακών φοιτητών και φοιτητριών,

καθώς και βιβλία για την κάλυψη προσωπικών αναγκών πληροφόρησης και ψυχαγωγίας. Τα ηλεκτρονικά αποθετήρια Διώνη και Πανδώρα, διαθέτουν μεταπτυχιακές/διδακτορικές εργασίες των αποφοίτων ή άρθρα των καθηγητών και ερευνητών του Πανεπιστημίου. Οι μεταπτυχιακοί φοιτητές και φοιτήτριες μπορούν με την ακαδημαϊκή τους ταυτότητα να δανείζονται βιβλία είτε από τη βιβλιοθήκη του Πανεπιστημίου Πειραιώς είτε από συνεργαζόμενες βιβλιοθήκες. Μπορούν να έχουν πρόσβαση π.χ. μέσω του HEAL-link σε αμέτρητα, πλήρη κείμενα ηλεκτρονικών περιοδικών, ηλεκτρονικών διδακτικών εγχειριδίων (ΚΑΛΛΙΠΟΣ), βιβλιογραφικών βάσεων δεδομένων και ηλεκτρονικών βιβλίων.

Σε όλες τις υπηρεσίες και πηγές πληροφόρησης προσφέρεται απομακρυσμένη πρόσβαση στα μέλη του Πανεπιστημίου Πειραιώς, μέσω VPN (οδηγίες για την υπηρεσία VPN υπάρχουν διαθέσιμες στη σελίδα https://www.unipi.gr/unipi/el/hu-sundesh-vpn.html).

Στη διάθεση των μεταπτυχιακών φοιτητών και φοιτητριών ή υποψηφίων διδακτόρων, υπάρχει ο Οδηγός απόθεσης τεκμηρίου για αυτές και αυτούς που υποβάλλουν ηλεκτρονικά τη Μεταπτυχιακή Διπλωματική εργασία ή τη διδακτορική διατριβή.

3.19.2.4 Υγειονομική περίθαλψη

Οι προπτυχιακοί και μεταπτυχιακοί φοιτητές και φοιτήτριες, καθώς και οι υποψήφιοι διδάκτορες που δεν έχουν άλλη ιατροφαρμακευτική και νοσοκομειακή περίθαλψη, δικαιούνται πλήρους ιατροφαρμακευτικής και νοσοκομειακής περίθαλψης στο Εθνικό Σύστημα Υγείας (Ε.Σ.Υ.), με κάλυψη των σχετικών δαπανών από τον Ε.Ο.Π.Υ.Υ. Περισσότερες πληροφορίες είναι διαθέσιμες στη σελίδα https://www.unipi.gr/ygeionomiki-perithalpsi/.

3.19.2.5 Ευρωπαϊκή Κάρτα Ασφάλισης Ασθένειας (Ε.Κ.Α.Α.)

Το Πανεπιστήμιο Πειραιώς παρέχει τη δυνατότητα έκδοσης της Ευρωπαϊκής Κάρτας Ασφάλισης Ασθένειας (Ε.Κ.Α.Α.) για τους μεταπτυχιακούς φοιτητές και φοιτήτριες του Π.Μ.Σ., οι οποίοι και οι οποίες μετακινούνται σε χώρες της Ευρωπαϊκής Ένωσης και δεν έχουν άλλη ιατροφαρμακευτική και νοσοκομειακή περίθαλψη.

3.19.2.6 Ιατρείο

Από το Ιατρείο παρέχονται υπηρεσίες πρωτοβάθμιας υγείας. Λειτουργεί καθημερινά στο Ισόγειο του κεντρικού κτιρίου, ΓΡ.003. Τον πληθυσμό του Πανεπιστημίου εξυπηρετούν:

- Η Ασημίνα Γανωτοπούλου, Ειδικός Παθολόγος - Διαβητολόγος, η οποία παρίσταται Δευτέρα, Τρίτη, Πέμπτη, Παρασκευή 9.30-11.30 και Πέμπτη 16.30-18.30
- Ο Νικόλαος Δέγλερης, Νευρολόγος - Ψυχίατρος, ο οποίος παρίσταται Δευτέρα, Τρίτη 9.00-11.00 και 18.30μ.μ.-20.30μ.μ. και Πέμπτη, Παρασκευή 9.00-13.00. Ο . Δέγλερης παρέχει τηλεσυμβουλευτική - τηλεψυχοθεραπεία μέσω skype κάθε Τετάρτη κατόπιν

ραντεβού (email: deglerispsy@yahoo.gr)

3.19.2.7 Συμβουλευτικό Κέντρο

Το Συμβουλευτικό Κέντρο λειτουργεί ως χώρος Συνάντησης, Υποστήριξης, Επικοινωνίας και Παρέμβασης. Τα στελέχη του Συμβουλευτικού Κέντρου, αναγνωρίζοντας την ιδιαιτερότητα των δυσκολιών που μπορεί να αντιμετωπίσουν οι μεταπτυχιακοί φοιτητές και φοιτήτριες, διαπραγματεύονται θέματα σημαντικά για όλες και όλους και αφορούν σε:

- Επιτυχή προσαρμογή σε νέες ανάγκες και απαιτήσεις
- Κοινωνική επιδεξιότητα, σχέσεις και οικογένεια
- Αντιμετώπιση αγχογόνων καταστάσεων
- Πρόληψη και υγεία
- Τρόποι δημιουργικής έκφρασης και ψυχαγωγίας
- Ανάπτυξη δεξιοτήτων απαραίτητων για επιτυχημένη πορεία
- Ενεργητική μάθηση.

Η παρέμβαση και η αντιμετώπιση των αναγκών που προκύπτουν, γίνεται είτε μέσω της ατομικής και ομαδικής ψυχολογικής συμβουλευτικής, είτε μέσω της διεξαγωγής σεμιναρίων εστιάζοντας στην προαγωγή της ακαδημαϊκής προσαρμογής του φοιτητικού πληθυσμού.

Κύριοι Στόχοι του Συμβουλευτικού Κέντρου είναι:

- Η ολόπλευρη ανάπτυξη του ατόμου
- Η βελτίωση της ποιότητας ζωής μέσα και έξω από το χώρο του Πανεπιστημίου
- Η σύνδεση του Πανεπιστημίου με την ευρύτερη κοινότητα, σε επίπεδο ψυχοκοινωνικής και πολιτισμικής παρέμβασης.

Το Συμβουλευτικό Κέντρο, λειτουργεί καθημερινά 7.30-15.00 στο γραφείο 013 (ισόγειο κεντρικού κτηρίου). Τηλ. 210-4142042 Υπεύθυνη Κοινωνική Λειτουργός: Μάρθα Κατσούλη.

3.19.2.8 Εθελοντική ομάδα Πανεπιστήμιου Πειραιώς - Kerykes

Στο Πανεπιστήμιό μας δραστηριοποιείται η εθελοντική ομάδα Kerykes, η οποία συμμετέχει τόσο σε δράσεις του Πανεπιστημίου όσο και σε δράσεις με άξονες τον άνθρωπο, την κοινωνία και το περιβάλλον.

3.19.2.9 Πολιτιστικές δραστηριότητες στο Πανεπιστήμιο Πειραιώς

Στο Πανεπιστήμιο λειτουργούν πολιτιστικές ομάδες :

- Θεάτρου
- Χορού (Παραδοσιακοί χοροί, Ελεύθερη γυμναστική με μουσική)
- Κινηματογράφου

- Μουσικής.

3.19.2.10 Αθλητικές δραστηριότητες στο Πανεπιστήμιο Πειραιώς

Στο Πανεπιστήμιο προσφέρεται ένα σύνολο από διαφορετικές αθλητικές δραστηριότητες, έτσι ώστε κάθε μεταπτυχιακός φοιτητής ή φοιτήτρια να μπορεί να αθληθεί, ανάλογα με το ενδιαφέρον και το αθλητικό του επίπεδο. Οι μεταπτυχιακοί φοιτητές και φοιτήτριες μπορούν να λάβουν μέρος στα αθλήματα:

- Μπάσκετ
- Βόλεϊ
- Ποδόσφαιρο
- Πόλο
- Τένις
- Σκάκι.

Για την ομάδα εθελοντισμού, τις πολιτιστικές ή τις αθλητικές ομάδες του Πανεπιστημίου, χρειάζεται η συμπλήρωση της αντίστοιχης αίτησης που βρίσκεται στον σύνδεσμο που ακολουθεί:
https://docs.google.com/forms/d/e/1FAIpQLSegplY_IKhDzDbp7nMlzCg5o-CryciVsGYVJ1jluLufZM2j9Q/viewform?usp=sharing

3.19.2.11 Ψηφιακός πίνακας ανακοινώσεων

Στο Πανεπιστήμιο Πειραιώς λειτουργεί σύστημα οθονών αναρτημένων σε κεντρικά σημεία του Πανεπιστημίου, μέσω του οποίου οι μεταπτυχιακοί φοιτητές και φοιτήτριες ενημερώνονται για τα μαθήματα που γίνονται εντός της ημέρας και την αίθουσα στην οποία πραγματοποιούνται οι διαλέξεις.

3.19.2.12 Κέντρο Υποστήριξης Διδασκαλίας και Μάθησης (ΚΕΔΙΜΑ)

Το Κέντρο Υποστήριξης Διδασκαλίας και Μάθησης (ΚΕΔΙΜΑ) του Πανεπιστημίου Πειραιώς αποσκοπεί στη διασφάλιση συνεχούς υποστήριξης της διδακτικής και μαθησιακής διαδικασίας, όπως επίσης στην ενημέρωση και υποστήριξη του συνόλου του διδακτικού προσωπικού σε καινοτόμες πρακτικές σχετικά με την εκπαίδευση. Η υποστήριξη του συνόλου του διδακτικού προσωπικού βασίζεται στην ανταλλαγή τεχνογνωσίας σε σχέση με τις σύγχρονες εκπαιδευτικές τάσεις και προσεγγίσεις.

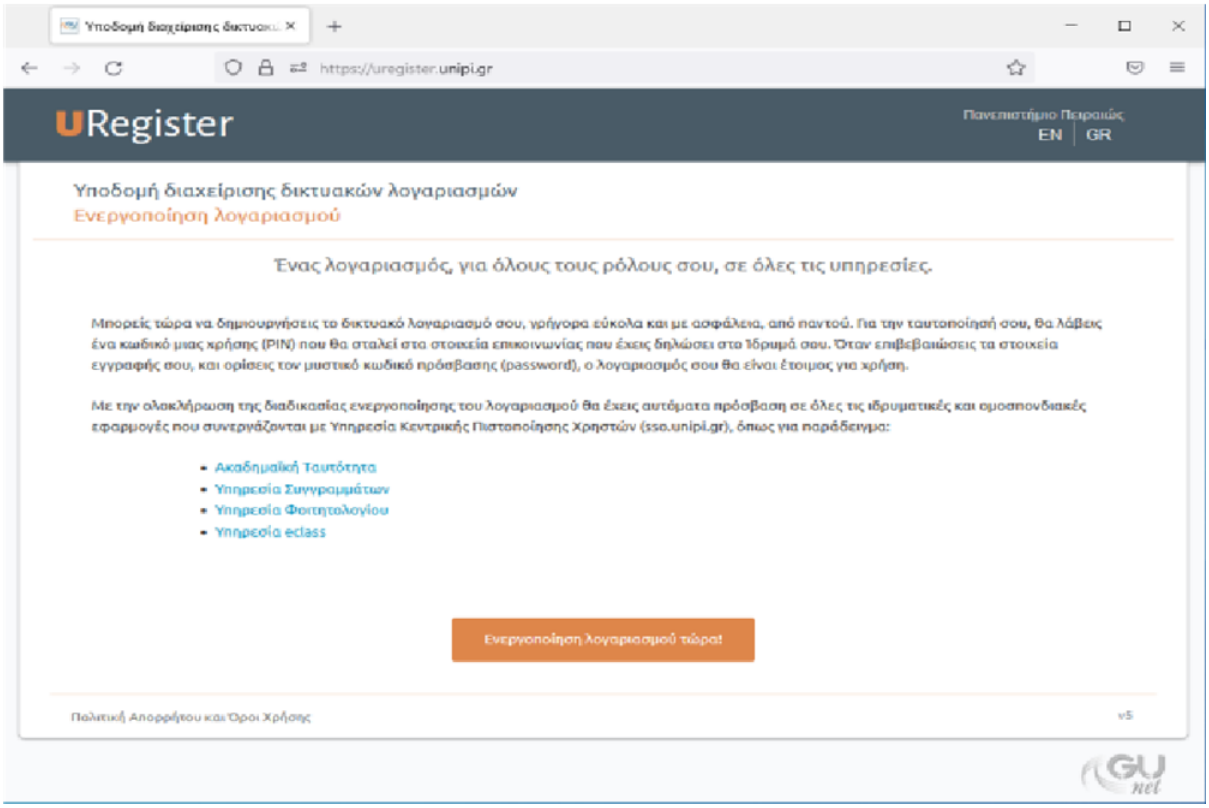
Σκοπός του ΚΕΔΙΜΑ είναι η άμεση, αποτελεσματική και ολοκληρωμένη υποστήριξη του διδακτικού έργου του ακαδημαϊκού προσωπικού του Ιδρύματος, καθώς και η προαγωγή της συνολικής εκπαιδευτικής εμπειρίας των μεταπτυχιακών φοιτητών και φοιτητριών με γνώμονα τη δημιουργία του κατάλληλου περιβάλλοντος μάθησης για τη βελτίωση της

ποιότητας της διδασκαλίας και της μάθησης.

3.19.3 Οδηγός ενεργοποίησης ηλεκτρονικών υπηρεσιών Π.Μ.Σ. και Ακαδημαϊκής Μονάδας

3.19.3.1 Δημιουργία και διαχείριση ιδρυματικού λογαριασμού

Για να γίνει χρήση των ηλεκτρονικών υπηρεσιών του Πανεπιστημίου, ως πρώτο βήμα, είναι αναγκαίο να δημιουργηθεί ο ιδρυματικός λογαριασμός. Μόλις ολοκληρωθεί η εισαγωγή και ο έλεγχος των στοιχείων στο Πληροφοριακό Σύστημα της Γραμματείας και οριστικοποιηθεί η εγγραφή, με την επίσκεψη της υπηρεσίας https://uregister.unipi.gr, όπου, με τη χρήση του κινητού τηλεφώνου ή του email που δηλώθηκε κατά την εγγραφή, θα δημιουργηθεί ο ιδρυματικός λογαριασμός.

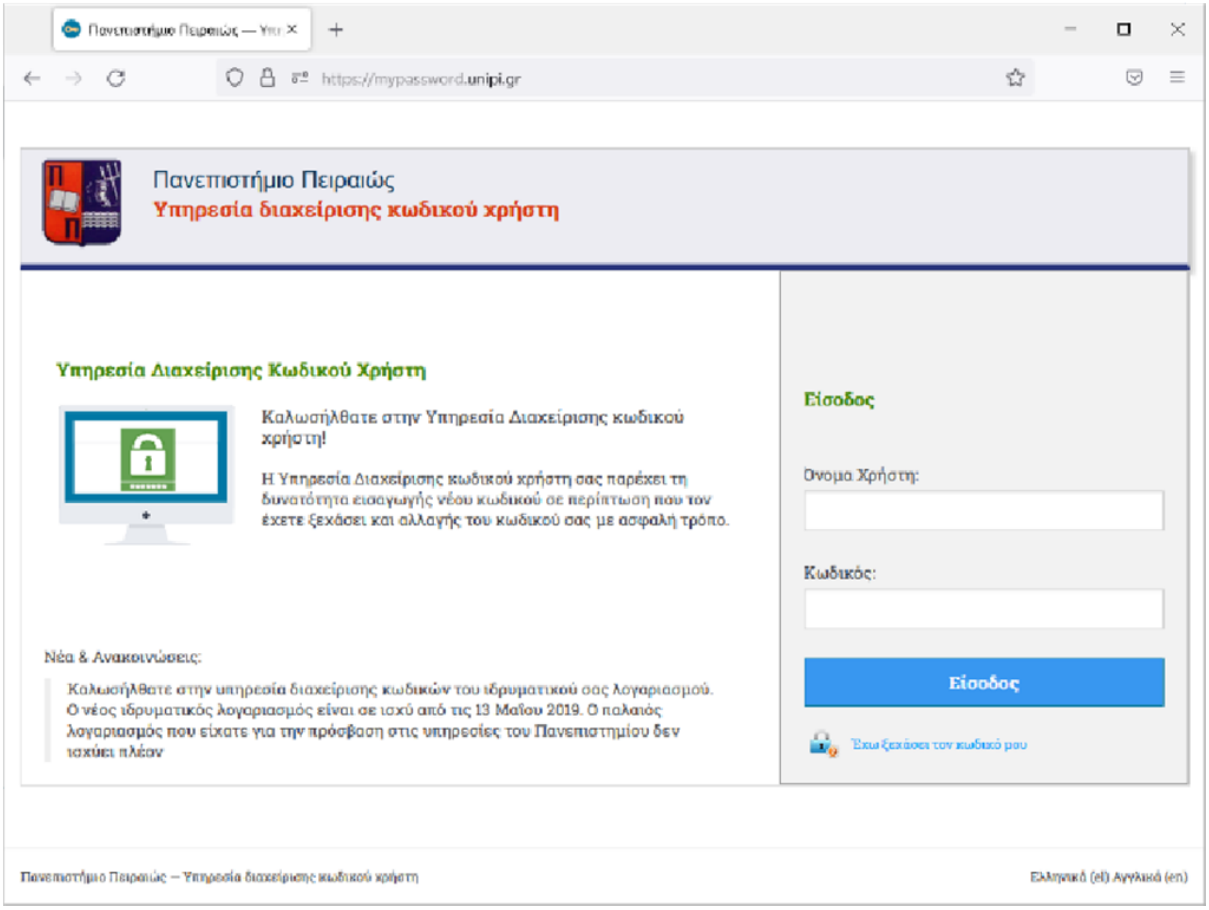


Εικόνα 6: Αρχική ιστοσελίδα υπηρεσίας uregister (https://uregister.unipi.gr)

Κατά τη διαδικασία του uregister δηλώνεται αριθμός κινητού τηλεφώνου και ηλεκτρονικής διεύθυνσης για την αλλαγή του κωδικού σε περίπτωση απώλειας. Επίσης, το uregister επιβεβαιώνει ορισμένα στοιχεία (όπως πχ email, κινητό, ονοματεπώνυμο, πατρώνυμο και Α.Μ.Κ.Α.), οπότε, εάν υπάρχει κάποιο λάθος στα στοιχεία που έχουν καταχωριστεί στο σύστημα του Υπουργείου Παιδείας θα προκύψει πρόβλημα κατά τη δημιουργία του λογαριασμού και θα χρειαστεί διόρθωση των στοιχείων μέσω της Γραμματείας. Περισσότερες πληροφορίες είναι διαθέσιμες στη σελίδα: https://www.unipi.gr/unipi/el/hu-uregister.html-uregister.html

3.19.3.2 Υπηρεσία mypassword

Συμπληρωματική της υπηρεσίας uregister είναι η υπηρεσία mypassword https://mypassword.unipi.gr, από όπου μπορεί να αλλάξει ο κωδικός πρόσβασης στο λογαριασμό μέσω του email ή του κινητού ανάκτησης που δηλώθηκε κατά τη δημιουργία του ιδρυματικού λογαριασμού μέσω του uregister, καθώς και αλλαγή του email ή το κινητού που βρίσκονται καταχωρισμένα στην υπηρεσία mypassword.unipi.gr. Περισσότερες πληροφορίες είναι διαθέσιμες στη σελίδα https://www.unipi.gr/unipi/el/hu-mypassword.html



Εικόνα 7: Αρχική ιστοσελίδα υπηρεσίας mypassword (https://mypassword.unipi.gr)

3.19.4 Ηλεκτρονικές Υπηρεσίες Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού

Λίγες ώρες αφού δημιουργηθεί ο ιδρυματικός λογαριασμός, ώστε να ολοκληρωθεί η αυτοματοποιημένη ενημέρωση ενδιάμεσων υποσυστημάτων, παρέχεται η δυνατότητα εγγραφής στα ακόλουθα πρόσθετα συστήματα:

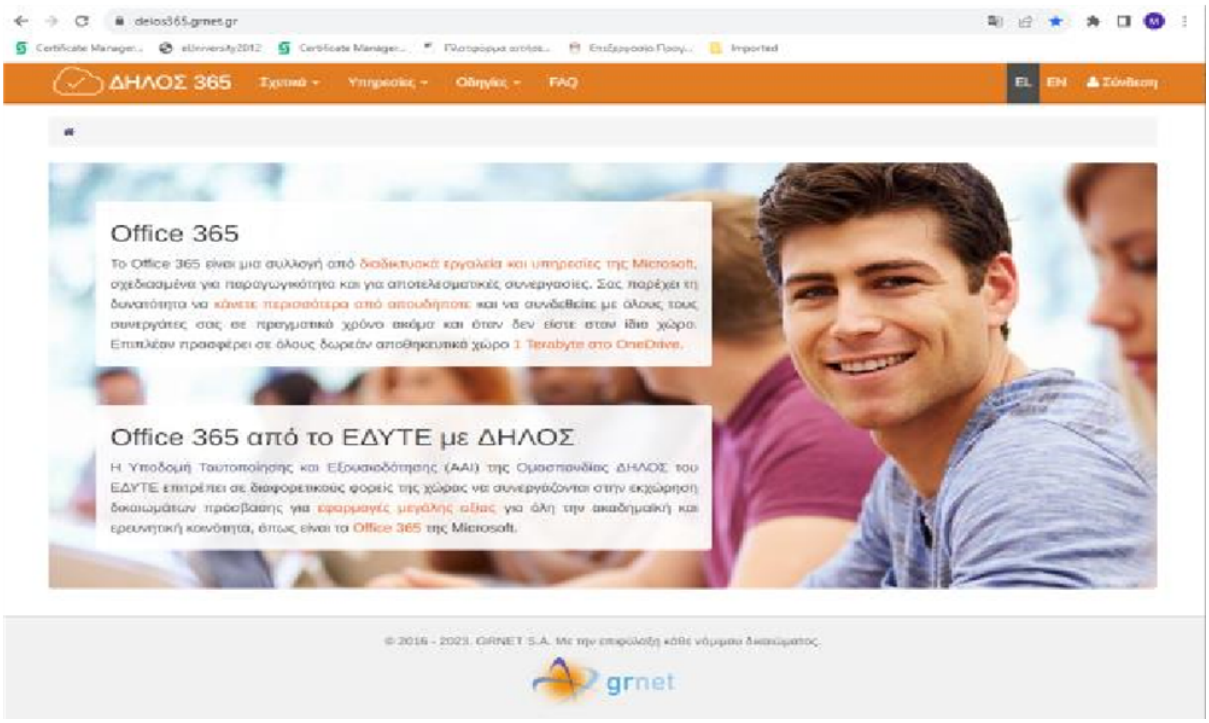
3.19.4.1 Υπηρεσία Ηλεκτρονικής Ακαδημαϊκής Ταυτότητας

Εικόνα 8: Αρχική ιστοσελίδα υπηρεσίας academicid (https://academicid.minedu.gov.gr)

Μετά τη δημιουργία του ιδρυματικού λογαριασμού, υπάρχει η δυνατότητα εγγραφής στην υπηρεσία της Ηλεκτρονικής Ακαδημαϊκής Ταυτότητας https://academicid.minedu.gov.gr η οποία έχει και ρόλο Δελτίου Φοιτητικού Εισιτηρίου (πάσο) και χρησιμοποιείται για την ταυτοποίηση στις εκπαιδευτικές διαδικασίες του Πανεπιστημίου (π.χ. εξετάσεις).

Σημειώνεται ότι η υπηρεσία ηλεκτρονικής ακαδημαϊκής ταυτότητας παρέχεται απευθείας από το Υπουργείο Παιδείας, Θρησκευμάτων και Αθλητισμού.

3.19.4.2 Πλατφόρμα ΔΗΛΟΣ365



Εικόνα 9: Αρχική ιστοσελίδα πλατφόρμας ΔΗΛΟΣ365 (https://delos365.grnet.gr)

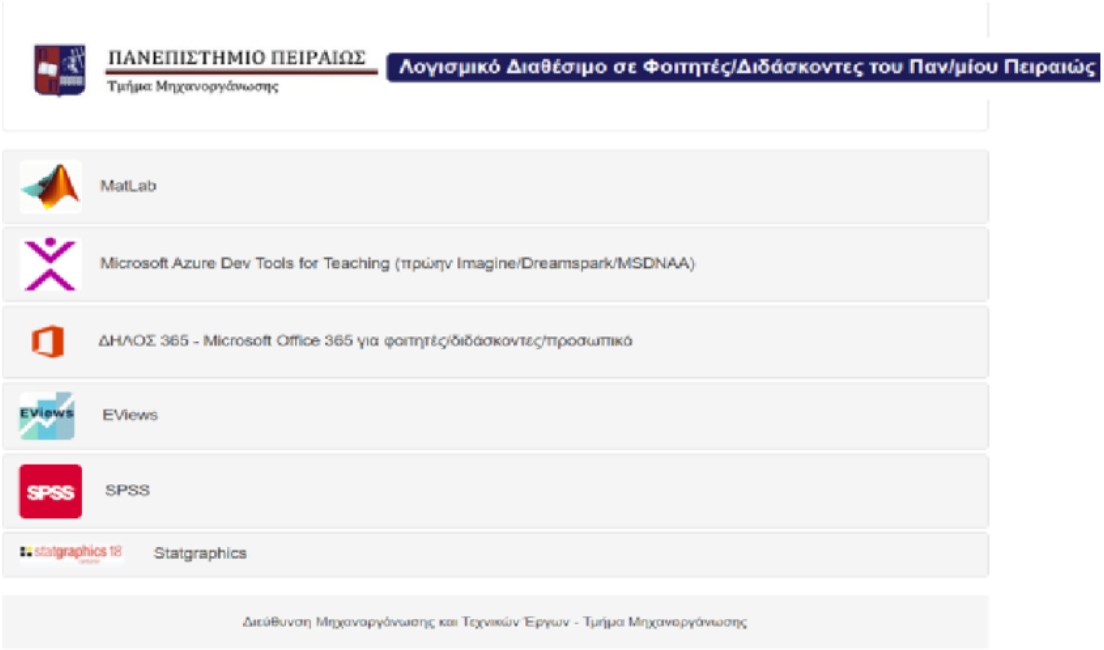
Με την εγγραφή στην πλατφόρμα https://delos365.grnet.gr αποκτάται πρόσβαση στο λογισμικό Office365 και την εφαρμογή Microsoft Teams. Για την εγγραφή αρκεί η επίσκεψη στη σελίδα και η είσοδος με τον ιδρυματικό λογαριασμό που δημιουργήθηκε. Η δημιουργία του λογαριασμού στο Office 365 και το Microsoft Teams γίνεται απευθείας σε διαδικτυακές υποδομές της εταιρείας Microsoft και ενδεχομένως να απαιτήσει χρόνο έως και μίας ημέρας για την πλήρη ενεργοποίηση όλων των υπηρεσιών.

Περισσότερες πληροφορίες είναι διαθέσιμες στη σελίδα https://helpdesk.unipi.gr/software/

3.19.5 Υποστηρικτικές Υπηρεσίες μεταπτυχιακών φοιτητών και φοιτητριών του Πανεπιστήμιου Πειραιώς

Εκτός από την εκπαιδευτική διαδικασία, ο ιδρυματικός λογαριασμός χρησιμοποιείται επίσης και στις ακόλουθες υποστηρικτικές υπηρεσίες:

3.19.5.1 Ιστοσελίδα διανομής λογισμικού



Εικόνα 10: Ιστοσελίδα διανομής λογισμικού (https://helpdesk.unipi.gr/software)

Δωρεάν εμπορικό λογισμικό για εκπαιδευτική χρήση είναι διαθέσιμο μέσω της σελίδας https://helpdesk.unipi.gr/software, όπου περιλαμβάνονται οδηγίες για κάθε διατιθέμενο λογισμικό. Σημειώνεται ότι η διαθεσιμότητα του λογισμικού εξαρτάται από το Τμήμα φοίτησης.

3.19.5.2 Υπηρεσίες ασύρματου δικτύου και εικονικά τοπικά δίκτυα (VPN)

Για ορισμένες υπηρεσίες ή τη χρήση λογισμικού απαιτείται σύνδεση στο δίκτυο του Πανεπιστημίου Πειραιώς. Αυτό είναι δυνατό και εξ αποστάσεως, από προσωπικό υπολογιστή, με χρήση της Υπηρεσίας εικονικού τοπικού δικτύου VPN που παρέχεται από το Κέντρο Δικτύων του Πανεπιστημίου, ακολουθώντας τις οδηγίες που υπάρχουν στη σελίδα https://www.unipi.gr/sundesh-sto-vpn/

Είναι διαθέσιμη πρόσβαση στο πανευρωπαϊκό ασύρματο δίκτυο Eduroam, το οποίο λειτουργεί σε μεγάλο αριθμό ακαδημαϊκών και ερευνητικών ιδρυμάτων στην Ελλάδα και την Ευρώπη (https://www.unipi.gr/wifi-kai-eduroam/).

3.19.6 Υποστηρικτικές Υπηρεσίες μεταπτυχιακών φοιτητών και φοιτητριών από εξωτερικούς φορείς

Επιπλέον των υπηρεσιών του Πανεπιστημίου Πειραιώς, με τον ιδρυματικό λογαριασμό αποκτάται πρόσβαση σε υπηρεσίες που παρέχονται από εξωτερικούς φορείς και οι οποίες μπορεί να χρειαστούν κατά τη διάρκεια των σπουδών, όπως οι ακόλουθες:

- Λοιπές υπηρεσίες Εθνικού Δικτύου Υποδομών Τεχνολογίας & Έρευνας:

https://www.unipi.gr/unipi/el/hu-edet.html και https:/grnet.gr/education/

3.20 Υποχρεώσεις και δικαιώματα μεταπτυχιακών φοιτητών και φοιτητριών

1. Οι μεταπτυχιακοί φοιτητές και φοιτήτριες έχουν όλα τα δικαιώματα και τις παροχές που προβλέπονται για τους φοιτητές του πρώτου κύκλου σπουδών, πλην του δικαιώματος παροχής δωρεάν διδακτικών συγγραμμάτων. Το Πανεπιστήμιο μεριμνά για τη διασφάλιση ισότιμης πρόσβασης στους χώρους του ιδρύματος στους μεταπτυχιακούς φοιτητές και φοιτήτριες με αναπηρία ή με ειδικές εκπαιδευτικές ανάγκες, καθώς και την προσβασιμότητα των υποδομών, των υπηρεσιών, φυσικών και ψηφιακών, του εξοπλισμού και του εκπαιδευτικού υλικού.
2. Οι μεταπτυχιακοί φοιτητές και φοιτήτριες καλούνται να συμμετέχουν και να παρακολουθούν τις δραστηριότητες όπως διαλέξεις, σεμινάρια ερευνητικών ομάδων, επισκέψεις εργαστηρίων, συνέδρια/ημερίδες με γνωστικό αντικείμενο συναφές με αυτό του Π.Μ.Σ., λοιπές επιστημονικές εκδηλώσεις του Π.Μ.Σ. κ.ά.
3. Οι μεταπτυχιακοί φοιτητές και φοιτήτριες συμμετέχουν στα μαθήματα πληροφοριακής παιδείας που διεξάγει η Βιβλιοθήκη του Πανεπιστημίου που αφορούν: στρατηγικές αναζήτησης πληροφοριακών πηγών και αξιολόγηση αποτελεσμάτων (εγκυρότητα, επικαιρότητα, σχετικότητα), σύνταξη βιβλιογραφίας και πρότυπα βιβλιογραφικών αναφορών, δεοντολογία της πληροφορίας (αποφυγή λογοκλοπής) και αυτοαπόθεση των Διπλωματικών εργασιών στο Ιδρυματικό Αποθετήριο ΔΙΩΝΗ.
4. Η Συνέλευση του Τμήματος, μετά από εισήγηση της Σ.Ε. και μετά την κλήση τους να εκφράσουν γνώμη στο πλαίσιο του δικαιώματος προηγούμενης ακρόασης, δύναται να αποφασίσει τη διαγραφή μεταπτυχιακών φοιτητών και φοιτητριών εάν:
   α) υπερβούν το ανώτατο όριο απουσιών
   β) έχουν αποτύχει στην εξέταση μαθήματος ή μαθημάτων και δεν έχουν ολοκληρώσει επιτυχώς το πρόγραμμα
   γ) υπερβούν τη μέγιστη χρονική διάρκεια φοίτησης στο Π.Μ.Σ., όπως ορίζεται στον Κανονισμό
   δ) έχουν παραβιάσει τις κείμενες διατάξεις όσον αφορά την αντιμετώπιση πειθαρχικών παραπτωμάτων από τα αρμόδια πειθαρχικά όργανα
   ε) αυτοδίκαια κατόπιν αιτήσεως των ίδιων των μεταπτυχιακών φοιτητών και φοιτητριών
   στ) δεν καταβάλλουν το προβλεπόμενο τέλος φοίτησης στον δέοντα χρόνο, όπως προβλέπεται.
5. Για κάθε μάθημα τίθεται ανώτατο όριο απουσιών 25%. Σε περίπτωση υπέρβασης του ορίου αυτού ο μεταπτυχιακός φοιτητής ή φοιτήτρια θεωρείται αποτυχών ή αποτυχούσα στο μάθημα αυτό. Σε περίπτωση που το ποσοστό απουσιών μεταπτυχιακού φοιτητή ή φοιτήτριας ξεπερνά το 25% ανά μάθημα για κάθε μάθημα του εξαμήνου, τίθεται θέμα διαγραφής του μεταπτυχιακού φοιτητή ή φοιτήτριας. Το εν λόγω θέμα εξετάζεται από τη Σ.Ε., η οποία γνωμοδοτεί σχετικά στη Συνέλευση του Τμήματος.
6. Για όλους τους κύκλους λειτουργίας του ΠΜΣ, στο πλαίσιο υποβολής υποψηφιότητας οι ενδιαφερόμενες/οι καταβάλουν τέλος υποβολής υποψηφιότητας ύψους διακοσίων (200)

ευρώ. Το τέλος αυτό δεν επιστρέφεται στις υποψήφιες και στους υποψήφιους, ανεξαρτήτως του αποτελέσματος της αξιολόγησης.

7. Για τους πρώτους δύο (2) κύκλους λειτουργίας του ΠΜΣ τα τέλη φοίτησης φοιτητριών και φοιτητών προερχομένων από χώρες της ΕΕ καλύπτονται καθ' ολοκληρίαν από το Ευρωπαϊκό έργο EU-iNSPIRE (EU iNnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce) που χρηματοδοτείται από το πρόγραμμα DIGITAL-2023-SKILLS-05 (Αρ. Συμβολαίου 101190054). Για φοιτητές και φοιτήτριες που προέρχονται από χώρες εκτός της ΕΕ τα τέλη φοίτησης είναι πέντε χιλιάδες (5.000) ευρώ.
8. Από τον τρίτο (3ο) κύκλο λειτουργίας του ΠΜΣ τα τέλη φοίτησης φοιτητριών και φοιτητών προερχομένων από χώρες της ΕΕ είναι πέντε χιλιάδες (5.000) ευρώ, ενώ για φοιτητές και φοιτήτριες που προέρχονται από χώρες εκτός της ΕΕ τα τέλη φοίτησης είναι επτά χιλιάδες (7.000) ευρώ.
9. Σύμφωνα με τον Κανονισμό Μεταπτυχιακών Σπουδών τα τέλη φοίτησης καταβάλλονται σε δύο ισόποσες δόσεις: η πρώτη δόση με την ανακοίνωση όσων γίνονται δεκτοί στο Π.Μ.Σ. για δέσμευση της θέσης (Σεπτέμβριος), και η δεύτερη δόση κατά την έναρξη του 2ου ακαδημαϊκού εξαμήνου.

   Στους επιλεγέντες μεταπτυχιακούς φοιτητές και επιλεγείσες μεταπτυχιακές φοιτήτριες που θα απαλλαγούν των τελών φοίτησης στο πλαίσιο της κείμενης νομοθεσίας, τα μέχρι εκείνη τη στιγμή καταβληθέντα τέλη επιστρέφονται εν όλω.
10. Εγγεγραμμένοι μεταπτυχιακοί φοιτητές και φοιτήτριες του Π.Μ.Σ., οι οποίοι δεν είναι πολίτες τρίτων χωρών, δύνανται να φοιτούν δωρεάν στο Π.Μ.Σ. εφόσον πληρούν τα οικονομικά ή κοινωνικά κριτήρια σύμφωνα με τις προβλέψεις στις κείμενες διατάξεις (άρθρο 86 του ν. 4957/2022 και των υπό στοιχεία 84560/Ζ1/27.07.2023 και 108990/Ζ1/8.9.2022 υπουργικών αποφάσεων) (Διευκρίνιση: Τρίτη χώρα είναι κάθε χώρα που είναι εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ). Οι χώρες του ΕΟΧ είναι τα 28 κράτη-μέλη της Ευρωπαϊκής Ένωσης, καθώς και η Ισλανδία, η Νορβηγία και το Λιχτενστάιν.) Προϋπόθεση για τη χορήγηση του δικαιώματος δωρεάν φοίτησης λόγω οικονομικών ή κοινωνικών κριτηρίων (άρθρο 86 του ν. 4957/2022), είναι, επιπλέον, η πλήρωση των προϋποθέσεων αριστείας κατά τον πρώτο κύκλο σπουδών (βασικό πτυχίο), δηλαδή κατ' ελάχιστον κατοχή βασικού πτυχίου με βαθμό ίσο ή ανώτερο του επτά μισή με άριστα το δέκα (7.5/10). Ο συνολικός αριθμός των μεταπτυχιακών φοιτητών και φοιτητριών που φοιτούν δωρεάν, στο πλαίσιο της ως άνω κείμενης νομοθεσίας, δε δύναται να υπερβαίνει τον αριθμό που αντιστοιχεί στο τριάντα τοις εκατό (30%) του συνόλου των εγγεγραμμένων μεταπτυχιακών φοιτητών και φοιτητριών ανά ακαδημαϊκό έτος. Η υποβολή των αιτήσεων για τη δωρεάν φοίτηση ανά Π.Μ.Σ. πραγματοποιείται μετά την ολοκλήρωση της διαδικασίας εγγραφής των μεταπτυχιακών φοιτητών και φοιτητριών στο Π.Μ.Σ.. Η εξέταση πλήρωσης των κριτηρίων περί απαλλαγής από τα τέλη φοίτησης για αιτούντες και αιτούσες πραγματοποιείται από τη Συνέλευση του Τμήματος. Η απαλλαγή αυτή παρέχεται αποκλειστικά για τη φοίτηση σε ένα (1) Π.Μ.Σ. που οργανώνεται από Α.Ε.Ι της ημεδαπής.
11. Το ακαδημαϊκό ημερολόγιο και το ωρολόγιο πρόγραμμα του Π.Μ.Σ. καταρτίζονται στο πλαίσιο του ακαδημαϊκού ημερολογίου του Πανεπιστημίου και εγκρίνονται από τη Συνέλευση με εισήγηση της Σ.Ε. Με την εγγραφή τους στο Π.Μ.Σ. οι μεταπτυχιακοί φοιτητές και φοιτήτριες παραλαμβάνουν από τη Γραμματεία το ετήσιο Ακαδημαϊκό

Ημερολόγιο του Προγράμματος, το οποίο περιλαμβάνει τις ημερομηνίες έναρξης και λήξης των διδακτικών περιόδων, τις περιόδους εξετάσεων, τις αργίες κ.λπ.

12. Κάθε υποψήφιος και υποψήφια, πριν εγγραφεί στο Π.Μ.Σ., οφείλει να λαμβάνει γνώση του Κανονισμού Λειτουργίας και να δηλώνει ενυπογράφως ότι αποδέχεται τους κανόνες λειτουργίας του Π.Μ.Σ.

3.21 Χορήγηση υποτροφιών

Σύμφωνα με τον Κανονισμό Μεταπτυχιακών Σπουδών του Π.Μ.Σ. το Π.Μ.Σ. μπορεί να παρέχει αριθμό υποτροφιών ανά ακαδημαϊκό εξάμηνο σε μεταπτυχιακούς φοιτητές και φοιτήτριες που καταβάλουν τέλη φοίτησης σύμφωνα με απόφαση της Συνέλευσης του Τμήματος, κατόπιν εισήγησης της Σ.Ε. του Π.Μ.Σ. Το ύψος κάθε υποτροφίας δεν μπορεί να υπερβαίνει το ύψος των τελών φοίτησης ενός εξαμήνου. Οι υποτροφίες παρέχονται με βάση ακαδημαϊκά κριτήρια κατά τη διάρκεια των σπουδών στο Π.Μ.Σ. με απόφαση της Συνέλευσης του Τμήματος, κατόπιν εισήγησης της Σ.Ε. του Π.Μ.Σ. και εγγράφονται στον προϋπολογισμό του Π.Μ.Σ. Τυχόν υποχρεώσεις των υποτρόφων καθορίζονται με την ίδια απόφαση της Συνέλευσης του Τμήματος κατόπιν εισήγησης της Σ.Ε. του Π.Μ.Σ. Εφόσον προκύψουν περισσότεροι του ενός δικαιούχοι υποτροφίας με τη ίδια βαθμολογία, είτε θα γίνεται κλήρωση μεταξύ τους ενώπιον της Σ.Ε. είτε θα κατανέμεται ισόποσα το ποσόν της υποτροφίας μεταξύ τους, μετά από απόφαση της Συνέλευσης του Τμήματος κατόπιν εισήγησης της Σ.Ε. του Π.Μ.Σ.

3.22 Κινητικότητα μεταπτυχιακών φοιτητών και φοιτητριών

Η τυχόν μετακίνηση των μεταπτυχιακών φοιτητών και φοιτητριών του Π.Μ.Σ. για σπουδές ή πρακτική άσκηση πραγματοποιείται σύμφωνα με τον Κανονισμό κινητικότητας (Παράρτημα 3: Κανονισμός Κινητικότητας Φοιτητών και Φοιτητριών και Προσωπικού (Πρόγραμμα ERASMUS+ και ERASMUS+ International)).

3.23 Ακαδημαϊκός Σύμβουλος Σπουδών

Για την ποιοτική αναβάθμιση της λειτουργίας του μεταπτυχιακού προγράμματος έχει θεσπιστεί και λειτουργεί ο θεσμός του Ακαδημαϊκού Συμβούλου Σπουδών, θέτοντας στο επίκεντρο τον μεταπτυχιακό φοιτητή και τη φοιτήτρια και θεωρώντας ότι θα συμβάλλει καθοριστικά στην ακαδημαϊκή και μετέπειτα επαγγελματική του πορεία.

Για περισσότερες πληροφορίες σχετικά με τον θεσμό του Ακαδημαϊκού Συμβούλου Σπουδών ανατρέξτε στο Παράρτημα 4: Κανονισμός Ακαδημαϊκού Συμβούλου Σπουδών.

3.24 Μηχανισμός διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών

Η υιοθέτηση του κανονισμού διαχείρισης αιτημάτων ή/και παραπόνων μεταπτυχιακών

φοιτητών και φοιτητριών των Π.Μ.Σ., στοχεύει στην ποιοτική αναβάθμιση της λειτουργίας των μεταπτυχιακών προγραμμάτων, θέτοντας στο επίκεντρο το σεβασμό όλων των εμπλεκομένων στην εκπαιδευτική διαδικασία, αλλά πολύ περισσότερο των αποδεκτών αυτής έναντι των οποίων οφείλει να λογοδοτεί. Στο πλαίσιο, λοιπόν, των αρχών της διαφάνειας και της λογοδοσίας και προς ενίσχυση της φοιτητο-κεντρικής εκπαιδευτικής διαδικασίας καταρτίστηκε ο Κανονισμός, στον οποίο περιγράφεται αναλυτικά η διαδικασία διαχείρισης αιτημάτων/παραπόνων καθώς και τα εμπλεκόμενα μέρη.

Για περισσότερες πληροφορίες σχετικά, ο Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών του Π.Μ.Σ. είναι διαθέσιμος στο Παράρτημα 5: Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών .

3.25 Αξιολόγηση μεταπτυχιακών φοιτητών και φοιτητριών

3.25.1 Περιγραφή συστήματος αξιολόγησης μαθησιακών αποτελεσμάτων

Η αξιολόγηση των επιδόσεων των μεταπτυχιακών φοιτητών και φοιτητριών αποτελεί αναπόσπαστο μέρος της εκπαιδευτικής διαδικασίας, συνδέει τη διδασκαλία με τη μάθηση και την αξιολόγηση της επίτευξης των μαθησιακών αποτελεσμάτων και λαμβάνει χώρα καθ' όλη τη διάρκεια του ακαδημαϊκού εξαμήνου.

Η τελική διαδικασία αξιολόγησης και βαθμολογία στα επιμέρους μαθήματα του Π.Μ.Σ. καθορίζεται από τον διδάσκοντα ή τη διδάσκουσα. Σε περίπτωση αποτυχίας ή μη προσέλευσης του φοιτητή στην εξέταση μαθήματος παρέχεται η δυνατότητα συμμετοχής σε επαναληπτική εξέταση. Κάθε μεταπτυχιακός φοιτητής δύναται να αποτύχει σε δύο (2) μαθήματα ανά ακαδημαϊκό εξάμηνο. Αποτυχία σε τρία (3) και άνω μαθήματα στο εξάμηνο οδηγεί σε διαγραφή από το πρόγραμμα μετά από απόφαση της Συνέλευσης του Τμήματος με εξαίρεση ειδικών περιπτώσεων ανωτέρας βίας (ασθένεια, φόρτος εργασίας, κ.λπ.) κατά τις οποίες δύναται να επιτρέπεται μεγαλύτερος αριθμός μαθημάτων. Οι προβλεπόμενες επανεξετάσεις των μαθημάτων πραγματοποιούνται κατόπιν σχετικών αποφάσεων. Στην περίπτωση που ο φοιτητής αποτύχει περισσότερες από δύο (2) φορές στο ίδιο μάθημα, εξετάζεται ύστερα από αίτησή του, από τριμελή επιτροπή διδασκόντων/ουσών του Π.Μ.Σ., τα μέλη της οποίας έχουν το ίδιο ή συναφές αντικείμενο με το εξεταζόμενο μάθημα και ορίζονται από την Συνέλευση. Από την επιτροπή εξαιρείται ο υπεύθυνος της εξέτασης διδάσκων.

3.25.2 Μαθησιακά Αποτελέσματα

Τα μαθησιακά αποτελέσματα είναι οι διατυπώσεις όλων αυτών που οι εκπαιδευόμενοι και οι εκπαιδευόμενες γνωρίζουν, κατανοούν και μπορούν να κάνουν μετά την ολοκλήρωση της μαθησιακής διαδικασίας.

Ουσιαστικά, μαθησιακά αποτελέσματα ενός μαθήματος είναι:

- οι γνώσεις, θεωρητικές ή/και πρακτικές που αποκτώνται
- οι δεξιότητες, η κατανόηση και αξιοποίηση της γνώσης
- οι ικανότητες, η τεκμηριωμένη επάρκεια στη χρήση των γνώσεων και δεξιοτήτων που αποκτήθηκαν,

που οι μεταπτυχιακοί φοιτητές και φοιτήτριες θα πρέπει να γνωρίζουν, να έχουν, να είναι σε θέση να επιδεικνύουν, αντίστοιχα, μετά την επιτυχή ολοκλήρωση του μαθήματος.

Στο πλαίσιο της φοιτητοκεντρικής προσέγγισης της διδασκαλίας που ακολουθείται, τα μαθησιακά αποτελέσματα είναι στο επίκεντρο της μαθησιακής διαδικασίας, η επίτευξή τους είναι μετρήσιμη, αξιολογείται και καθορίζει την επίδοση των μεταπτυχιακών φοιτητών και φοιτητριών σε κάθε εκπαιδευτική συνιστώσα. Με την έναρξη των μαθημάτων οι μεταπτυχιακοί φοιτητές και φοιτήτριες ενημερώνονται για τα προσδοκώμενα μαθησιακά αποτελέσματα του κάθε μαθήματος, για το σύστημα αξιολόγησης, καθώς και τα κριτήρια αξιολόγησης του κάθε μαθήματος από τους διδάσκοντες και τις διδάσκουσες και παροτρύνονται να πληροφορηθούν περαιτέρω λεπτομέρειες για τη διαδικασία και τον τύπο των εξετάσεων από το περίγραμμα του κάθε μαθήματος το οποίο βρίσκεται αναρτημένο στην ιστοσελίδα του Τμήματος.

3.25.3 Σύστημα Αξιολόγησης

Η διαδικασία αξιολόγησης των φοιτητών/τριών ανά εκπαιδευτική δραστηριότητα θα πραγματοποιείται με εξ αποστάσεως μεθόδους όπως:

- Τεστ (Quizzes) με ερωτήσεις σύντομης απάντησης
- Τεστ (Quizzes) με ερωτήσεις εκτεταμένης απάντησης
- Αξιολόγηση γραπτής εργασίας/αναφοράς/project (βιβλιογραφικά θέματα, αυτοτελείς μελέτες περιπτώσεων, επίλυση προβλημάτων σε υποθετικά σενάρια κ.λπ.)
- Αξιολόγηση εργαστηριακών / πρακτικών ασκήσεων
- Αξιολόγηση της συμμετοχής στη μαθησιακή διαδικασία στο πλαίσιο θεωρητικών, ή σεμιναριακών μαθημάτων και σε forums του Π.Μ.Σ.
- Συνδυασμός δύο ή περισσότερων από τις παραπάνω μεθόδους.

Ο καθορισμός του τρόπου και της διαδικασίας αξιολόγησης των φοιτητών/τριων σε ένα μάθημα, αποτελεί αποκλειστική ευθύνη του/της διδάσκοντος/ουσας, στον/ην οποίο/α από τη Συνέλευση έχει ανατεθεί η διδασκαλία του μαθήματος.

Η αξιολόγηση και η βαθμολόγηση σε κάθε μάθημα γίνεται σε πλήρη ανεξαρτησία από τα άλλα μαθήματα και αποτελεί παράγωγο της αντικειμενικής εκτίμησης της απόδοσης του φοιτητή ή της φοιτήτριας στο συγκεκριμένο μάθημα (εργασίες, εξετάσεις, κ.λπ.). Τα κριτήρια αξιολόγησης είναι σαφώς προσδιορισμένα, γνωστοποιούνται στην αρχή του ακαδ. εξαμήνου από τον /την διδάσκοντα/ουσα- υπευθύνου/συντονιστή του μαθήματος και αναγράφονται επίσης στην φόρμα περιγραφής (περίγραμμα) του κάθε μαθήματος που

είναι αναρτημένη στην ιστοσελίδα του ΠΜΣ.

Ο τελικός βαθμός κάθε μαθήματος προκύπτει από το σύνολο των επιδόσεων του φοιτητή ή της φοιτήτριας σε συγκεκριμένους τομείς (π.χ. εργασίες, εξετάσεις) σύμφωνα με τις οδηγίες που παρέχει ο διδάσκων ή η διδάσκουσα στην αρχή του εξαμήνου. Ο ελάχιστος αποδεκτός βαθμός μαθήματος είναι το πέντε (5,00), με ανώτερο το δέκα (10,00), με δυνατότητα βαθμολόγησης και της μορφής Χ.5. Κάθε μάθημα που περιλαμβάνεται στο πρόγραμμα σπουδών, καθώς και η Μεταπτυχιακή Διπλωματική Εργασία, βαθμολογείται αυτοτελώς.

Ειδικά για τις γραπτές εργασίες που εκπονούνται στο πλαίσιο κάθε μαθήματος, αυτές αποτιμώνται με κριτήρια την άρτια επιλογή βιβλιογραφικών πηγών, την επιστημονική ορθότητα της ανάλυσης της υπάρχουσας γνώσης, την εμβάθυνση στο πεδίο, το εύρος κάλυψης του θέματος, την ακρίβεια κατά την περιγραφή, τη συνεκτική δομή και εναργή αποτύπωση των επιχειρημάτων του τελικού κειμένου, τη συνολική επιστημονική ωριμότητα του πονήματος, τη συμμόρφωση της εμφάνισης και των περιεχομένων της εργασίας με τις σχετικές οδηγίες. Τα κριτήρια αξιολόγησης εξειδικεύονται και αναλύονται έτι περαιτέρω, όπου απαιτείται, στην παρουσίαση των διδασκόντων και διδασκουσών κατά την πρώτη διάλεξη του μαθήματος.

Η ανατροφοδότηση για τον βαθμό ικανοποίησης των μεταπτυχιακών φοιτητών και φοιτητριών από τα κριτήρια και τον τρόπο αξιολόγησης λαμβάνεται από τα ερωτηματολόγια αξιολόγησης των μεταπτυχιακών φοιτητών και φοιτητριών του Π.Μ.Σ..

Οι Μεταπτυχιακές Διπλωματικές Εργασίες αποτιμώνται με κριτήρια την άρτια επιλογή βιβλιογραφικών πηγών, την επιστημονική ορθότητα της ανάλυσης της υπάρχουσας γνώσης, την εμβάθυνση στο πεδίο, το εύρος κάλυψης του θέματος, την ακρίβεια κατά την περιγραφή, τη συνεκτική δομή και εναργή αποτύπωση των επιχειρημάτων, τα στοιχεία ερευνητικής συνεισφοράς και παραγωγής νέας γνώσης στο επιστημονικό πεδίο, τη συνολική επιστημονική ωριμότητα του πονήματος, τη συμμόρφωση της εμφάνισης και των περιεχομένων της εργασίας με τις σχετικές οδηγίες, καθώς και την πληρότητα και ωριμότητα κατά την προφορική παρουσίαση, τη συνέπεια στον διαθέσιμο χρόνο και την επιστημονικά ορθή ανταπόκριση του μεταπτυχιακού φοιτητή ή της φοιτήτριας σε ερωτήματα της Εξεταστικής Επιτροπής.

Τα κριτήρια βαθμολόγησης της Μ.Δ.Ε. περιλαμβάνουν:

Βαθμός [9-10]

- Επιδεικνύει εξαιρετική κατανόηση όλων των κύριων θεμάτων
- Η σχετική βιβλιογραφία έχει ερευνηθεί πλήρως και αξιολογηθεί κριτικά
- Προχωρημένη ικανότητα αξιοποίησης της θεωρίας στην προσέγγιση πρακτικών προβλημάτων (όπου είναι ενδεδειγμένο)
- Ιδιαιτέρως κατατοπιστική ερμηνεία των ευρημάτων με κριτική επίγνωση τόσο των δυνατοτήτων όσο και των περιορισμών

- Εύστοχη χρήση πινάκων και σχημάτων
- Καλά επιλεγμένες και ενημερωμένες βιβλιογραφικές αναφορές που χρησιμοποιούνται στα κατάλληλα σημεία
- Πλήρης και καλά διαμορφωμένη βιβλιογραφία
- Εξαιρετικά οργανωμένη και άρτια αναπτυγμένη διατριβή εντός του ορίου λέξεων.

Βαθμός [8-9)
- Επιδεικνύει πλήρη κατανόηση των σημαντικών θεμάτων
- Έχει ερευνηθεί και αξιολογηθεί ικανοποιητικά η σχετική βιβλιογραφία
- Ικανότητα εκλεπτυσμένης αξιοποίησης της θεωρίας στην προσέγγιση πρακτικών προβλημάτων
- Εντοπίζονται και αντιμετωπίζονται εν όλω ή μερικώς τα σημαντικά θέματα που απορρέουν από το θέμα
- Χωρίς σημαντικά πραγματολογικά ή ερμηνευτικά σφάλματα
- Άρτια και αποτελεσματική χρήση πινάκων και σχημάτων
- Καλά επιλεγμένες και ενημερωμένες αναφορές που χρησιμοποιούνται στα κατάλληλα σημεία
- Άρτια οργάνωση και λογική δομή σε ολόκληρη τη διατριβή εντός του ορίου λέξεων.

Βαθμός [7-8)
- Επιδεικνύει ικανοποιητική κατανόηση των σημαντικών θεμάτων με κάποια κενά ή ανεπάρκειες
- Η βιβλιογραφία έχει ερευνηθεί σε αποδεκτό επίπεδο, αλλά όχι πέραν αυτού
- Ικανοποιητική ικανότητα αξιοποίησης της θεωρίας στην προσέγγιση πρακτικών προβλημάτων (όπου είναι ενδεδειγμένο)
- Εντοπίζονται και αντιμετωπίζονται κάποια σημαντικά θέματα που απορρέουν από το θέμα
- Λίγα πραγματολογικά ή ερμηνευτικά σφάλματα που υποδηλώνουν παρερμηνεία της βιβλιογραφίας
- Πίνακες και σχήματα κατά βάσιν κατάλληλα
- Κατάλληλες αναφορές με ορισμένες παραλείψεις και αποδεκτή χρήση της βιβλιογραφίας
- Λογική δομή με περιστασιακές αντιφάσεις εντός του ορίων λέξεων.

Βαθμοί [5-7)
- Επιδεικνύει λιγότερο από ικανοποιητική κατανόηση των σημαντικών θεμάτων
- Ερεύνησε μερικώς τη βιβλιογραφία, αλλά άφησε σημαντικά κενά
- Περιορισμένη ικανότητα συσχέτισης της έρευνας με πρακτικά προβλήματα (όπου είναι ενδεδειγμένο)
- Δεν προσεγγίζονται αρκετά σημαντικά θέματα που απορρέουν από το θέμα
- Κάποια σοβαρά πραγματολογικά ή ερμηνευτικά σφάλματα που υποδηλώνουν

παρανοήσεις του κύριου υλικού
- Ακατάλληλη ή ατελής χρήση πινάκων και σχημάτων
- Ακατάλληλες ή ατελείς αναφορές
- Παρουσίαση, σελιδοποίηση, τίτλος, περιθώρια και παράγραφοι όχι όπως καθορίζεται στις σχετικές οδηγίες.

Βαθμοί [1-4] (μη επιτυχής)
- Επιδεικνύει αδυναμία κατανόησης των σημαντικών θεμάτων
- Έχει ερευνηθεί ανεπαρκώς η βιβλιογραφία, επισημαίνοντας κενά γνώσεων
- Πολύ περιορισμένη ικανότητα συσχέτισης της έρευνας με πρακτικά προβλήματα (όπου είναι ενδεδειγμένο)
- Ελάχιστα έως κανένα από τα σημαντικά θέματα που απορρέουν από το θέμα εντοπίζονται και παρουσιάζονται
- Σοβαρά πραγματολογικά και ερμηνευτικά σφάλματα
- Ακατάλληλη ή ατελής χρήση πινάκων και σχημάτων
- Ακατάλληλες ή ατελείς αναφορές
- Απρόσεκτη παρουσίαση, ελλιπής μέριμνα για τη σελιδοποίηση, τον τίτλο, τα περιθώρια και τις παραγράφους.

Βαθμός 0
- Δεν υποβλήθηκε εργασία

3.25.4 Προσαρμογή του συστήματος αξιολόγησης για μεταπτυχιακούς φοιτητές και φοιτήτριες με σοβαρές παθήσεις και μαθησιακές δυσκολίες

Πέρα από τα οριζόμενα παραπάνω, στους μεταπτυχιακούς φοιτητές και φοιτήτριες που προσκομίζουν στη Γραμματεία του Π.Μ.Σ. διαγνωστικές βεβαιώσεις που αποδεικνύουν προβλήματα υγείας, όπως όρασης, ακοής, κινητικά προβλήματα, δυσλεξία ή άλλες διαταραχές και καθιστούν δύσκολη τη συμμετοχή τους σε γραπτές ή προφορικές εξετάσεις, λαμβάνεται ειδική μέριμνα για τη διευκόλυνση και προσαρμογή της διαδικασίας εξέτασης σύμφωνα με το εκάστοτε νομοθετικό πλαίσιο και την υποστήριξη των διδασκόντων και διδασκουσών:
- παροχή επιπρόσθετου χρόνου εξέτασης, ανάλογα με την περίπτωση
- προφορική εξέταση για μεταπτυχιακούς φοιτητές και φοιτήτριες που αδυνατούν να γράψουν ή δυσκολεύονται να γράψουν ή χρειάζονται υποστήριξη κατά τη διάρκεια της εξέτασης ή δυσκολεύονται να συμμετάσχουν σε προφορικές εξετάσεις κατά ομάδες
- διαφοροποίηση της οπτικής παρουσίασης των ερωτήσεων με αναλογική μεγέθυνση των γραμμάτων, ανάλογα με την περίπτωση προβλήματος όρασης
- ανάγνωση των ερωτήσεων στις περιπτώσεις που αυτό απαιτείται
- χρήση μετατροπέων όταν αυτό απαιτείται

- επιπρόσθετες διευκολύνσεις για μεταπτυχιακούς φοιτητές και φοιτήτριες με κινητική αναπηρία, ανάλογα με την περίπτωση και στο πλαίσιο του εξοπλισμού και των υποδομών που διαθέτει το Πανεπιστήμιο Πειραιώς (Ενότητα 3.30.2).

3.26 Διαδικασίες και κριτήρια επιλογής διδακτικού προσωπικού

Με απόφαση της Συνέλευσης του Τμήματος ανατίθεται διδασκαλία σε μέλη ΔΕΠ του Τμήματος Ψηφιακών Συστημάτων και άλλων Τμημάτων του Πανεπιστημίου ή Τμημάτων άλλων Πανεπιστημίων της ημεδαπής ή της αλλοδαπής (κυρίως των συνεργαζόμενων ακαδημαϊκών ιδρυμάτων - βλέπε Ενότητα 3), καθώς και άλλες κατηγορίες διδασκόντων σύμφωνα με τις διατάξεις του ν. 4957/2022 (Α141') όπως ισχύει και του Κανονισμού για τα προγράμματα 2ου & 3ου Κύκλου Σπουδών του Πανεπιστημίου. Οι ειδικότερες προϋποθέσεις και η διαδικασία πρόσκλησης από την ημεδαπή ή την αλλοδαπή, καθώς και οι ειδικότεροι όροι απασχόλησης και κάθε θέμα σχετικό με τους διδάσκοντες που ανήκουν στις κατηγορίες των περιπτώσεων ε), στ) και ζ) της παρ. 1 του άρθρου 83 του Ν. 4957/2022 θα ορίζονται με απόφαση Συνέλευσης και στο πλαίσιο της κείμενης νομοθεσίας.

Με απόφαση της Συνέλευσης του Τμήματος δύναται να ανατίθεται επικουρικό διδακτικό έργο στους υποψήφιους διδάκτορες του Τμήματος ή της Σχολής, υπό την επίβλεψη διδάσκοντος ή διδάσκουσας του Π.Μ.Σ..

Η ανάθεση του διδακτικού έργου του Π.Μ.Σ. πραγματοποιείται με απόφαση της Συνέλευσης του Τμήματος, κατόπιν τεκμηριωμένης εισήγησης της Σ.Ε. του Π.Μ.Σ., άλλως του Διευθυντή του Π.Μ.Σ.. Η εισήγηση που κατατίθεται από τη Σ.Ε. του Π.Μ.Σ. λαμβάνει υπ' όψιν ως κριτήρια για την επιλογή τη συνάφεια της ειδικότητας, της εμπειρίας και του διδακτικού και ερευνητικού έργου των διδασκόντων και διδασκουσών, με το αντικείμενο του προς ανάθεση μαθήματος, καθώς και εν γένει του Π.Μ.Σ.. Εάν υπάρχουν αποτελέσματα αξιολόγησης της διδακτικής ικανότητας διδασκόντων και διδασκουσών, αυτά λαμβάνονται υπ' όψιν στην εισήγηση.

Κάθε μάθημα διδάσκεται από έναν ή περισσότερους διδάσκοντες. Σε κάθε μάθημα ορίζεται από τη Συνέλευση του Τμήματος ένας διδάσκων ή μία διδάσκουσα ως υπεύθυνος ή υπεύθυνη συντονισμού του μαθήματος. Για τον ορισμό του συντονιστή ή της συντονίστριας λαμβάνεται υπ' όψιν η εμπειρία και το έργο εκάστου διδάσκοντα και διδάσκουσας, καθώς και η διαθεσιμότητά τους να ασκήσουν τα καθήκοντα του συντονιστή.

3.27 Καθομολόγηση / ορκωμοσία

Μεταπτυχιακός φοιτητής ή φοιτήτρια που ολοκλήρωσε επιτυχώς τις μεταπτυχιακές σπουδές του, καθομολογεί / ορκίζεται σε τελετή, ενώπιον του Πρύτανη ή του Αντιπρύτανη ως εκπροσώπου του Πρύτανη, του Κοσμήτορα της Σχολής, του Προέδρου του Τμήματος και του Διευθυντή του Π.Μ.Σ. Η ορκωμοσία δεν αποτελεί συστατικό τύπο της επιτυχούς περάτωσης των σπουδών, είναι όμως αναγκαία προϋπόθεση για τη χορήγηση του

μεταπτυχιακού διπλώματος.

Για λόγους ανωτέρας βίας και με αίτησή του προς τη Γραμματεία του Τμήματος ο απόφοιτος ή η απόφοιτη μπορεί να ζητήσει τη χορήγηση του τίτλου σπουδών χωρίς να συμμετάσχει στην τελετή καθομολόγησης / ορκωμοσίας ή να ζητήσει να συμμετάσχει σε επόμενη τελετή. Πριν από την καθομολόγηση / ορκωμοσία ή την απαλλαγή τους από αυτή μπορεί να δίδεται στους αποφοίτους σχετικό πιστοποιητικό για την επιτυχή περάτωση των σπουδών τους.

Το κείμενο της καθομολόγησης / όρκου για τους απόφοιτους που αποκτούν Δ.Μ.Σ. ορίζεται με απόφαση της Συγκλήτου. Στους απόφοιτους που δεν επιθυμούν να δώσουν όρκο θρησκευτικού τύπου επιτρέπεται απλή επίκληση της τιμής και συνείδησής τους.

3.28 Υποδομή Π.Μ.Σ.

Για την εύρυθμη λειτουργία του Π.Μ.Σ. διατίθενται αίθουσες διδασκαλίας και σεμιναρίων, αμφιθέατρα εξοπλισμένα με οπτικοακουστικά μέσα και εργαστήρια του Πανεπιστημίου.

Η βασική χρηματοδότηση του Π.Μ.Σ. κατά τους δύο (2) πρώτους κύκλους λειτουργίας προέρχεται από το Ευρωπαϊκό έργο EU-iNSPIRE (EU iNnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce) το οποίο ξεκίνησε τον Ιανουάριο του 2025, έχει διάρκεια (4) τέσσερα χρόνια και χρηματοδοτείται από το πρόγραμμα DIGITAL-2023-SKILLS-05 (Αρ. Συμβολαίου 101190054). Συγκεκριμένα, τα έξοδα οργάνωσης και λειτουργίας του Π.Μ.Σ., συμπεριλαμβανομένων των τελών φοίτησης μεταπτυχιακών φοιτητών και φοιτητριών προερχομένων από την Ελλάδα και λοιπές χώρες της ΕΕ, για τους πρώτους δύο (2) κύκλους λειτουργίας του Π.Μ.Σ. καλύπτονται από τη χρηματοδότηση του συγκεκριμένου έργου, από τα τέλη υποβολής υποψηφιότητας, καθώς και από τα τέλη φοίτησης μεταπτυχιακών φοιτητών και φοιτητριών εκτός ΕΕ

Η χρηματοδότηση του Π.Μ.Σ. από τον τρίτο (3ο) κύκλο λειτουργίας και εφεξής θα προέρχεται από: δωρεές, παροχές, κληροδοτήματα, χορηγίες, ερευνητικά προγράμματα, προγράμματα της Ε.Ε. ή άλλων διεθνών οργανισμών, τέλη υποβολής υποψηφιότητας και φοίτησης όλων των μεταπτυχιακών φοιτητών και φοιτητριών από την Ελλάδα τις λοιπές χώρες της ΕΕ και από τρίτες χώρες, καθώς και από άλλες πηγές, όπως προβλέπεται από την κείμενη νομοθεσία.

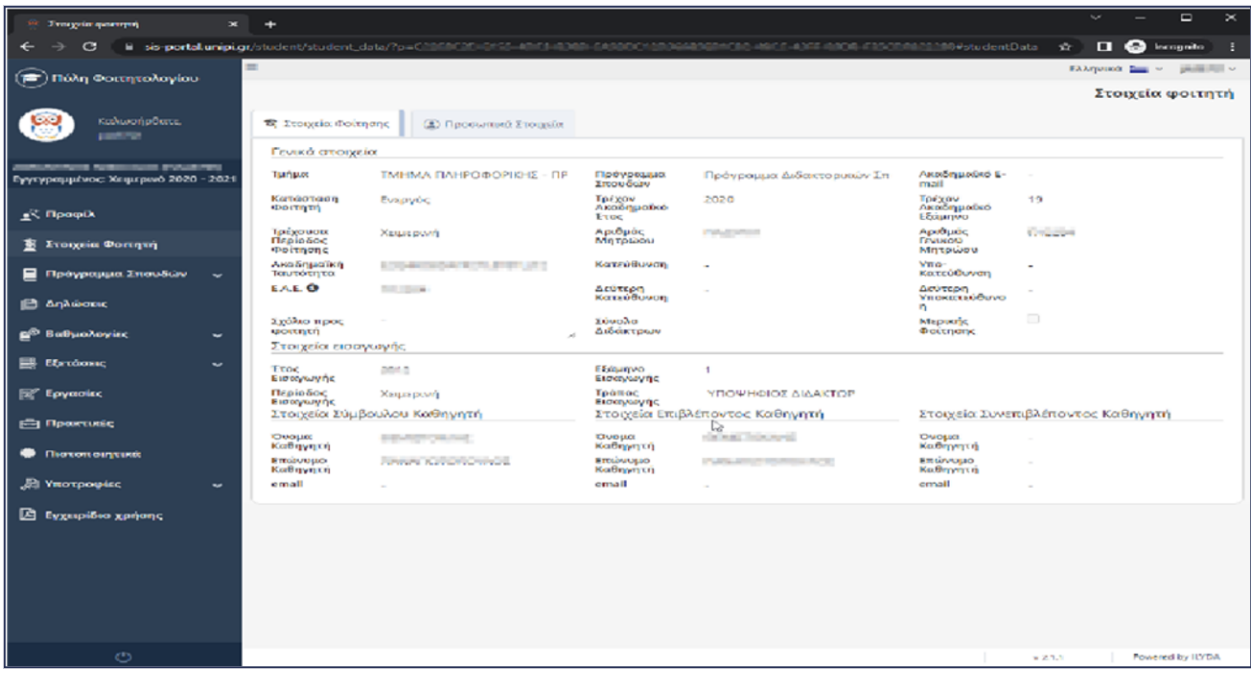
Περισσότερα για την υλικοτεχνική υποδομή του Τμήματος είναι διαθέσιμη στην Ενότητα 2.5.

3.29 Αξιολόγηση Π.Μ.Σ.

Στο τέλος κάθε εξαμήνου πραγματοποιείται αξιολόγηση κάθε μαθήματος και κάθε διδάσκοντος και διδάσκουσας από τους μεταπτυχιακούς φοιτητές και φοιτήτριες. Η πιστοποίηση του Π.Μ.Σ. γίνεται από την Εθνική Αρχή Ανώτατης Εκπαίδευσης (ΕΘ.Α.Α.Ε.),

σύμφωνα με την κείμενη νομοθεσία. Στο πλαίσιο αυτό αξιολογείται η συνολική αποτίμηση του έργου που επιτελέστηκε από το Π.Μ.Σ., ο βαθμός εκπλήρωσης των στόχων που είχαν τεθεί κατά την ίδρυσή του, η βιωσιμότητά του, η απορρόφηση των αποφοίτων από την αγορά εργασίας, ο βαθμός συμβολής του Π.Μ.Σ. στην έρευνα, η εσωτερική αξιολόγησή του από τους μεταπτυχιακούς φοιτητές και φοιτήτριες, η σκοπιμότητα παράτασης της λειτουργίας του, καθώς και λοιπά στοιχεία σχετικά με την ποιότητα του έργου που παράγεται και τη συμβολή του στην εθνική στρατηγική για την ανώτατη εκπαίδευση. Για τη συνέχιση της λειτουργίας του Π.Μ.Σ. απαιτείται η περιοδική πιστοποίησή του στο πλαίσιο της περιοδικής αξιολόγησης/πιστοποίησης του Τμήματος Ψηφιακών Συστημάτων. Το Π.Μ.Σ. έχει δυνατότητα να πιστοποιηθεί και από άλλους φορείς, αν το επιθυμεί.

Μέσω της Πύλης του Φοιτητολογίου (https://sis-portal.unipi.gr/) πραγματοποιείται αξιολόγηση κάθε μαθήματος, κάθε διδάσκοντος και διδάσκουσας καθώς και των υποδομών του Π.Μ.Σ. με εμπιστευτική συμπλήρωση ερωτηματολογίων αξιολόγησης.



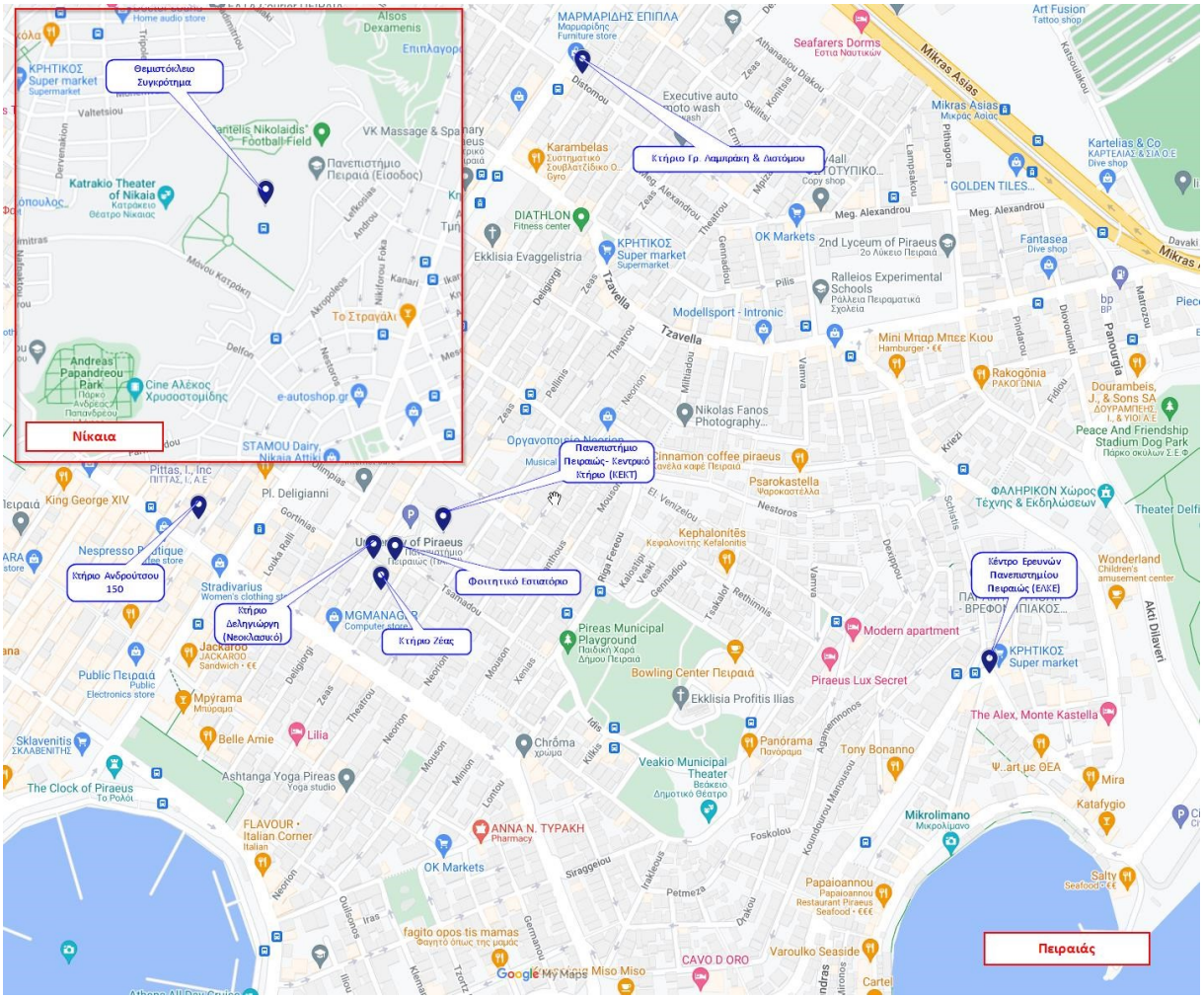
Εικόνα 11: Αρχική ιστοσελίδα υπηρεσίας ηλεκτρονικής γραμματείας (https://sis-portal.unipi.gr)

3.30 Πρόσβαση στους χώρους του Πανεπιστημίου Πειραιώς

3.30.1 Πρόσβαση στους χώρους του Πανεπιστημίου με Μέσα Μαζικής Μεταφοράς

Στον παρακάτω σύνδεσμο, αποτυπώνονται τα κτήρια του πανεπιστημίου Πειραιώς και στον Πίνακα που ακολουθεί προκύπτει με ποιο μέσο μεταφοράς μπορεί να προσεγγιστεί έκαστο.

Κτήρια Πανεπιστημίου Πειραιώς - Google Maps (επιλέξτε το σύνδεσμο)



ΚΤΗΡΙΑ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ	ΟΔΟΣ	ΠΡΟΣΒΑΣΗ ΜΕ ΜΕΣΑ ΜΑΖΙΚΗΣ ΜΕΤΑΦΟΡΑΣ
Πανεπιστήμιο Πειραιώς (ΠΑΠΕΙ) - κεντρικό κτήριο (ΚΕΚΤ)	Καραολή και Δημητρίου 80, Πειραιάς 185 34	• **ΜΕΤΡΟ ΓΡΑΜΜΗ 3** (ΔΗΜΟΤΙΚΟ ΘΕΑΤΡΟ ΠΕΙΡΑΙΑ – ΑΕΡΟΔΡΟΜΙΟ) - **Στάση "ΔΗΜΟΤΙΚΟ ΘΕΑΤΡΟ"** • **ΤΡΑΜ ΓΡΑΜΜΗ 7** (Αγία Τριάδα - Ασκληπιείο Βούλας) - **Στάση "ΠΛΑΤΕΙΑ ΔΕΛΗΓΙΑΝΝΗ"** • **ΓΡΑΜΜΕΣ ΛΕΩΦΟΡΕΙΩΝ**: 040 (ΠΕΙΡΑΙΑΣ - ΣΥΝΤΑΓΜΑ), 049
Πανεπιστήμιο Πειραιώς - κτήριο Νεοκλασικό (ΝΕΟΚΛ/ΔΕΛ107)	Δεληγιώργη 107, Πειραιάς 185 34	(ΠΕΙΡΑΙΑΣ - ΟΜΟΝΟΙΑ), 130 (ΠΕΙΡΑΙΑΣ - Ν. ΣΜΥΡΝΗ), 217 (ΠΕΙΡΑΙΑΣ - ΑΓ. ΔΗΜΗΤΡΙΟΣ - ΣΤ. ΔΑΦΝΗ), 218 (ΠΕΙΡΑΙΑΣ - ΣΤ. ΔΑΦΝΗ), 229 (ΠΕΙΡΑΙΑΣ - ΑΓ. ΔΗΜΗΤΡΙΟΣ - ΣΤ. ΔΑΦΝΗ), Α1 (ΠΕΙΡΑΙΑΣ - ΒΟΥΛΑ), Β1 (ΠΕΙΡΑΙΑΣ - ΑΝΩ ΓΛΥΦΑΔΑ), 915 (ΛΟΦΟΣ ΒΩΚΟΥ - ΠΡ. ΗΛΙΑΣ) - **Στάση "ΒΕΝΙΖΕΛΟΥ"** • **ΓΡΑΜΜΗ ΗΛΕΚΤΡΙΚΟΥ ΗΣΑΠ** (ΠΕΙΡΑΙΑΣ - ΚΗΦΙΣΙΑ) - **Στάση "ΠΕΙΡΑΙΑΣ"** (*ΑΝΤΑΠΟΚΡΙΣΗ ΜΕ ΓΡΑΜΜΗ ΜΕΤΡΟ Μ3 ΚΑΙ ΛΕΩΦΟΡΕΙΟ 915*) • **ΓΡΑΜΜΕΣ ΛΕΩΦΟΡΕΙΩΝ**: 915 (ΛΟΦΟΣ ΒΩΚΟΥ - ΠΡ. ΗΛΙΑΣ), 420 (ΠΕΙΡΑΙΑΣ - ΑΓ. ΑΝΑΡΓΥΡΟΙ (ΜΕΣΩ ΚΗΦΙΣΟΥ)), 703 (ΠΕΙΡΑΙΑΣ - ΑΓ. ΑΝΑΡΓΥΡΟΙ - ΑΓ. ΕΛΕΥΘΕΡΙΟΣ), 803 (ΔΑΣΟΣ ΧΑΪΔΑΡΙΟΥ - ΠΕΙΡΑΙΑΣ), 814 (ΣΧΙΣΤΟ ΚΑΡΑΒΑΣ - ΠΕΙΡΑΙΑΣ), 824 (ΝΕΑΠΟΛΗ - ΑΓ. ΑΝΤΩΝΙΟΣ - ΠΕΙΡΑΙΑΣ Α), 825 (ΝΕΑΠΟΛΗ - ΑΓ. ΑΝΤΩΝΙΟΣ - ΠΕΙΡΑΙΑΣ Β), 826 (ΠΕΙΡΑΙΑΣ - ΑΓ. ΜΗΝΑΣ), 832 (ΕΥΓΕΝΕΙΑ - ΧΑΡΑΥΓΗ - ΠΕΙΡΑΙΑΣ Α), 833 (ΕΥΓΕΝΕΙΑ - ΧΑΡΑΥΓΗ - ΠΕΙΡΑΙΑΣ Β), 843 (ΠΕΡΑΜΑ - ΠΕΙΡΑΙΑΣ), 845 (ΕΛΕΥΣΙΝΑ - ΠΕΙΡΑΙΑΣ), 909 (ΚΡΑΤ.
Πανεπιστήμιο Πειραιώς - κτήριο Γρ.Λαμπράκη (ΓΛ21)	Διστόμου 43, Πειραιάς 185 33	
Πανεπιστήμιο Πειραιώς - κτήριο Ανδρούτσου (ΑΝΔ150)	Οδυσσέα Ανδρούτσου 150, Πειραιάς 185 32	
Πανεπιστήμιο Πειραιώς - κτήριο Ζέας	Ζέας 82, Πειραιάς 185 34	
Φοιτητικό εστιατόριο Πανεπιστημίου Πειραιώς	Τσαμαδού 78, Πειραιάς 185 34	ΝΙΚΑΙΑΣ - ΑΓ. ΣΟΦΙΑ - ΑΓ. ΒΑΣΙΛΕΙΟΣ) - **Στάση "ΣΤ.ΜΕΤΡΟ ΠΕΙΡΑΙΑΣ"** (*ΑΝΤΑΠΟΚΡΙΣΗ ΜΕ ΓΡΑΜΜΗ ΜΕΤΡΟ Μ3 ΚΑΙ ΛΕΩΦΟΡΕΙΟ*

ΚΤΗΡΙΑ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ	ΟΔΟΣ	ΠΡΟΣΒΑΣΗ ΜΕ ΜΕΣΑ ΜΑΖΙΚΗΣ ΜΕΤΑΦΟΡΑΣ
		915)
Πανεπιστήμιο Πειραιώς - Θεμιστόκλειο Συγκρότημα- Κτήριο Άρσης Βαρών (ΝΙΚΑΙΑ Α, Γ, Δ)	Κυράς Της Ρώ 17, Νίκαια 184 51	**ΓΡΑΜΜΗ ΛΕΩΦΟΡΕΙΟΥ**: 750 (ΝΙΚΑΙΑ - ΣΤ.ΜΕΤΡΟ ΑΙΓΑΛΕΩ - ΑΤΤΙΚΟ ΝΟΣΟΚΟΜΕΙΟ) - **Στάση "ΝΙΚΑΙΑ"**
Κέντρο Ερευνών Πανεπιστημίου Πειραιώς	Λεωφ. Αλ. Παπαναστασίου 91, Πειραιάς 185 33	**ΓΡΑΜΜΗ ΤΡΟΛΕΪ**: 20 (Ν. ΦΑΛΗΡΟ - ΚΑΣΤΕΛΛΑ - ΔΡΑΠΕΤΣΩΝΑ) - **Στάση "ΜΙΚΡΟΛΙΜΑΝΟ"**

3.30.2 Υποδομές προσβασιμότητας για ΑΜΕΑ

Στα κτίρια του Πανεπιστημίου Πειραιώς έχουν γίνει ενέργειες εφαρμογής αναφορικά με τις υποδομές προσβασιμότητας για τα άτομα με μειωμένη κινητικότητα και αισθητηριακή αναπηρία. Με την ενίσχυση της πρόσβασης επιτυγχάνεται η ασφαλής λειτουργία των ανελκυστήρων, η διαρρύθμιση των τουαλετών (W.C.), η εγκατάσταση ειδικών αναβατορίων/πλατφόρμες ΑμεΑ, η κατασκευή ραμπών, η τοποθέτηση κιγκλιδωμάτων κατάλληλης μορφής και ύψους (εξώστες, είσοδοι κ.α.), η τοποθέτηση χειρολισθήρων, η δημιουργία χώρων στάθμευσης με επιδαπέδια σήμανση πλησίον των ανελκυστήρων. Κάθε κτίριο που χρησιμοποιείται από τα Π.Μ.Σ. είναι προσβάσιμο από άτομα ΑμεΑ από δύο τουλάχιστον εισόδους: α) την κεντρική είσοδο και β) τους υπόγειους χώρους στάθμευσης. Δεδομένης της μετακίνησης των ατόμων με ειδικές ανάγκες στους εσωτερικούς χώρους των κτιρίων, υπάρχουν πυροδιαμερίσματα σύμφωνα με εγκεκριμένες μελέτες πυροπροστασίας, οι οποίες προβλέπουν χώρους μετακίνησης (ανελκυστήρες) που χρησιμοποιούνται και σαν έξοδοι διαφυγής σε περίπτωση ανάγκης.

3.31 Στοιχεία Επικοινωνίας

3.31.1 Ακαδημαϊκή Γραμματεία Τμήματος

Διεύθυνση: Οδός Ζέας 80-82 (2ος όροφος), ΤΚ 18532, Πειραιάς
Ομαδικό E-mail Γραμματείας : gramds@unipi.gr

Ονομ/μο: Παρασκευή Αντωνίου (Προϊσταμένη)
Τηλ.: 210-4142235
email: panton@unipi.gr

Ονομ/μο: Σοφία Σκούντζου
Τηλ.: 210-4142373
email: sskountz@unipi.gr

Ονομ/μο: Ιωάννης Φρεντζάς
Τηλ.: 210-4142426
email: fretzas@unipi.gr

Ονομ/μο: Παναγιώτης Θεοδωρόπουλος
Τηλ.: 210-4142369
e-mail: ptheodor@unipi.gr

3.31.2 Γραμματεία Μεταπτυχιακών Σπουδών

Διεύθυνση: Οδός Οδυσσέα Ανδρούτσου 150 (1ος όροφος, γραφείο 103), ΤΚ 18532 Πειραιάς (ώρες λειτουργίας 10:00–16:00)
Τηλέφωνο: 210-414.2757
Website: https://cybersecgov.ds.unipi.gr/
Email: cybersecgov@unipi.gr

3.31.3 Κοινωνικά Δίκτυα

Τα κοινωνικά δίκτυα του Π.Μ.Σ. είναι τα παρακάτω:

Facebook: https://www.facebook.com/cybersecgov/
Linkedin: https://www.linkedin.com/company/cybersecgov
Instagram: https://www.instagram.com/cybersecgov.msc/

4 ΠΑΡΑΡΤΗΜΑΤΑ

4.1 Παράρτημα 1: Έντυπο αίτησης υποψηφιότητας

Θέση Φωτογραφίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Π.Μ.Σ.)

ΠΡΟΗΓΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ

MSc in Advanced Cybersecurity Technologies and Governance

ΑΙΤΗΣΗ ΥΠΟΨΗΦΙΟΤΗΤΑΣ

Προσωπικά Στοιχεία			
Επώνυμο		**Όνομα**	
Ημερομηνία Γέννησης		**Email**	
Αριθμός Ταυτότητας ή Διαβατηρίου		**Τηλ. Κινητό**	
Διεύθυνση Κατοικίας			
Διεύθυνση Επικοινωνίας *(εάν είναι διαφορετική από τη διεύθυνση κατοικίας)*			
Τηλ. Σταθερό			

Σπουδές			
ΠΡΟΠΤΥΧΙΑΚΕΣ ΣΠΟΥΔΕΣ			
ΑΕΙ	**Τμήμα**	**Ημερομηνία Αποφοίτησης**	**Βαθμός Πτυχίου ή Διπλώματος**
ΜΕΤΑΠΤΥΧΙΑΚΕΣ ΣΠΟΥΔΕΣ			
ΑΕΙ	**Τμήμα**	**Ημερομηνία Αποφοίτησης**	**Βαθμός Διπλώματος**

- Στη διαδικασία υποβολής αιτήσεων και αξιολόγησης μπορούν να συμμετάσχουν τελειόφοιτοι φοιτητές και φοιτήτριες που αναμένεται να ολοκληρώσουν τις σπουδές τους πριν την έναρξη του νέου ακαδημαϊκού έτους για το Π.Μ.Σ. Η αποδοχή φοιτητών και φοιτητριών που ανήκουν στη συγκεκριμένη κατηγορία γίνεται με την προϋπόθεση ότι θα προσκομίσουν βεβαίωση ολοκλήρωσης των σπουδών τους από τη Γραμματεία του Τμήματος στο οποίο σπουδάζουν, κατά τη διάρκεια των εγγραφών του παρόντος Π.Μ.Σ.
- Οι υποψήφιοι και υποψήφιες 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. Σε κάθε περίπτωση, τίτλοι σπουδών της αλλοδαπής υποβάλλονται και γίνονται αποδεκτοί σύμφωνα με τις κείμενες διατάξεις

Ξένες Γλώσσες (* βλέπε σημείωση στο τέλος)		
Γλώσσα	**Επίπεδο Γνώσης**	**Τίτλος**

Πτυχιακές Εργασίες (για πτυχιούχους/τελειόφοιτους), Διπλωματικές Εργασίες (για διπλωματούχους/τελειόφοιτους μηχανικούς), Μεταπτυχιακές Εργασίες (για κατόχους Π.Μ.Σ.)			
Είδος Εργασίας	**Θέμα Εργασίας**	**Επιβλέπων Καθηγητής ή Καθηγήτρια**	**Βαθμός**

Βραβεία, Διακρίσεις, Υποτροφίες

Επαγγελματική Δραστηριότητα			
Θέση Εργασίας	**Οργανισμός**	**Χρονικό Διάστημα**	
		από: *Μήνας/Έτος*	*έως:* *Μήνας/Έτος*

Ερευνητική Δραστηριότητα *(τυχόν ερευνητικές εργασίες ή ερευνητικά έργα στα οποία έχετε συμμετάσχει)*

Συστατικές Επιστολές *(στοιχεία δύο ατόμων, από τα οποία έχετε λάβει συστατική επιστολή)*					
	Όνομα / Επώνυμο	**Τίτλος**	**Ίδρυμα/Οργανισμός**	**Τηλέφωνο**	**e-mail**
1					
2					

Άλλα μεταπτυχιακά προγράμματα στα οποία έχετε υποβάλει ή σκοπεύετε να υποβάλετε αίτηση	
Ίδρυμα	**Τίτλος**

Τρόπος με τον οποίο ενημερωθήκατε για τα Μεταπτυχιακά Προγράμματα του Τμήματος Ψηφιακών Συστημάτων					
☐	Παγκόσμιος Ιστός	☐	Μέσα Κοινωνικής Δικτύωσης	☐	Φιλικό Πρόσωπο
☐	Απόφοιτος/Απόφοιτη του Π.Μ.Σ.	☐	Ημερίδα Τμήματος	☐	Άλλο

Άλλες Πληροφορίες *(συμπληρώστε ότι στοιχεία θεωρείτε ότι μπορεί να ενισχύσουν την υποψηφιότητά σας)*

Συνημμένα Δικαιολογητικά	
ΥΠΟΧΡΕΩΤΙΚΑ	
☐	Αναλυτικό βιογραφικό σημείωμα
☐	Απλά αντίγραφα τίτλων σπουδών ή άλλα στοιχεία (π.χ. βεβαίωση περάτωσης, αναλυτική βαθμολογία) από τα οποία να προκύπτει ότι έχουν αποφοιτήσει (για τους τελειόφοιτους ότι βρίσκονται ενώπιον αποφοίτησης)
☐	Απλή αναλυτική βαθμολογία (μία για κάθε τίτλο σπουδών)
☐	Απλό αποδεικτικό καλής γνώσης της Αγγλικής γλώσσας
☐	Δύο (2) Συστατικές Επιστολές (μπορούν να αποσταλούν ηλεκτρονικά, απευθείας από τους Συστήνοντες, στην ηλεκτρονική διεύθυνση: cybersecgov@unipi.gr)
☐	Απλά αντίγραφα τυχόν επιστημονικών εργασιών και δημοσιεύσεων
☐	Απλή φωτοτυπία διαβατηρίου ή εθνικού εγγράφου ταυτοποίησης
☐	Μια (1) φωτογραφία
ΠΡΟΣΘΕΤΑ	
☐	
☐	

(*) Η καλή γνώση της αγγλικής γλώσσας αποδεικνύεται με:

• FIRST CERTIFICATE IN ENGLISH του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH ή FIRST CERTIFICATE IN ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179.

• CERTIFICATE IN ADVANCED ENGLISH του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179

• BULATS English Language Test, βαθμολογία 60-74, του Πανεπιστημίου CAMBRIDGE ή του CAMBRIDGE ASSESSMENT ENGLISH (Για πιστοποιητικά που έχουν εκδοθεί έως και 19/11/2019).

• INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) από το University of Cambridge Local Examinations Syndicate

(UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH – The British Council – IDP Education Australia IELTS Australia με βαθμολογία από 5,5 έως 6,5.

•BUSINESS ENGLISH CERTIFICATE – VANTAGE (BEC VANTAGE) από το University of Cambridge Local Examinations Syndicate (UCLES) ή το CAMBRIDGE ASSESSMENT ENGLISH ή BUSINESS ENGLISH CERTIFICATE VANTAGE του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-179

• BUSINESS ENGLISH CERTIFICATE PRELIMINARY του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-170

• PRELIMINARY ENGLISH TEST του CAMBRIDGE ASSESSMENT ENGLISH overall score 160-170

• (ECCE)- CERTIFICATE OF COMPETENCY IN ENGLISH του Πανεπιστημίου MICHIGAN (ENGLISH LANGUAGE INSTITUTE ή Cambridge Michigan Language Assessments - CaMLA ή Michigan Language Assessment.)

• LONDON TESTS OF ENGLISH LEVEL 3 - UPPER INTERMEDIATE COMMUNICATION- του EDEXCEL ή PEARSON TEST OF ENGLISH GENERAL LEVEL 3 UPPER- INTERMEDIATE COMMUNICATION- του EDEXCEL ή EDEXCEL LEVEL I CERTIFICATE IN ESOL INTERNATIONAL (CEF B2) ή PEARSON EDEXCEL LEVEL I CERTIFICATE IN ESOL INTERNATIONAL (CEF B2) (ENGLISH INTERNATIONAL CERTIFICATE)

•CERTIFICATE IN INTEGRATED SKILLS IN ENGLISH ISE II του TRINITY COLLEGE LONDON.

• CITY & GUILDS LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (reading, writing, and listening) -COMMUNICATOR- και CITY & GUILDS LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (Spoken) -COMMUNICATOR- (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης) ή CITY & GUILDS CERTIFICATE IN INTERNATIONAL ESOL - COMMUNICATOR - και CITY & GUILDS CERTIFICATE IN INTERNATIONAL SPOKEN ESOL - COMMUNICATOR - (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης).

•Assessment Board for Language Examinations: Level B2 (ABLE B2)του Hellenic American University (Nashua, New Hampshire, USA)

•TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC) του EDUCATIONAL TESTING SERVICE/CHAUNCEY, USA, βαθμολογία από 505 έως 780.

• EDI Level 1 Certificate in ESOL International JETSET Level 5 (CEF B2) ή PEARSON EDI Level 1 Certificate in ESOL International (CEF B2) ή PEARSON LCCI LEVEL 1 CERTIFICATE IN ESOL INTERNATIONAL (CEFR B2)

•PEARSON LCCI EFB LEVEL 3 (Ενότητες: Reading, Writing, Listening, Speaking, σε περίπτωση που η μία εκ των ενοτήτων είναι με βαθμό "Pass").

• PEARSON LCCI EFB LEVEL 2 (Ενότητες: Reading, Writing, Listening, Speaking, με βαθμό «Distinction" ή "Credit.

• OCNW Certificate in ESOL International at Level 1 (Common European Framework equivalent level B2)) (μέχρι 31/8/2009)

• Ascentis Level 1 Certificate in ESOL International (CEF B2)

• ESB Level 1 Certificate in ESOL International All Modes (Council of Europe Level B2).

• Michigan State University – Certificate of English Language Competency (MSU – CELC) : CEF B2.

• Test of Interactive English, B2 + Level (ACELS)

• Test of Interactive English, B2 Level (ACELS) ή Test of Interactive English, B2 Level (Gatehouse Awards).

• NOCN Level 1 Certificate in ESOL International (B2).

•AIM Awards Level 1 Certificate in ESOL International (B2) (Ενότητες: Listening, Reading, Writing, Speaking) ή AIM Qualifications Level 1 Certificate in ESOL International (B2) (Anglia Advanced) (Ενότητες: Listening, Reading, Writing, Speaking).

• MICHIGAN ENGLISH LANGUAGE ASSESSMENT BATTERY (MELAB) βαθμολογία από 80 έως 90 του CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS ή του MICHIGAN LANGUAGE ASSESSMENT

MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading, Speaking) βαθμολογία από 157 έως 189 του Michigan Language Assessment ή CAMBRIDGE MICHIGAN LANGUAGE ASSESSMENTS- CaMLA ή

MET - MICHIGAN ENGLISH TEST (Ενότητες: Listening, Reading ή Listening, Reading, Speaking, Writing) βαθμολογία από 53 έως 63 του Michigan Language Assessment

• LRN Level 1 Certificate in ESOL International (CEF B2)

• GA Level 1 Certificate in ESOL International –(CEFR: B2) ή GA Level 1 Certificate in ESOL International (Classic B2)

• B2 -LanguageCert Level 1 Certificate in ESOL International (Listening, Reading, Writing) (Communicator B2) και B2 - LanguageCert Level 1 Certificate in ESOL International (Speaking) (Communicator B2) (Συνυποβάλλονται αθροιστικά για την απόδειξη της καλής γνώσης).

•Open College Network West Midlands Level 1 Certificate in ESOL International (CEFR B2)

• NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level B2

• LanguageCert Test of English (LTE) - LanguageCert Level 1 Certificate in ESOL International (Listening, Reading) (LanguageCert Test of English B2)

• OCNLR Level 1 Certificate in ESOL International (CEFR B2)

• VTCT (ITEC) Level 1 Certificate in ESOL International (B2)

ή Κρατικό Πιστοποιητικό Γλωσσομάθειας επιπέδου Β2 του Ν.2740/1999, όπως αντικαταστάθηκε με την παρ.19 του άρθρου 13 του ν.3149/2003..

Δηλώνω ότι:

1. Τα στοιχεία που αναφέρω στην παρούσα αίτηση και τα συνημμένα δικαιολογητικά είναι πλήρη και ακριβή
2. Θα προσκομίσω αντίγραφα κατά την εγγραφή μου στο Π.Μ.Σ.
3. Εφόσον δεν προσκομίσω βεβαίωση περάτωσης των προπτυχιακών σπουδών μου και αποδεικτικό καλής γνώσης της αγγλικής γλώσσας μέχρι και την 30η Σεπτεμβρίου τρέχοντος έτους δε θα πραγματοποιηθεί η εγγραφή μου στο Π.Μ.Σ.
4. Το ποσό της πρώτης δόσης των τελών που θα καταβάλω εφόσον γίνω δεκτός ή δεκτή, δεν επιστρέφεται για οποιονδήποτε λόγο (εκτός των περιπτώσεων μεταπτυχιακών φοιτητών και φοιτητριών που δεν καταστούν πτυχιούχοι μέχρι τη λήξη των εγγραφών Σεπτεμβρίου στο Π.Μ.Σ.)
5. Από τον τρίτο κύκλο λειτουργίας και εφεξής, σε περίπτωση που ανήκω στους επιλεγέντες φοιτητές και επιλεγείσες φοιτήτριες που απαλλάσσονται των τελών φοίτησης στο πλαίσιο της κείμενης νομοθεσίας τα μέχρι εκείνη τη στιγμή καταβληθέντα τέλη θα μου επιστραφούν εν όλω.
6. Έχω μελετήσει, έχω κατανοήσει και συναινώ με το περιεχόμενο της «Πολιτικής Προστασίας των Προσωπικών Δεδομένων» των αιτήσεων των υποψηφίων μεταπτυχιακών φοιτητών και φοιτητριών του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς που επισυνάπτεται στο τέλος της παρούσας αίτησης, τους σύμφωνους προς αυτή σκοπούς επεξεργασίας των προσωπικών δεδομένων μου, αλλά και τον ισχύοντα Κανονισμό του Π.Μ.Σ.

Ημερομηνία

Ο Αιτών–Δηλών / Η Αιτούσα-Δηλούσα

Υπογραφή

4.2 Παράρτημα 2: Πρότυπο Συστατικής Επιστολής

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (Π.Μ.Σ.)
ΠΡΟΗΓΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΔΙΑΚΥΒΕΡΝΗΣΗ
MSc in Advanced Cybersecurity Technologies and Governance

ΣΥΣΤΑΤΙΚΗ ΕΠΙΣΤΟΛΗ

ΟΔΗΓΙΕΣ

- Παρακαλούμε συμπληρώστε τις απαραίτητες πληροφορίες για τον υποψήφιο ή την υποψήφια στα πεδία που ακολουθούν.
- Εάν προτιμάτε, μπορείτε να χρησιμοποιήσετε δικό σας επιστολόχαρτο για να συντάξετε τη συστατική επιστολή, την οποία παρακαλούμε να επισυνάψετε στην παρούσα σελίδα. Σε αυτή την περίπτωση, παρακαλούμε να λάβετε υπόψη τις πληροφορίες που ζητάμε σε αυτή τη φόρμα.
- Η επιστολή – αν δεν μας αποσταλεί απευθείας ηλεκτρονικά - θα πρέπει να παραδοθεί σφραγισμένη σε φάκελο.

Ευχαριστούμε για τη βοήθειά σας!

Στοιχεία Υποψήφιου / Υποψήφιας			
Ονοματεπώνυμο			
Στοιχεία Συντάκτη			
Ονοματεπώνυμο Συντάκτη			
Τίτλος		**Ίδρυμα/Οργανισμός/Εταιρεία**	
Διεύθυνση			
Τηλέφωνο		**E-mail**	

Από πότε και με ποια ιδιότητα γνωρίζετε τον υποψήφιο / την υποψήφια;

Εάν ο υποψήφιος / η υποψήφια παρακολούθησε μαθήματα που διδάξατε, τι μαθήματα παρακολούθησε, τι βαθμό πήρε σε κάθε μάθημα και ποια ήταν η σχετική κατάταξη που είχε στην τάξη του;

Σχολιάστε τις δεξιότητες και τις δυνατότητες του υποψηφίου / της υποψήφιας σε προφορική και γραπτή επικοινωνία, συνεργασία με άλλους και άλλες και εμπρόθεσμη επίτευξη στόχων

Εξηγήστε τους λόγους για τους οποίους προτείνετε τον υποψήφιο / την υποψήφια για το συγκεκριμένο πρόγραμμα μεταπτυχιακών σπουδών

ΣΥΝΙΣΤΑΤΕ ΤΟΝ ΥΠΟΨΗΦΙΟ / ΤΗΝ ΥΠΟΨΗΦΙΑ ΓΙΑ ΤΟ ΣΥΓΚΕΚΡΙΜΕΝΟ ΜΕΤΑΠΤΥΧΙΑΚΟ;	
☐	τον συνιστώ ανεπιφύλακτα
☐	τον συνιστώ με επιφυλάξεις
☐	δεν τον συνιστώ
☐	δεν έχω διαμορφώσει εικόνα/δεν είμαι σίγουρος

Ημερομηνία

Υπογραφή Συντάκτη

4.3 Παράρτημα 3: Κανονισμός Κινητικότητας Φοιτητών και Φοιτητριών και Προσωπικού (Πρόγραμμα ERASMUS+ και ERASMUS+ International)

Ο Κανονισμός Κινητικότητας Φοιτητών και Φοιτητριών και Προσωπικού (Πρόγραμμα ERASMUS+ και ERASMUS+ International) αναλύεται στο έγγραφο "D5.2β. Κανονισμός Κινητικότητας φοιτητών/φοιτητριών και προσωπικού (Πρόγραμμα ERASMUS+ και ERASMUS+ International)". Αναρτάται στην ιστοσελίδα του Π.Μ.Σ. και ανανεώνεται όποτε υπάρξουν αλλαγές.

4.4 Παράρτημα 4: Κανονισμός Ακαδημαϊκού Συμβούλου Σπουδών

Ο Κανονισμός Ακαδημαϊκού Συμβούλου Σπουδών αναλύεται στο έγγραφο "D4.4. Κανονισμός λειτουργίας θεσμού Ακαδημαϊκού Συμβούλου Σπουδών". Αναρτάται στην ιστοσελίδα του Π.Μ.Σ. και ανανεώνεται όποτε υπάρξουν αλλαγές.

4.5 Παράρτημα 5: Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων μεταπτυχιακών φοιτητών και φοιτητριών

Ο Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων φοιτητών αναλύεται στο έγγραφο "D4.3. Κανονισμός λειτουργίας μηχανισμού διαχείρισης παραπόνων και ενστάσεων φοιτητών". Αναρτάται στην ιστοσελίδα του Π.Μ.Σ. και ανανεώνεται όποτε υπάρξουν αλλαγές.

4.6 Παράρτημα 6: Κανονισμός Εκπόνησης Εργασιών

Ο Κανονισμός Εκπόνησης Εργασιών του Π.Μ.Σ. αναλύεται στο έγγραφο "D5.2γ. Κανονισμός Εκπόνησης Εργασιών ". Αναρτάται στην ιστοσελίδα του Π.Μ.Σ. και ανανεώνεται όποτε υπάρξουν αλλαγές.

4.7 Παράρτημα 7: Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας

Ο Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας αναλύεται στο έγγραφο "D5.2δ. Κανονισμός Εκπόνησης Μεταπτυχιακής Διπλωματικής Εργασίας". Αναρτάται στην ιστοσελίδα του Π.Μ.Σ. και ανανεώνεται όποτε υπάρξουν αλλαγές.