ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ. «Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης»

Οδηγός Σπουδών
2024-2025

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

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. Το 1945 μετονομάστηκε σε «Ανωτέρα Σχολή Βιομηχανικών Σπουδών» και ως σκοπός της ορίσθηκε η συστηματική, θεωρητική και πρακτική κατάρτιση διοικητικών στελεχών. Το 1958 μετονομάστηκε σε «Ανωτάτη Βιομηχανική Σχολή» με έδρα τον Πειραιά. Η φοίτηση έγινε τετραετής και τα πτυχία που χορηγούνταν ήταν ισότιμα με αυτά των άλλων Ανωτάτων Εκπαιδευτικών Ιδρυμάτων (Α.Ε.Ι.). Από το ακαδημαϊκό έτος 1971-1972 οι σπουδές στη Σχολή διαχωρίστηκαν από το δεύτερο έτος σε σπουδές Οικονομικών Επιστημών και Οργάνωσης και Διοίκησης Επιχειρήσεων, ενώ από το 1977-1978 λειτούργησε το Τμήμα Στατιστικής και Ασφαλιστικής Επιστήμης.

Τον Ιούνιο του 1989, με το ΠΔ 377/89, η Ανώτατη Βιομηχανική Σχολή μετονομάστηκε σε Πανεπιστήμιο Πειραιώς.

Περιεχόμενα

Π.Μ.Σ. «Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης»

Το Πρόγραμμα « Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης» στοχεύει στη μελέτη και εφαρμογή Παραδοσιακών Τεχνολογιών αλλά και Τεχνολογιών Τεχνητής Νοημοσύνης για την παροχή και υποστήριξη λύσεων Κυβενοασφάλειας, αλλά και στο πως μηχανισμοί Κυβερνοασφάλειας θα διασφαλίσουν την ανάπτυξη, λειτουργία και χρήση συστημάτων και υπηρεσιών τεχνητής νοημοσύνης.

Σ' αυτό το πλαίσιο, οι απόφοιτοι του Π.Μ.Σ. δύνανται να στελεχώσουν υπηρεσίες και οργανισμούς του δημόσιου και ιδιωτικού τομέα, καθώς και να ακολουθήσουν Ακαδημαϊκή ή Ερευνητική καριέρα.

Συντονιστική Επιτροπή

Χρήστος Ξενάκης, Καθηγητής (Διευθυντής ΠΜΣ)
Κωνσταντίνος Λαμπρινουδάκης, Καθηγητής
Στέφανος Γκρίτζαλης, Καθηγητής
Γεώργιος Βούρος, Καθηγητής
Νικήτας Μαρίνος Σγούρος, Καθηγητής

Στόχοι

Οι βασικοί στόχοι του Π.Μ.Σ «Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης», είναι:

01 Η περαιτέρω επιστημονική ειδίκευση νέων επιστημόνων στα γνωστικά αντικείμενα της της Κυβερνοασφάλειας, των Τεχνολογιών Τεχνητής Νοημοσύνης, και της προστασίας της ιδιωτικότητας των χρηστών και η προετοιμασία για σπουδές διδακτορικού επιπέδου στα γνωστικά αντικείμενα του τμήματος Ψηφιακών Συστημάτων.

02 Η εκπαίδευση/ειδίκευση επιστημόνων που ήδη απασχολούνται σε ελληνικές ή διεθνείς επιχειρήσεις και οργανισμούς του δημόσιου και ιδιωτικού τομέα.

03 Η ανάπτυξη ακαδημαϊκών ικανοτήτων και η ενδυνάμωση των δεξιοτήτων επικοινωνίας, συνεργασίας και διαχείρισης υποχρεώσεων του φοιτητικού δυναμικού μέσω ομαδικών εργασιών, ομαδικών παρουσιάσεων και άλλων συνεργατικών μορφών ακαδημαϊκής μελέτης και εκπόνησης εργασιών.

04 Η παροχή υψηλού επιπέδου μεταπτυχιακής εκπαίδευσης, ώστε οι απόφοιτοι/ες να έχουν τη δυνατότητα να συμβάλουν αναπτυξιακά στην τεχνολογική πολιτική της Ελλάδας.

Με την απόκτηση του συγκεκριμένου Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.), οι κάτοχοί του θα είναι σε θέση να:

- να ανιχνεύουν τις αδυναμίες και τα τρωτά σημεία ασφάλειας και ιδιωτικότητας που παρουσιάζουν ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες, τα οποία είτε από ατύχημα είτε επί σκοπού (εάν γίνουν αντικείμενο εκμετάλλευσης από κακόβουλους) δύναται να οδηγήσουν σε εκδήλωση κυβερνοπεριστατικών, τα οποία έχουν ως αποτέλεσμα είτε την διαρροή δεδομένων είτε την κατάρρευση - προβληματική λειτουργεία συστημάτων και υπηρεσιών.
- να καταγράφουν τις απαιτήσεις ασφάλειας και ιδιωτικότητας που παρουσιάζουν ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες σύμφωνα με το λειτουργικό τους μοντέλο, τα διεθνή πρότυπα, καθώς και το διεθνές κανονιστικό και νομικό πλαίσιο.
- να σχεδιάζουν, να αναλύουν, να υλοποιούν και να εφαρμόζουν διαδικασίες και λύσεις κυβερνοασφάλειας και ιδιωτικότητας σε ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες.
- να υπολογίζουν, να διαχειρίζονται και να μειώνουν τις τιμές του ρίσκου κυβερνοασφάλειας, στο οποίο εκτίθενται ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες.
- να αντιμετωπίζουν και να διαχειρίζονται, δυναμικά, κυβερνοπεριστασικά με σκοπό να περιορίζουν τον αντίκτυπο και τις επιπτώσεις τους
- να έχουν την ικανότητα να ερμηνεύουν, να αναλύουν και να ενημερώνουν κοινό και επαγγελματίες/επιστήμονες άλλων χώρων για θέματα κυβερνοασφάλειας και προστασίας της ιδιωτικότητας
- να κατανοούν τις επιστημονικές, τεχνολογικές και οικονομικές εξελίξεις που συνδέονται ή επηρεάζουν το χώρο της κυβερνοασφάλειας και ιδιωτικότητας, και να μπορούν να παρεμβαίνουν, όπου απαιτείται, ώστε να πετυχαίνουν τα καθήκοντα που τους έχουν ανατεθεί
- να μπορούν να συνεισφέρουν ουσιαστικά στην πρόοδο της επιστήμης, της τεχνολογίας, της οικονομίας, της ασφάλειας της κοινωνίας και της πατρίδας τους
- να έχουν την ικανότητα να διεξαγάγουν έρευνα υψηλού επιπέδου στο χώρο της ασφάλειας και της ιδιωτικότητας.

Φοίτηση

Εισαγωγή στο Π.Μ.Σ.

Ο ετήσιος αριθμός εισακτέων ανέρχεται σε μέχρι σαράντα (40) μεταπτυχιακούς/ες φοιτητές/τριες.

Στο ΠΜΣ γίνονται δεκτοί κάτοχοι τίτλου πρώτου κύκλου σπουδών Α.Ε.Ι. της ημεδαπής ή ομοταγών ιδρυμάτων της αλλοδαπής. Αλλοδαποί υποψήφιου και υποψήφιες θα πρέπει να γνωρίζουν επαρκώς την Ελληνική γλώσσα και καλώς την Αγγλική γλώσσα.

Τα μέλη των κατηγοριών Ε.Ε.Π., Ε.ΔΙ.Π. και Ε.Τ.Ε.Π. και διοικητικών υπαλλήλων του ιδρύματος, που πληρούν τις προϋποθέσεις της προηγούμενης παραγράφου, μπορούν μετά από αίτησή τους να γίνουν δεκτοί ως υπεράριθμοι, και μόνο ένας κατ' έτος, σύμφωνα με τον Εσωτερικό Κανονισμό του ιδρύματος.

Οι αιτήσεις των Υποψηφίων πρέπει να συνοδεύονται από τα προβλεπόμενα δικαιολογητικά σύμφωνα με την προκήρυξη. Η αίτηση και τα ηλεκτρονικά αντίγραφα των δικαιολογητικών κατατίθενται στο σύστημα «ΑΡΙΣΤΥΛΛΟΣ». Τυχόν έντυπα αντίγραφα κατατίθενται κατά την εγγραφή.

Σπουδές στο Π.Μ.Σ.

Η χρονική διάρκεια σπουδών για την απονομή του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) ορίζεται σε τρία (3) εξάμηνα για το πρόγραμμα πλήρους φοίτησης, στα οποία περιλαμβάνεται και ο χρόνος εκπόνησης διπλωματικής εργασίας. Ο ανώτατος επιτρεπόμενος χρόνος ολοκλήρωσης των σπουδών, ορίζεται στα πέντε (5) ακαδημαϊκά εξάμηνα.

Το ΠΜΣ ξεκινά το χειμερινό εξάμηνο κάθε ακαδημαϊκού έτους. Για την απόκτηση του Διπλώματος Μεταπτυχιακών Σπουδών απαιτείται η συμπλήρωση 90 πιστωτικών μονάδων (ECTS), η οποία αντιστοιχεί στην επιτυχή εξέταση σε όλα τα μαθήματα του προγράμματος σπουδών και στην επιτυχή εκπόνηση της μεταπτυχιακής διπλωματικής εργασίας.

Περισσότερες πληροφορίες για την οργάνωση των σπουδών στο ΠΜΣ μπορείτε να βρείτε στον Κανονισμό Λειτουργίας του ΠΜΣ. Το ενδεικτικό αναλυτικό πρόγραμμα σπουδών του Π.Μ.Σ. κατά τη διάρκεια των τριών εξαμήνων παρουσιάζεται αναλυτικά σε επόμενες σελίδες του παρόντος οδηγού σπουδών.

Π.Μ.Σ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

Κατά τη διάρκεια των σπουδών, οι μεταπτυχιακοί φοιτητές υποχρεούνται σε παρακολούθηση και επιτυχή εξέταση μεταπτυχιακών μαθημάτων, ερευνητική απασχόληση ή /και πρακτική άσκηση, κ.ά. καθώς και σε εκπόνηση μεταπτυχιακής διπλωματικής εργασίας.

Η διδασκαλία των μαθημάτων γίνεται συνδυαστικά δια ζώσης και με μέσα εξ αποστάσεως εκπαίδευσης, με στόχο την προώθηση ίσων ευκαιριών και (καθολικής) πρόσβασης σε κατηγορίες μεταπτυχιακών φοιτητών/τριών με περιορισμούς συμμετοχής σε (εξ ολοκλήρου) δια ζώσης εκπαιδευτικές δραστηριότητες, όπως εργαζόμενοι, γονείς, μόνιμοι κάτοικοι εκτός της έδρας του Ιδρύματος, άτομα με κινητικές δυσκολίες και άλλοι. Τουλάχιστον 10% των διδακτικών ωρών πραγματοποιούνται δια ζώσης. Η χρήση μεθόδων ασύγχρονης εξ αποστάσεως εκπαίδευσης δεν υπερβαίνει το 25% των πιστωτικών μονάδων του ΠΜΣ.

Διδακτικοί στόχοι

Οι φοιτητές/τριες του Π.Μ.Σ. «Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης », μετά την ολοκλήρωση των σπουδών τους, θα είναι σε θέση να:

- να ανιχνεύουν τις αδυναμίες και τα τρωτά σημεία ασφάλειας και ιδιωτικότητας που παρουσιάζουν ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες, τα οποία είτε από ατύχημα είτε επί σκοπού (εάν γίνουν αντικείμενο εκμετάλλευσης από κακόβουλους) δύναται να οδηγήσουν σε εκδήλωση κυβερνοπεριστατικών, τα οποία έχουν ως αποτέλεσμα είτε την διαρροή δεδομένων είτε την κατάρρευση - προβληματική λειτουργεία συστημάτων και υπηρεσιών.
- να καταγράφουν τις απαιτήσεις ασφάλειας και ιδιωτικότητας που παρουσιάζουν ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες σύμφωνα με το λειτουργικό τους μοντέλο, τα διεθνή πρότυπα, καθώς και το διεθνές κανονιστικό και νομικό πλαίσιο.
- να σχεδιάζουν, να αναλύουν, να υλοποιούν και να εφαρμόζουν διαδικασίες και λύσεις κυβερνοασφάλειας και ιδιωτικότητας σε ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες.
- να υπολογίζουν, να διαχειρίζονται και να μειώνουν τις τιμές του ρίσκου κυβερνοασφάλειας, στο οποίο εκτίθενται ψηφιακά περιβάλλοντα, συστήματα και υπηρεσίες.
- να αντιμετωπίζουν και να διαχειρίζονται, δυναμικά, κυβερνοπεριστασικά με σκοπό να περιορίζουν τον αντίκτυπο και τις επιπτώσεις τους
- να έχουν την ικανότητα να ερμηνεύουν, να αναλύουν και να ενημερώνουν κοινό και επαγγελματίες/επιστήμονες άλλων χώρων για θέματα κυβερνοασφάλειας και προστασίας της ιδιωτικότητας
- να κατανοούν τις επιστημονικές, τεχνολογικές και οικονομικές εξελίξεις που συνδέονται ή επηρεάζουν το χώρο της κυβερνοασφάλειας και ιδιωτικότητας, και να μπορούν να παρεμβαίνουν, όπου απαιτείται, ώστε να πετυχαίνουν τα καθήκοντα που τους έχουν ανατεθεί
- να μπορούν να συνεισφέρουν ουσιαστικά στην πρόοδο της επιστήμης, της τεχνολογίας, της οικονομίας, της ασφάλειας της κοινωνίας και της πατρίδας τους
- να έχουν την ικανότητα να διεξαγάγουν έρευνα υψηλού επιπέδου στο χώρο της ασφάλειας και της ιδιωτικότητας.

Μαθήματα

ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ		
ΜΑΘΗΜΑ	**ΚΑΤΗΓΟΡΙΑ**	**ECTS**
Ασφάλεια Δικτύων (Network Security)	Υ	8,0
Εφαρμοσμένη Κρυπτογραφία και Κρυπτανάλυση (Applied Cryptography and Cryptanalysis)	Υ	7,0
Αποτίμηση Ασφάλειας και Ηθικό Χάκινγκ (Penetration Testing and Ethical Hacking)	Υ	8,0
Διαχείριση Ασφάλειας Πληροφοριών (Information Security management)	Υ	7,0
Σύνολο ECTS:		**30**

ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ		
ΜΑΘΗΜΑ	**ΚΑΤΗΓΟΡΙΑ**	**ECTS**
Ασφάλεια Ασύρματων και Κινητών Δικτύων (Wireless and Mobile Networks Security)	Υ	8,0
Κυβερνοάμυνα και Ψηφιακή Εγκληματολογία (Cyberdefense and Digital Forensics)	Υ	8,0
Νομικό Πλαίσιο Ασφάλειας και Απορρήτου (Legal Framework of Security and Privacy)	Υ	6,5
Προχωρημένα Θέματα Κυβερνοασφάλειας και Τεχνητής Νοημοσύνης (Advanced Cybersecurity Topics and Artificial Intelligence)	Υ	7,5
Σύνολο ECTS:		**30**

Ασφάλεια Δικτύων

Το μάθημα επικεντρώνεται στα ενσύρματα δίκτυα που βασίζονται στην τεχνολογία του διαδικτύου για την επικοινωνία των υπολογιστών και την παροχή διαδικτυακών υπηρεσιών. Παρουσιάζονται, αναλύονται και αξιολογούνται οι απαιτήσεις ασφάλειας (από την πλευρά των χρηστών και των δικτύων), οι τεχνολογίες, οι μηχανισμοί, οι τεχνικές και τα πρωτόκολλα ασφάλειας που προστατεύουν τη λειτουργία των δικτύων και των παρεχόμενων υπηρεσιών, καθώς επίσης και οι επιθέσεις που απειλούν τα συστήματα αυτά. Τέλος, επισημαίνονται τα ανοιχτά θέματα της περιοχής που αποτελούν αντικείμενο έρευνας.

A **Εξάμηνο**

8 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Ασκήσεις, Παρουσιάσεις, Γραπτή Εξέταση

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να καθορίσουν τις απαιτήσεις ασφάλειας ενός δικτυακού συστήματος.
- Να αναλύσουν τις πιθανές απειλές/κινδύνους που ενδέχεται να επηρεάσουν τη λειτουργία, αποτελεσματικότητα, αποδοτικότητα και ιδιωτικότητα ενός δικτυακού συστήματος.
- Να σχεδιάσουν μηχανισμούς και πρωτόκολλα ασφάλειας που ικανοποιούν καλά προσδιορισμένες απαιτήσεις και προστατεύουν από συγκεκριμένες απειλές.
- Να αξιολογήσουν την αποτελεσματικότητα και αποδοτικότητα μιας αρχιτεκτονικής ασφάλειας δικτύου αναγνωρίζοντας τις πιθανές αδυναμίες και περιορισμούς.
- Να γνωρίζουν τις τρέχουσες τάσεις της έρευνας και να εκτιμήσουν την επίδραση που αυτές μπορεί να έχουν στο χώρο τα επόμενα χρόνια.

Διδάσκων

Καθηγητής Χρήστος Ξενάκης

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC101

Ενδεικτική Βιβλιογραφία

- Willam, Stallings. Cryptography and Network Security: Principles and Practice (Global Edition-). Pearson Education, 2022.
- Orzach, Yoram, and Deepanshu Khanna. Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd, 2022.
- Perlman, Radia, Charlie Kaufman, and Mike Speciner. Network security: private communication in a public world. Pearson Education, 2016.
- Σημειώσεις διδάσκοντα.

Εφαρμοσμένη Κρυπτογραφία και Κρυπτανάλυση

Το μάθημα εισάγει τους φοιτητές στον κόσμο της κρυπτογραφίας, προσφέροντας ένα σφαιρικό εισαγωγικό υπόβαθρο στην τέχνη και την επιστήμη αυτού του εξειδικευμένου πεδίου. Καλύπτει εκτενώς τους βασικούς τύπους κρυπτογραφικών μηχανισμών και πρωτοκόλλων, παρουσιάζοντας μια ποικιλία αλγορίθμων και αναλύοντας τους. Επιπλέον, εξηγεί πώς οι διάφοροι μηχανισμοί κρυπτογράφησης χρησιμοποιούνται στην πράξη, ενώ προβαίνει σε μια λεπτομερή ανάλυση της σχέσης μεταξύ της απόδοσης υλοποίησης και της ασφάλειας για διάφορα είδη αλγορίθμων. Με αυτόν τον τρόπο, παρέχει στους φοιτητές μια ισχυρή βάση για την κατανόηση και την αξιολόγηση των κρυπτογραφικών μεθόδων στο ευρύτερο πλαίσιο της πληροφορικής και των τηλεπικοινωνιών.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να εξηγήσουν ακριβώς το ρόλο και τη σημασία της κρυπτογραφίας.
- Να προσδιορίσουν τα όρια της κρυπτογραφίας.
- Να κατανοήσουν τις διαφορές μεταξύ των διαφόρων τύπων κρυπτογραφικών μηχανισμών και κριτικά να συγκρίνουν τις ιδιότητές τους.
- Να επιλέξουν τον πιο κατάλληλο μηχανισμό κρυπτογράφησης ως προς τις επιδόσεις και την ικανοποίηση των καθορισμένων απαιτήσεων ασφάλειας.
- Να γνωρίζουν τις τρέχουσες τάσεις της έρευνας και να εκτιμήσουν την επίδραση που αυτές μπορεί να έχουν στο χώρο τα επόμενα χρόνια.

Διδάσκοντες

Αναπλ. Καθ.Παναγιώτης Ρυζομυλιώτης

Καθηγητής Νικήτας Μαρίνος Σγούρος

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC103/

Ενδεικτική Βιβλιογραφία

- K. M. Martin. Everyday Cryptography. Oxford University Press.
- J. Katz, Y. Lindell. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall/CRC Cryptography and Network Security Series.
- A. Menezes, P. Van Oorschot and S. Vanstone. The Handbook of Applied Cryptography. CRC Press.
- Σημειώσεις διδάσκοντα.

A Εξάμηνο

7 Πιστωτικές Μονάδες

3 Εβδομαδιαίες Ώρες Διδασκαλίας

Αξιολόγηση

Ασκήσεις, Παρουσίαση, Γραπτή Εξέταση.

Αποτίμηση Ασφάλειας και Ηθικό Χάκινγκ

Το μάθημα προσφέρει πρακτική εμπειρία πάνω στην διεξαγωγή αποτίμησης ασφάλειας και εκμετάλλευση ευπαθειών λογισμικού. Οι φοιτητές θα μάθουν πώς να πραγματοποιούν αποτίμηση ασφάλειας σε πληροφοριακά συστήματα, χρησιμοποιώντας τεχνικές συλλογής πληροφοριών για την αναγνώριση και απαρίθμηση στόχων που έχουν διάφορα λειτουργικά συστήματα και υπηρεσίες. Οι φοιτητές επίσης θα εξασκηθούν σε εργαστηριακές ασκήσεις, με σκοπό να αποκτήσουν πρακτική εμπειρία με χρήση αυτοματοποιημένων εργαλείων όπως το Metasploit αλλά και χειροκίνητα με την ανάλυση, διόρθωση και τροποποίηση του κώδικα εκμετάλλευσης αδυναμιών.

A **Εξάμηνο**

8 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Εργαστηριακή Άσκηση, Εξέταση Πολλαπλής Επιλογής, Γραπτή Εργασία.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να κατανοούν τη μεθοδολογία της αποτίμησης και να διεξάγουν αποτίμηση ασφάλειας σε βάθος και πλάτος (πχ. σε διαδικτυακές εφαρμογές).
- Να έχουν αντίληψη τεχνικών χάκινγκ, εμπειρία σε διάφορα εργαλεία χάκινγκ ανοικτού κώδικα (π.χ., Nmap, Metasploit) και να μπορούν να δημιουργούν τα δικά τους εργαλεία.
- Να κατανοούν την έννοια της υπερχείλισης μνήμης.
- Να κατανοούν διάφορες ευπάθειες στη γλώσσα προγραμματισμού C/C++
- Κατανοούν την έννοια των shellcodes και της εκτέλεσης απομακρυσμένου κώδικα καθώς και να γράφουν shellcodes.
- Αναλύουν και αξιολογούν τον πηγαίο κώδικα για να βρουν ευπάθειες και να τις εκμεταλλευτούν.

Διδάσκων

Επικ. Καθηγητής Χριστόφορος Νταντογιάν

Δρ Ευάγγελος Δραγώνας

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC102/

Ενδεικτική Βιβλιογραφία

- Hickey, Matthew, and Jennifer Arcuri. Hands on Hacking: Become an Expert at Next Gen Penetration Testing and Purple Teaming.
- John Wiley & Sons, 2020. Wiley Jon Erickson (2008): Hacking, The Art of Exploitation, 2nd Edition. No Starch Press.Course Notes.
- Hoffman, Andrew. Web Application security: exploitation and countermeasures for modern web applications. O'Reilly Media, 2020.
- Rahalkar, Sagar. Metasploit 5.0 for Beginners: Perform penetration testing to secure your IT environment against threats and vulnerabilities. Packt Publishing Ltd, 2020
- Σημειώσεις διδάσκοντα.

Διαχείριση Ασφάλειας Πληροφοριών

Το μάθημα εξετάζει τον ορολογικό και τις αρχές της Ασφάλειας Συστημάτων Πληροφοριών και Επικοινωνίας. Διερευνά την ανάγκη και τις επιστημονικές βάσεις της 'Ανάλυσης Κινδύνου', επικεντρώνοντας σε βέλτιστες πρακτικές για τη Διαχείριση Κινδύνων και τον εντοπισμό κατάλληλων μέτρων ασφαλείας. Παρέχεται λεπτομερής παρουσίαση της Μεθόδου Ανάλυσης και Διαχείρισης Κινδύνων CRAMM. Το πρόγραμμα σπουδών καλύπτει μηχανισμούς Ταυτοποίησης και Πιστοποίησης, μηχανισμούς Ελέγχου Πρόσβασης, αρχές, εναλλακτικές προσεγγίσεις και απαιτούμενα χαρακτηριστικά των Πολιτικών Ασφαλείας.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να κατανοήσουν με λεπτομέρεια τις βασικές έννοιες της επιστημονικής περιοχής της “Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων”.
- Να εφαρμόσουν μια μεθοδολογία Ανάλυσης και Διαχείρισης Επικινδυνότητας.
- Να κατανοήσουν τη δομή και τους στόχους της Πολιτικής Ασφάλειας ενός οργανισμού.
- Να κατανοήσουν τους μηχανισμούς ταυτοποίησης, αυθεντικοποίησης και ελέγχου προσπέλασης.
- Να αξιολογήσουν την ευχρηστία ενός προϊόντος ασφάλειας.
- Να εκτιμήσουν τις συνέπειες των κινδύνων που αντιμετωπίζουν στον κυβερνοχώρο.

Διδάσκοντες

Καθηγητής Κωσταντίνος Λαμπρινουδάκης

Καθηγητής Στέφανος Γκρίτζαλης

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC104

Ενδεικτική Βιβλιογραφία

- “Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο”, Στέφανος Γκρίτζαλης Σωκράτης Κάτσικας Κωνσταντίνος Λαμπρινουδάκης, Εκδόσεις Νέων Τεχνολογιών, ISBN: 978-960-578-064-7, 2021
- Michael E. Whitman, Herbert J. Mattord, Management of Information Security, 6th edition, Cengage Learning, 2018
- Λαμπρινουδάκης Κ. & Μήτρου Λ. & Γκρίτζαλης Σ. & Κάτσικας Σ. (2009): Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα, Εκδόσεις Παπασωτηρίου.

- Επιστημονικές δημοσιεύσεις, σημειώσεις ή/και βιβλία.

A **Εξάμηνο**

7 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Ασκήσεις, Προφορική Εξέταση.

Ασφάλεια Ασύρματων και Κινητών Δικτύων

Το μάθημα παρέχει μια ολοκληρωμένη εξερεύνηση της ασφάλειας κινητών και ασύρματων συστημάτων, καλύπτοντας θέματα όπως η ασφάλεια του διαδικτύου κινητής τηλεφωνίας, οι απαιτήσεις ασφαλείας και οι προκλήσεις που σχετίζονται. Επικεντρώνεται στην ασφάλεια των Ασύρματων Τοπικών Δικτύων (WLANs), εξετάζοντας τα μέτρα ασφαλείας τους, τις σημαντικές ευπάθειες και τις πιθανές επιθέσεις. Το πρόγραμμα σπουδών περιλαμβάνει μια λεπτομερή μελέτη του προτύπου ασφαλείας IEEE 802.11i, καλύπτοντας τους βασικούς μηχανισμούς και τις υπηρεσίες ασφαλείας του. Το μάθημα εξετάζει επίσης θέματα ασφαλείας σε ασύρματα ανοργάνωτα δίκτυα, συμπεριλαμβανομένων των δικτύων ad hoc και του Διαδικτύου των πραγμάτων (IoT). Επιπρόσθετα, το μάθημα εξετάζει τα χαρακτηριστικά ασφαλείας των δημοφιλών λειτουργικών συστημάτων κινητών.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να καθορίσουν τις απαιτήσεις ασφάλειας ενός ασύρματου/κινητού δικτυακού συστήματος.
- Να αναλύσουν τις πιθανές απειλές/κινδύνους που ενδέχεται να επηρεάσουν τη λειτουργία, αποτελεσματικότητα, αποδοτικότητα και ιδιωτικότητα ενός ασύρματου δικτυακού συστήματος.
- Να σχεδιάσουν μηχανισμούς και πρωτόκολλα ασφάλειας που ικανοποιούν καλά προσδιορισμένες απαιτήσεις και προστατεύουν από συγκεκριμένες απειλές.
- Να αξιολογήσουν την αποτελεσματικότητα και αποδοτικότητα μιας αρχιτεκτονικής ασφάλειας ασύρματου δικτύου αναγνωρίζοντας τις πιθανές αδυναμίες και περιορισμούς.

Διδάσκων

Καθηγητής Χρήστος Ξενάκης

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC101

Ενδεικτική Βιβλιογραφία

- Jim Doherty, Wireless and Mobile Device Security, 2nd Edition, Jones & Bartlett Learning, April 2021
- Sabhyata Soni, 5G Cyber Risks and Mitigation 1st Edition, CRC Press, April 2023
- Σημειώσεις διδάσκοντα.

B **Εξάμηνο**

8 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Ασκήσεις, Παρουσιάσεις, Γραπτή Εξέταση.

Κυβερνοάμυνα και Ψηφιακή Εγκληματολογία

Το μάθημα «Κυβερνοάμυνα και Ψηφιακή Εγκληματολογία» εισάγει και αναλύει τους βασικότερους μηχανισμούς ανίχνευσης και αναγνώρισης επιθέσεων. Οι φοιτητές θα εξασκηθούν στη διαχείριση εισβολών και στην αποτελεσματική και έγκαιρη αντιμετώπιση των επιθέσεων. Το συγκεκριμένο μάθημα εξετάζει την αμυντική κυβερνοασφάλεια που επιτρέπει στους φοιτητές κατά την επιτυχή ολοκλήρωση του να είναι σε θέση να προστατεύσουν τα πληροφοριακά συστήματα και να διαχειριστούν περιστατικά ασφάλειας υπό πραγματικές συνθήκες.

B **Εξάμηνο**

8 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες**

Αξιολόγηση

Εργαστηριακή Άσκηση, Εξέταση με Πολλαπλή Επιλογή, Γραπτή Εργασία.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να ελέγξουν την ασφάλεια λογισμικού με αυτοματοποιημένα εργαλεία αλλά και χειροκίνητα.
- Να κατανοήσουν αρχιτεκτονικές για συστήματα Διαχείρισης πληροφοριών ασφαλείας και συμβάντων (SIEM).
- Να εγκαταστήσουν και να παραμετοποιήσουν SIEM.
- Να σχεδιάσουν και να υλοποιήσουν δείκτες εισβολής και υπογραφές για συστήματα ανίχνευσης εισβολών.
- Να κατανοήσουν το πλαίσιο ATT&CK και πώς εφαρμόζεται για το εντοπισμό απειλών.
- Να μελετήσουν δικτυακή κίνηση για ευρήματα.
- Να κατανοήσουν τη βασική θεωρία και τις τεχνικές των κακόβουλων λογισμικών και να διεξάγουν στατική και δυναμική ανάλυση.
- Να υλοποιήσουν στρατηγικές για αναφορά συμβάντος (Incident Response playbooks).
- Να μελετήσουν προχωρημένα θέματα ψηφιακής εγκληματολογίας στις τεχνολογίες του διαδικτύου των Πραγμάτων και Νεφουπολογιστικής.
- Ερευνήσουν σενάρια επιθέσεων και να αναχαιτήσουν τις κυβερνοεπιθέσεις για την ανάκτηση του πληροφοριακού συστήματος.

Διδάσκων

ΕΕπικ. Καθηγ.Χριστόφορος Νταντογιάν

Δρ Ευάγγελος Δραγώνας

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC

Ενδεικτική Βιβλιογραφία

- Joshua Picolet, Operator Handbook: Red Team + OSINT + Blue Team Reference (2020), Independently published
- Kohnfelder, Loren. Designing Secure Software (2021): A Guide for Developers. No Starch.
- Σημειώσεις διδάσκοντα.

Νομικό Πλαίσιο Ασφάλειας και Απορρήτου

Το μάθημα παρέχει μια εισαγωγή στο Δίκαιο της Κοινωνίας της Πληροφορίας, καλύπτοντας το περιβάλλον πλαίσιο, τις βασικές έννοιες, τις αρχές και τα βασικά θεσμικά όργανα που διαμορφώνουν τα νομικά πλαίσια. Εξετάζει τις κρίσιμες πτυχές της ασφάλειας, της εμπιστευτικότητας/μυστικότητας, της ιδιωτικότητας και της προστασίας δεδομένων, ερευνώντας τις νομικές διαστάσεις της ασφάλειας πληροφοριών και συστημάτων. Το πρόγραμμα σπουδών προσφέρει μια σφαιρική εξέταση του Δικαίου Προστασίας Δεδομένων εντός του Ευρωπαϊκού και Εθνικού Ρυθμιστικού Πλαισίου, επισημαίνοντας τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας, τις Αρχές του Σχεδιασμού και της Προεπιλογής της Ιδιωτικότητας.

B **Εξάμηνο**

6,5 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Γραπτή Εργασία, Παρουσιάσεις, Γραπτή Εξέταση.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Να αποκτήσουν εποπτεία των νομικών ζητημάτων που τίθενται σε σχέση με τις ΠΕ και τις εφαρμογές τους.
- Να αποκτήσουν γνώση των βασικών ρυθμιστικών κανόνων και αρχών που συγκροτούν το κανονιστικό πλαίσιο.
- Να εντοπίζουν τα βασικά ζητήματα δικαίου που σχετίζονται με την ασφάλεια ενός πληροφοριακού συστήματος ώστε να αναζητούν εφαρμογές και λύσεις που είναι σύμφωνες με το κανονιστικό πλαίσιο.
- Να εντάξουν τις γνώσεις που αποκομίζουν από τον βασικό κορμό των σπουδών τους στις ΤΠΕ σε ένα ευρύτερο κοινωνικό, οικονομικό και θεσμικό πλαίσιο ώστε να αποκτήσουν μία σφαιρική θεώρηση των ζητημάτων που καλούνται να αντιμετωπίσουν.

Διδάσκοντες

Καθηγήτρια Λίλιαν Μήτρου

Καθηγητής Κωνσταντίνος Λαμπρινουδάκης

Καθηγητής Στέφανος Γκρίτζαλης

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC107

Ενδεικτική Βιβλιογραφία

- Μήτρου Λ., Πισκοπάνη Α.Μ., Τάσσης Σ., Καρύδα Μ.-Κοκολάκης Σ., Facebook, Blogs και Δικαιώματα (2013)
- Λαμπρινουδάκης Κ. & Μήτρου Λ. & Γκρίτζαλης Σ. & Κάτσικας Σ. (2010): Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα
- Μήτρου Λ. (2004): Προστασία Προσωπικών Δεδομένων σε Σ. Κάτσικας/Δ.Γκρίτζαλης/Σ. Γκρίτζαλης (επιμ.), «Ασφάλεια Πληροφοριακών Συστημάτων».
- Συνοδινού Ε.Τ, Πνευματική Ιδιοκτησία και Νέες Τεχνολογίες (2008)
- Καλλινίκου Δ. (2005): Προστασία της πνευματικής ιδιοκτησίας στο Διαδίκτυο.
- Καράκωστας Ι. (2003): Δίκαιο και Internet.
- Μανιάτης Α. (2010): Δίκαιο Πληροφορικής και Τηλεπικοινωνιών.
- Μήτρου Λ. (2002): Το δίκαιο στην Κοινωνία της Πληροφορίας.
- Παπαχρίστου Θ., Βιδάλης Τ., Μήτρου Λ., Τάκης, Α. (2006): Το δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας.
- Σημειώσεις διδάσκουσας

Προχωρημένα Θέματα Κυβερνοασφάλειας και Τεχνητής Νοημοσύνης

Το μάθημα παρέχει εκτενή εισαγωγή στον χώρο του cloud computing και της ασφάλειας, εστιάζοντας στις τεχνολογίες Docker και Kubernetes για τη δημιουργία και διαχείριση εφαρμογών σε περιβάλλοντα containers. Περιλαμβάνει ανάλυση της Docker και ασφάλεια του Kubernetes, ενώ επεκτείνει το πεδίο του στην κυβερνοασφάλεια, με ενότητες για επιθέσεις στο Active Directory. Οι φοιτητές εξερευνούν μεθοδολογίες εκπαίδευσης στην τεχνητή νοημοσύνη και την υλοποίηση μοντέλων. Επιπλέον, εξετάζονται εφαρμογές τεχνητής νοημοσύνης στην κυβερνοασφάλεια. Το μάθημα καταλήγει με ανάλυση του blockchain και των έξυπνων συμβολαίων, εξετάζοντας τεχνικές επιθέσεων σε αυτά. Προσφέρει ισορροπημένη προσέγγιση μεταξύ θεωρητικών εννοιών και πρακτικής εμπειρίας, ετοιμάζοντας τους φοιτητές για προκλήσεις στην κυβερνοασφάλεια.

B **Εξάμηνο**

7,5 **Πιστωτικές Μονάδες**

3 **Εβδομαδιαίες Ώρες Διδασκαλίας**

Αξιολόγηση

Ασκήσεις, Γραπτή Εξέταση.

Στόχος

Με την ολοκλήρωση των σχετικών διαλέξεων, αναμένεται οι φοιτητές/τριες να είναι σε θέση:

- Κατανόηση αρχών ασφάλειας του Cloud computing.
- Απόκτηση γνώσης των τεχνολογιών εικονικοποίησης και της ασφάλειάς τους.
- Κατανόηση πώς η Τεχνητή Νοημοσύνη μπορεί να εφαρμοστεί στον εντοπισμό κακόβουλων δραστηριοτήτων (π.χ., malware, επιθέσεις δικτύου).
- Αναγνώριση αδυναμιών σε μοντέλα Τεχνητής Νοημοσύνης και ενίσχυση της ανθεκτικότητάς τους.
- Διαχείριση Ασφαλείας του Active Directory.
- Κατανόηση επιθέσεων στο Active Directory και αντιμετώπιση αυτών.
- Κατανόηση λειτουργίας της τεχνολογίας blockchain.
- Υλοποίηση έξυπνων συμβολαίων και των αντίστοιχων ασφαλείας (επιθέσεις και προστασία σε έξυπνα συμβόλαια).

Διδάσκων

Καθηγητής Χρήστος Ξενάκης
Δρ. Απόστολος Ζάρρας

Σελίδα Μαθήματος

https://lefkippos.ds.unipi.gr/courses/SEC

Ενδεικτική Βιβλιογραφία

- Chris Dotson (2019), Practical Cloud Security: A Guide for secure Design and Deployment
- Liz Rice (2020), Container Security: Fundamental Technology Concepts that Protect Containerized Applications
- Muhammad Nafees (2022), AD Attack Vectors: Top Active Directory Vulnerabilities
- Fei Hu, Xiali Hei (2023), AI, Machine Learning and Deep Learning: A Security Perspective
- Reza Montasari (2022), Artificial Intelligence and National Security
- Rajneesh Gupta (2018), Hands-On Cybersecurity with Blockchain
- Hasan YILDIZ, Solididty Academy (2023), Smart Contract Security Fundamentals, Vulnerabilities and Best Practices
- Σημειώσεις διδάσκοντα.

Διπλωματική Εργασία

Στο Γ’ εξάμηνο του Προγράμματος προβλέπεται η εκπόνηση μεταπτυχιακής διπλωματικής εργασίας (30 ECTS). Ο υποψήφιος καταθέτει αίτηση, στην οποία αναγράφεται ο προτεινόμενος τίτλος της διπλωματικής εργασίας, ο προτεινόμενος επιβλέπων. Η Συντονιστική Επιτροπή, εισηγείται στη Συνέλευση την τριμελή εξεταστική επιτροπή και τον επιβλέποντα. Η Συνέλευση συγκροτεί την τριμελή εξεταστική επιτροπή για την έγκριση της εργασίας και ορίζει τον επιβλέποντα.

Η γλώσσα συγγραφής της μεταπτυχιακής διπλωματικής εργασίας μπορεί να είναι στην ελληνική ή στην αγγλική γλώσσα.

Οι μεταπτυχιακές διπλωματικές εργασίες εφόσον εγκριθούν από την εξεταστική επιτροπή, αναρτώνται από τον ίδιο τον φοιτητή, στο Ιδρυματικό Αποθετήριο ΔΙΩΝΗ της Βιβλιοθήκης του Πανεπιστημίου Πειραιώς.

Διδάσκοντες

Χρήστος Ξενάκης

Ο Καθ. Χρήστος Ξενάκης ολοκλήρωσε τις σπουδές του στην Πληροφορική το 1993, και μεταπτυχιακά (M.Sc.) το 1996 στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Αθηνών. Το 2004 έλαβε το Διδακτορικό δίπλωμα (Ph.D) από το Πανεπιστήμιο Αθηνών (Τμήμα Πληροφορικής και Τηλεπικοινωνιών). Το διάστημα 1998 – 2001 εργάστηκε ως μηχανικός τηλεπικοινωνιών. Από το 1996 έως 2007 ήταν μέλος του Εργαστηρίου Δικτύων Επικοινωνιών του Τμήματος Πληροφορικής και Τηλεπικοινωνιών (Πανεπιστήμιο Αθηνών).

Από το 2007 ανήκει στο Διδακτικό Ερευνητικό Προσωπικό του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, όπου σήμερα είναι Καθηγητής.

Παράλληλα, είναι μέλος του Εργαστηρίου Ασφάλειας Συστημάτων του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς και διευθυντής του μεταπτυχιακού προγράμματος «Ασφάλεια Ψηφιακών Συστημάτων». Συμμετείχε ενεργά σε περισσότερα από 30 Ευρωπαϊκά (ACTS, ESPRIT, IST, AAL, DGHOME, Marie Curie, Horizon2020) και Εθνικά ερευνητικά προγράμματα. Είναι ο συντονιστής των έργων CUREX, SealedGRID, INCOGNITO και SECONDO που χρηματοδοτούνται από την Ευρωπαϊκή Επιτροπή (H2020), ενώ διατέλεσε συντονιστής του προγράμματος ReCRED (H2020) και είχε την επιστημονική/τεχνική διεύθυνση του προγράμματος UINFC2 που χρηματοδοτήθηκε από την DGHOME/ISEC.

Είναι μέλος της συντονιστικής επιτροπής του Ευρωπαϊκού διαγωνισμού κυβερνο-ασφάλειας (European Cyber Security Challenge) και αρχηγός της Ελληνικής Εθνικής Ομάδας Κυβερνοασφάλειας.
Επίσης, είναι μέλος των συντακτικών ομάδων των επιστημονικών περιοδικών Computers & Security και Computer Communications που εκδίδονται από τον εκδοτικό οίκο Elsevier, καθώς και του περιοδικού IET Information Security που εκδίδεται από το Ινστιτούτο Μηχανικής και Τεχνολογίας. Τα ερευνητικά του ενδιαφέροντα εστιάζουν στο χώρο της ασφάλειας συστημάτων, δικτύων και εφαρμογών.
Τέλος, έχει συνυπογράψει περισσότερες από 90 δημοσιεύσεις σε διεθνή επιστημονικά περιοδικά, κεφάλαια συλλογικών τόμων και συνέδρια.

Κωνσταντίνος Λαμπρινουδάκης

Ο Κωνσταντίνος Λαμπρινουδάκης έχει πτυχίο Ηλεκτρολόγου και Ηλεκτρονικού Μηχανικού από το Πανεπιστήμιο του Salford (1985), Μάστερ (M.Sc.) σε συστήματα αυτομάτου ελέγχου από το Πανεπιστήμιο του Λονδίνου (Imperial College – 1986) και διδακτορικό δίπλωμα (Ph.D.) από το Πανεπιστήμιο του Λονδίνου (Queen Mary and Westfield College – 1991). 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 Διευθυντής του Εργαστηρίου Ασφάλειας Συστημάτων, ενώ στο διάστημα 2015 έως και 2020 διετέλεσε Πρόεδρος του Τμήματος. Από το 2016 είναι τακτικό μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ενώ στο διάστημα 2012 έως και 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. Εδώ και πολλά χρόνια ασχολείται με θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων και τη συμμόρφωση των πληροφοριακών συστημάτων με την Εθνική και Ευρωπαϊκή Νομοθεσία. 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.

Στέφανος Γκρίτζαλης

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 Αναπληρωματικό Μέλος της Εθνικής Επιτροπής για τα Δικαιώματα του Ανθρώπου (ΕΕΔΑ) (08.2022+).

Διετέλεσε Πρύτανης στο Πανεπιστήμιο Αιγαίου (2014-2018).

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 25 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” του Stanford και της Elsevier, περιλαμβάνεται, για μία ακόμη χρονιά, στο 2% των κορυφαίων επιστημόνων σε όλο τον κόσμο, σε σύνολο 195.605 επιστημόνων, 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 329 επιστημονικά άρθρα (146 άρθρα σε διεθνή Επιστημονικά Περιοδικά και 183 σε Πρακτικά Διεθνών Συνεδρίων με έκδοση Πρακτικών).

Διατελεί Area Editor στο κορυφαίο περιοδικό IEEE Communications Surveys and Tutorials (ImpactFactor=35.6 (Clarivate JCR Report), κατετάγη #1 περιοδικό στην Επιστήμη Υπολογιστών και Τηλεπικοινωνιών στον κόσμο για τα έτη 2022, 2021, 2020, 2019, 2018, 2017).

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 9.900 Αναφορές (citations) στο έργο του με h-index=54, i-10 index=168 κατά Google Scholar.

Έχει επιβλέψει την εκπόνηση 17 διδακτορικών διατριβών που έχουν περατωθεί επιτυχώς. Επιπλέον, έχει διατελέσει μέλος επιτροπής αξιολόγησης / εξωτερικός αξιολογητής 60 και πλέον υποψηφίων διδακτόρων στην Ελλάδα, τη Γερμανία, την Ιταλία, την Ισπανία και την Ινδία. Έχει επιβλέψει 90 Μεταπτυχιακές Διπλωματικές Εργασίες και 160 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 (SNSF), 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.

Π.Μ.Σ. Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

Νικήτας-Μαρίνος Σγούρος

Ο Νικήτας-Μαρίνος Σγούρος είναι κάτοχος διδακτορικού διπλώματος από το Πανεπιστήμιο Northwestern, των ΗΠΑ, M.Sc. με διάκριση από το Πανεπιστήμιο του Εδιμβούργου του Ηνωμένου Βασιλείου και διπλώματος Ηλεκτρολόγου Μηχανικού από το ΕΜΠ. Σήμερα είναι καθηγητής στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.Έχει διατελέσει Διευθυντής του ΠΜΣ «Ψηφιακά Συστήματα & Υπηρεσίες» και Αναπληρωτής Πρόεδρος στο Τμήμα. Τα ερευνητικά του ενδιαφέροντα εστιάζονται σε Συστήματα Πολυμέσων, Ευφυή Συστήματα, Τεχνολογίες Ψυχαγωγίας και Ρομποτική. Ο κ. Σγούρος διευθυνει το εργαστήριο Ευφυών Συστημάτων και Τεχνολογιών Πολυμέσων και έχει συμμετάσχει σε πολυάριθμα ερευνητικά και αναπτυξιακά προγράμματα στην Ελλάδα και στην Ευρώπη.

Γεώργιος Βούρος

Ο Καθ. Γεώργιος Βούρος είναι Καθηγητής στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Οι δημοσιευμένες εργασίες του είναι στους τομείς των Expert Systems (έχει αναπτύξει 4 επιτυχημένα συστήματα σε κρίσιμους τομείς κατά την περίοδο 1990-1997), Διαχείριση Γνώσης, Συνεργατικά Συστήματα, Οντολογίες (μηχανική, ευθυγράμμιση, μάθηση οντολογιών και στιγμιότυπων, από διαφορετικές πηγές δεδομένων, εξαγωγή ενοτήτων , αποκεντρωμένη συλλογιστική, ενοποίηση σημασιολογικών δεδομένων), Agents and Multi-Agent Systems (εστίαση σε οργανισμούς και προσαρμογή, ανταλλαγή πληροφοριών, συντονισμός), Ενισχυτική και Μιμητική Μάθηση σε περιβάλλοντα ενός πράκτορα και πολλαπλών πρακτόρων.

Υπηρέτησε/υπηρέτησε ως πρόεδρος προγράμματος, πρόεδρος και μέλος οργανωτικών επιτροπών εθνικών (SETN) και διεθνών συνεδρίων (AAMAS, ECAI, AAAI, IJCAI, ISWC, WI/IA κλπ) και ως μέλος συντονιστικών επιτροπών/συμβουλίων διεθνών συνεδρίων/εργαστηρίων (π.χ. COIN, EUMAS). Έχει δώσει σεμινάρια και βασικές ομιλίες σε συνέδρια και έχει οργανώσει αρκετά εργαστήρια σε γνωστά συνέδρια. Υπηρέτησε/υπηρέτησε ως προσκεκλημένος συντάκτης σε ειδικά τεύχη σε έγκυρα περιοδικά και είναι/ήταν ανώτερος ερευνητής σε χρηματοδοτούμενα από την ΕΕ και εθνικά ερευνητικά προγράμματα (συνολικά 20).

Έχει επιβλέπει 13 διδακτορικούς φοιτητές και επί του παρόντος εποπτεύει 5 διδακτορικούς φοιτητές στους τομείς της μηχανικής μάθησης (κυρίως στην ενισχυτική μάθηση και στη μίμηση).

Εχει διατελέσει 4 φορές στο παρελθόν ως πρόεδρος του Διοικητικού Συμβουλίου της Ελληνικής Εταιρείας Τ.Ν (ΕΕΤΝ , μέλος του EurAI) και επί του παρόντος υπηρετεί ως πρόεδρος αυτού του συμβουλίου (2023-2024).

Είναι ο ιδρυτής και διευθυντής του διοργανικού MSc on AI μεταξύ του Πανεπιστημίου Πειραιώς και του ΕΚΕΦΕ «Δημόκριτος» (2019-σήμερα), και διευθύνει το Εργαστήριο Τεχνητής Νοημοσύνης στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς (2016-σήμερα).

Π.Μ.Σ. Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

Λίλιαν Μήτρου

Η Λίλιαν Μήτρου είναι καθηγήτρια στο Πανεπιστήμιο Αιγαίου. Σπούδασε στη Νομική Σχολή Αθηνών (ΕΚΠΑ) και εκπόνησε τη διδακτορική διατριβή της στη Νομική Σχολή του Πανεπιστημίου της Φρανκφούρτης υπό την εποπτεία του καθηγητή Σ. Σημίτη. Διδάσκει Δίκαιο Προστασίας Προσωπικών Δεδομένων και Δίκαιο της Πλη-ροφορίας/Διαδικτύου στο Τμήμα Μηχανικών και Πληροφοριακών Συστημάτων του Πανεπιστημίου Αιγαίου και ως επισκέπτρια καθηγήτρια στο Οικονομικό Πανεπιστήμιο Αθηνών και στο Πανεπιστήμιο Πειραιά (Προ-γράμματα Μεταπτυχιακών Σπουδών). Διετέλεσε σύμβουλος του π. Πρωθυπουργού Κ. Σημίτη (1996-2004), μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (1999-2003) και από τον Νοέμβριο 2016 είναι μέλος του Εθνικού Συμβουλίου Ραδιοτηλεόρασης. Κατά την Ελληνική Προεδρία του Συμβουλίου της Ευρωπαϊκής Ένωσης (2014) υπήρξε Πρόεδρος της Ομάδας Εργασίας για την προστασία δεδομένων (DAPIX). Έχει διατελέσει μέλος /
πρόεδρος πολλών νομοπαρασκευαστικών επιτροπών με αντικείμενο την προστασία προσωπικών δεδομένων, τις ηλεκτρονικές επικοινωνίες, την ασφάλεια υποδομών-δικτύων, την ηλεκτρονική διακυβέρνηση κ.α. Ασκεί συμβουλευτική δικηγορία και έχει συμμετάσχει σε πολλά ερευνητικά έργα σε διε-θνές και εθνικό επίπεδο. Έχει γράψει βιβλία και επιστημονικά άρθρα στα Ελληνικά, Αγγλικά και Γερμανικά.

Παναγιώτης Ριζομυλιώτης

Ο Δρ Παναγιώτης Ριζομηλιώτης γεννήθηκε στην Αθήνα. Έλαβε πτυχίο B.Sc. πτυχίο Πληροφορικής με άριστα το 1997 και M.Sc. το 1999 από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Είναι κάτοχος Ph.D. στη Σχεδίαση Ψευδοτυχαίων Ακολουθιών με Εφαρμογές Κρυπτογραφίας και Επικοινωνιών από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Το 2005, ο Παναγιώτης εντάχθηκε στην ομάδα COSIC στο Katholieke Universiteit Leuven και εργάστηκε ως μεταδιδακτορικός ερευνητής μέχρι το 2007. Η έρευνά του χρηματοδοτήθηκε, τον πρώτο χρόνο, από την υποτροφία Marie Curie που έλαβε και, τον δεύτερο χρόνο, από το Flemish Fund for Scientific Έρευνα (F.W.O.-Vlaanderen). Το 2010 εκλέχτηκε Επίκουρος Καθηγητής στο Πανεπιστήμιο Αιγαίου και σήμερα είναι Αναπληρωτής Καθηγητής στο Χαροκόπειο Πανεπιστήμιο. Τα κύρια ερευνητικά του ενδιαφέροντα περιλαμβάνουν εφαρμοσμένη κρυπτογραφία, σχεδιασμό ψευδοτυχαίων ακολουθιών, θεωρία πληροφοριών, ασφάλεια συστημάτων και ιδιωτικότητα.

Π.Μ.Σ. Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

Χριστόφορος Νταντογιάν

Ο Δρ. Χριστόφορος Νταντογιάν ολοκλήρωσε τις σπουδές του στην Πληροφορική και Τηλεπικοινωνίες το 2004, και μεταπτυχιακά (M.Sc.) το 2006 στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Αθηνών.

Το 2009 έλαβε το Διδακτορικό δίπλωμα (Ph.D) από το Πανεπιστήμιο Αθηνών (Τμήμα Πληροφορικής και Τηλεπικοινωνιών). Είναι Επίκουρος Καθηγητής στο Τμήμα Πληροφορικής του Ιόνιου Πανεπιστημίου. Συμμετείχε ενεργά σε πολυάριθμα Ευρωπαϊκά ερευνητικά προγράμματα. Τα ερευνητικά του ενδιαφέροντα εστιάζουν στο χώρο της ασφάλειας πληροφοριακών συστημάτων και δικτύων.

Δρ. Απόστολος Ζάρρας

Ο Δρ. Απόστολης Ζαρράς είναι συνεργαζόμενος ερευνητής στο Πανεπιστήμιο του Πειραιά. Προηγουμένως, υπήρξε επίκουρος καθηγητής στο Πανεπιστήμιο της Ντελφτ και το Πανεπιστήμιο του Μάαστριχτ, και πριν από αυτό, μεταδιδακτορικός ερευνητής στο Τεχνικό Πανεπιστήμιο του Μονάχου.

Έλαβε το διδακτορικό του δίπλωμα στην Ασφάλεια Πληροφοριακών Τεχνολογιών από το Πανεπιστήμιο του Μπόχουμ. Διαθέτει επίσης μεταπτυχιακό και προπτυχιακό δίπλωμα στην Επιστήμη Υπολογιστών από το Πανεπιστήμιο της Κρήτης.

Τα ερευνητικά του ενδιαφέροντα επικεντρώνονται κυρίως γύρω από την ασφάλεια των συστημάτων, τις δικτυακές τεχνολογίες και του διαδυκτίου. Συνολικά, το έργο του είναι αφιερωμένο στην προώθηση του τομέα της πληροφορικής ασφαλείας και της προστασίας των χρηστών και των συστημάτων από πιθανούς κινδύνους.

Π.Μ.Σ. Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

Δρ. Ευάγγελος Δραγώνας

Ο Βαγγέλης Δραγώνας είναι μεταδιδακτορικός ερευνητής του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, στον τομέα της Ψηφιακής Εγκληματολογίας. Είναι κάτοχος πτυχίου Πληροφορικής από το Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, μεταπτυχιακού διπλώματος ειδίκευσης στην Ασφάλεια Ψηφιακών Συστημάτων από το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς και διδακτορικού διπλώματος από το ίδιο τμήμα με αντικείμενο την εφαρμογή της Ψηφιακής Εγκληματολογίας στο Διαδίκτυο των Πραγμάτων (ΔτΠ). Κατέχει δεκαετή εργασιακή εμπειρία στον τομέα της Ψηφιακής Εγκληματολογίας. Έχει παρουσιάσει την έρευνα του σε διεθνή συνέδρια όπως τα SANS DFIR Summit και DFRWS-USA. Έχει συμμετάσχει σε ευρωπαϊκά ερευνητικά έργα. Διατηρεί τις ακόλουθες πιστοποιήσεις στον εν λόγω τομέα: Certified Forensic Computer Examiner (CFCE), Magnet Certified Forensics Examiner (MCFE) και Magnet Certified MAC Examiner (MCME). Ακόμη, είναι πιστοποιημένος ISMS Auditor κατά ISO 27001:2013. Τα τρέχοντα ερευνητικά του ενδιαφέροντα επικεντρώνονται στη μελέτη της Τεχνητής Νοημοσύνης (ΤΝ) υπό το πρίσμα της Ψηφιακής Εγκληματολογίας και την εφαρμογή της σε συσκευές του ΔτΠ. Συμμετέχει ως κριτής σε διεθνή επιστημονικά περιοδικά και συνέδρια. Το δημοσιευμένο του έργο εστιάζει στην εφαρμοσμένη Ψηφιακή Εγκληματολογία.

Επικοινωνία

	Τηλέφωνο	e-mail
Γραμματεία ΠΜΣ **Αλεξάνδρα Δρίτσα**	210 414 2773	adritsa@unipi.gr
Διευθυντής Π.Μ.Σ. **Καθηγητής Χρήστος Ξενάκης**	210 414 2776	xenakis@unipi.gr
Ακαδημαϊκή Γραμματεία	210 414 2235 210 414 2426 210 414 2373 210 414 2076	gramds@unipi.gr
Ιστοσελίδα	**https://masters.ds.unipi.gr/security/**	