ΗΥ-457 ΕΙΣΑΓΩΓΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1. ΓΕΝΙΚΑ

ΔΙΔΑΣΚΩΝ	ΕΥΑΓΓΕΛΟΣ ΜΑΡΚΑΤΟΣ		
ΕΞΑΜΗΝΟ ΔΙΔΑΣΚΑΛΙΑΣ	ΕΑΡΙΝΟ		
ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ / ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**ΗΥ-457**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**5ο-8ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΕΙΣΑΓΩΓΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις και φροντιστήρια	6	6

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	Επιστημονικής Περιοχής Ε5
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΗΥ-150
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική. Ενδέχεται να γίνεται και στην Αγγλική εάν υπάρχει ενδιαφέρον από αγγλόφωνο ακροατήριο.
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	http://www.csd.uoc.gr/~hy457

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος.

Συμβουλευτείτε το Παράρτημα Α

Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης

Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης

και Παράρτημα Β

Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων

Οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος

- θα κατέχουν τις βασικές έννοιες της ασφάλειας πληροφοριών και δικτύων
- θα έχουν εξοικειωθεί με βασικά εργαλεία κρυπτογράφησης και αποκρυπτογράφησης
- θα έχουν μάθει τις βασικές αρχές της θεωρίας κρυπτογραφίας και προστασίας δικτύων
- θα έχουν μάθει τις βασικές αρχές επιθέσεων στο διαδίκτυο και εντοπισμού κακόβουλου λογισμικού, και
- θα είναι σε θέση να υλοποιήσουν νέα εργαλεία ασφάλειας και προστασίας στο διαδίκτυο

Γενικές Ικανότητες

Λαμβάνοντας υπόψη τις γενικές ικανότητες που πρέπει να έχει αποκτήσει ο πτυχιούχος (όπως αυτές αναγράφονται στο Παράρτημα Διπλώματος και παρατίθενται ακολούθως) σε ποια / ποιες από αυτές αποσκοπεί το μάθημα;.

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
Προσαρμογή σε νέες καταστάσεις
Λήψη αποφάσεων
Αυτόνομη εργασία
Ομαδική εργασία
Εργασία σε διεθνές περιβάλλον
Εργασία σε διεπιστημονικό περιβάλλον
Παράγωγή νέων ερευνητικών ιδεών
Σχεδιασμός και διαχείριση έργων
Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα
Σεβασμός στο φυσικό περιβάλλον
Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και ευαισθησίας σε θέματα φύλου
Άσκηση κριτικής και αυτοκριτικής
Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- Προσαρμογή σε νέες καταστάσεις
- Λήψη αποφάσεων
- Αυτόνομη εργασία
- Ομαδική εργασία
- Σχεδιασμός και διαχείριση έργων
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

• Εισαγωγή: ιστορική αναδρομή, κλασσική κρυπτογραφία, σύγχρονες εφαρμογές
• Αρχιτεκτονική ασφάλειας: απειλές/επιθέσεις, μηχανισμοί/υπηρεσίες ασφάλειας, σχεδιασμός/πολιτικές ασφάλειας
• Συμμετρική κρυπτογραφία: κωδικοποιητές τμημάτων, αλγόριθμοι DES/3DES/AES, εφαρμογές/επιθέσεις
• Ασύμμετρη κρυπτογραφία: δομή κρυπτοσυστημάτων δημόσιου κλειδιού, ψηφιακές υπογραφές, διαχείριση κλειδιών, αλγόριθμοι RSA/DSS/ECC, εφαρμογές/επιθέσεις
• Αυθεντικοποίηση μηνυμάτων: ασφαλείς συναρτήσεις σύνοψης, αλγόριθμοι MD5/SHA/HMAC, εφαρμογές/επιθέσεις
• Κρυπτογραφικά πρωτόκολλα: αυθεντικοποίηση/διανομή κλειδιών, παραδείγματα (passwords, challenge-response, needham-schroeder, kerberos), αρχές σχεδιασμού/επιθέσεις
• Ασφάλεια στο Internet: πρωτόκολλα ασφάλειας επιπέδου Internet (IPsec) και επιπέδου μεταφοράς (SSL, TLS, SSH)
• Ασφάλεια εφαρμογών: ηλεκτρονικό ταχυδρομείο (PGP, S/MIME), ασφαλείς ηλεκτρονικές πληρωμές (SET, micro-payments)
• Υποδομή δημόσιων κλειδιών (PKI): ψηφιακά πιστοποιητικά, πάροχοι υπηρεσιών πιστοποίησης
• Λοιπές εφαρμογές: τραπεζικός τομέας (ATM), τηλεπικοινωνίες (GSM, wireless), ψηφιακά πνευματικά δικαιώματα (DVD, Pay-TV)
• Ασφάλεια λογισμικού και λειτουργικών συστημάτων: προγραμματιστικά λάθη, κρυπτογραφικές βιβλιοθήκες, trusted computing base
• Πρακτικά εργαλεία και τεχνικές: Viruses, Worms, Bots, Spyware, Phishing, διαχείριση ενημερωμένων εκδόσεων, εργαλεία επιτήρησης σταθμών εργασίας και δικτύων
• Διασφάλιση και αξιολόγηση ασφάλειας συστημάτων και προϊόντων: σκοπός, ζητήματα και μέθοδοι
• Ηλεκτρονικός πόλεμος: η πληροφορία σαν ανταγωνιστικό όπλο, κρίσιμες υποδομές, κυβερνοεπιθέσεις

• Κρυπτογραφική πολιτική: νομοθεσία, ιδιωτικότητα, ανωνυμία, προστασία δεδομένων, πνευματική ιδιοκτησία
• Οικονομικά της ασφάλειας: τεχνολογικά/οικονομικά κίνητρα για την ανάπτυξη ασφαλών προϊόντων

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο (αίθουσα διδασκαλίας)
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	• Ηλεκτρονικό ταχυδρομείο • Ιστοσελίδα μαθήματος • Ηλεκτρονική υποβολή ασκήσεων
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ *Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.* *Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ.* *Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης ώστε ο συνολικός φόρτος εργασίας σε επίπεδο εξαμήνου να αντιστοιχεί στα standards του ECTS*	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	52
Εργαστήρια / Φροντιστήρια	26
Εργαστηριακές ασκήσεις - Project	50
Μελέτη θεωρίας	50
Σύνολο Μαθήματος	**178**

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ *Περιγραφή της διαδικασίας αξιολόγησης* *Γλώσσα Αξιολόγησης, Μέθοδοι αξιολόγησης, Διαμορφωτική ή Συμπερασματική, Δοκιμασία Πολλαπλής Επιλογής, Ερωτήσεις Σύντομης Απάντησης, Ερωτήσεις Ανάπτυξης Δοκιμίων, Επίλυση Προβλημάτων, Γραπτή Εργασία, Έκθεση / Αναφορά, Προφορική Εξέταση, Δημόσια Παρουσίαση, Εργαστηριακή Εργασία, Κλινική Εξέταση Ασθενούς, Καλλιτεχνική Ερμηνεία, Άλλη / Άλλες* *Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.*	Γλώσσα ελληνική. Ενδέχεται να γίνεται και στην Αγγλική εάν υπάρχει ενδιαφέρον από αγγλόφωνο ακροατήριο. Τελικός βαθμός: • τελικό διαγώνισμα: 70%, • ασκήσεις: 30% (1:10%, 2:20%, 3:10% (bonus))

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία :

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ: ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ, WILLIAM STALLINGS, LAWRIE BROWN
Επιλογές Συγγραμμάτων στον ΕΥΔΟΞΟ:

1. Βιβλίο [50656354]: ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ: ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ, WILLIAM STALLINGS, LAWRIE BROWN Λεπτομέρειες
2. Βιβλίο [9771]: Σύγχρονη κρυπτογραφία, Γκρίτζαλης Στέφανος Λεπτομέρειες
3. Βιβλίο [13618]: ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ: ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΡΟΤΥΠΑ, WILLIAM STALLINGS Λεπτομέρειες

-Συναφή επιστημονικά περιοδικά: