3. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΟΥ ΜΕΛΛΟΝΤΟΣ

ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ		**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	1ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Κυβερνοασφάλεια στο Διαδίκτυο του Μέλλοντος		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ *σε περίπτωση που οι πιστωτικές μονάδες απονέμονται σε διακριτά μέρη του μαθήματος π.χ. Διαλέξεις, Εργαστηριακές Ασκήσεις κ.λπ. Αν οι πιστωτικές μονάδες απονέμονται ενιαία για το σύνολο του μαθήματος αναγράψτε τις εβδομαδιαίες ώρες διδασκαλίας και το σύνολο των πιστωτικών μονάδων*	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις	3	8

ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα περιλαμβάνει τις παρακάτω διδακτικές ενότητες:

1. Θεμελιώδεις έννοιες

- Επιτιθέμενοι και ειδικές κατηγορίες (εσωτερικά επιτιθέμενοι)
- Ευπάθειες Εφαρμογών και Συστημάτων
- Είδη Απειλών και Μέθοδοι Επίθεσης
- Υπηρεσίες και Μηχανισμοί Ασφάλειας (Έλεγχοι)

2. Κρυπτογραφία

- Κλασσικά Κρυπτοσυστήματα (Αντικατάστασης, Μετάθεσης, DES, AES)
- Κρυπτογράφηση δημοσίου κλειδιού (Diffie-Hellman, RSA)
- Ψηφιακές Υπογραφές
- PKI και ψηφιακά πιστοποιητικά
- Stream και Block Ciphers
- Αλγόριθμοι Hash
- Κρυπτογραφικά πρωτόκολλα δικτύων (Transport Layer Security - TLS)

3. Προστασία Λειτουργικών Συστημάτων

- Αντικείμενα και μέθοδοι προστασίας
- Προστασία μνήμης και διευθυνσιοδότησης
- Μηχανισμοί Ελέγχου Πρόσβασης
- Μηχανισμοί προστασίας αρχείων
- Μηχανισμοί Αυθεντικοποίησης

4. Ασφάλεια Δικτύων και Κατανεμημένων Συστημάτων

- Απειλές στα δίκτυα
- Μηχανισμοί Ασφάλειας (έλεγχοι) στα δίκτυα
- Πρωτόκολλα και Πρότυπα Ασφάλειας στο Διαδίκτυο
- Ασφάλεια Ασύρματων Δικτύων
- Ασφάλεια σε δίκτυα 5G
- Firewalls

5. Ασφάλεια στο Cloud Computing

- Ασφάλεια Δεδομένων στο cloud
- Διαχείριση ταυτοτήτων και πρόσβασης (Identity and Access Management -IAM)
- Ανάκτηση καταστροφής και σχεδιασμός συνέχισης επιχειρήσεων στο cloud (DR/BCP)
- Ανίχνευση εισβολών και incident response στο cloud

6. Στοιχεία και Ιδιότητες Ασφαλών και Έμπιστων Κατανεμημένων Συστημάτων

- Τεχνικές διασφάλισης
- Έμπιστο Σύστημα
- Κλάσεις, Ευπάθειες, και Επιθέσεις Κατανεμημένων Συστημάτων
- Ασφάλεια Κατανεμημένων Συστημάτων
- Έλεγχος πρόσβασης/αποδοχής και Διαχείριση ID
- Ασφάλεια Δεδομένων
- Επιθέσεις σε συστήματα P2P

7. Τεχνολογία Blockchain σε Κατανεμημένα Έμπιστα Συστήματα

- Κατανεμημένο (peer-based)
- Αμετάβλητο
- Κρυπτογραφική Ταυτότητα
- Consensus Algorithms (POW, POS, Next-gen: PBFT)
- Τομείς Εφαρμογής του Blockchain
- Το Πρόβλημα των Βυζαντινών Στρατηγών
- Λύση στο BGP με Blockchain
- Data Base στο Blockchain, Block, Δομή Block, Hash, Minor, Transaction, Consensus mechanism
- Δημόσιο (Public) και Ιδιωτικό (Private) Blockchain

8. Ασφάλεια και Ιδιωτικότητα στο Blockchain

- Επιθέσεις στο Blockchain
- Στοιχεία CAP στο Blockchain
- Στοιχεία Ασφάλειας και Μυστικότητας του Blockchain
- Απαιτήσεις Ασφάλειας και Μυστικότητας για online συναλλαγές στο Blockchain
- Αντοχή σε Επιθέσεις (DDoS, Double-Spending, Majority [51%] Consensus Attack, Ψευδωνυμία)
- Τεχνικές Ασφάλειας και Μυστικότητας που χρησιμοποιούνται στο Blockchain (Mixing, Anonymous Signatures, Homomorphic Encryption - HE, Attribute-based Encryption - ABE, Secure Multi-Party Computation, Non-Interactive Zero-Knowledge (NIZK) Proof, The Trusted Execution Environment Based Smart Contracts, Game-based Smart Contracts)

9. Ανίχνευση Εισβολών στο Διαδίκτυο των Αντικειμένων

- Τεχνικές Ανίχνευσης Εισβολών
- Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDSs)
- Εργαλεία, μέθοδοι και τεχνολογίες που χρησιμοποιούνται
- Η Ανίχνευση Εισβολών και η Θεωρία των Παιγνίων
- Ανίχνευση Εισβολών στο Cloud Computing
- Προβλήματα και περιορισμοί στα IDSs
- Machine Learning Anomaly Detection
- Machine Learning Categories
- Supervised learning για Intrusion Detection
- Unsupervised learning για Intrusion Detection
- Σύγκριση υλοποιήσεων IDS με βάση την τοποθέτηση
- Σύγκριση Προβλημάτων Ασφάλειας και Αντιμετώπισης
- Αρχιτεκτονική IoT και Επιθέσεις/Επίπεδο
- Επιθέσεις σε IoT: Taxonomy
- GAN for Distributed ID in IoT

10. Ψηφιακή Δικανική (Digital Forensics)

- Μεθοδολογία εφαρμογής
- Απαιτήσεις για Digital Forensics

- File System Forensics
- Application Forensics
- Cloud Computing Forensics
- IoT Forensics
- Network Forensics