ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	*Προπτυχιακό*		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ΠΛΥ07041	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**7ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ**		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις	2	
Ασκήσεις Πράξης	1	
Εργαστηριακές Ασκήσεις	1	
ΣΥΝΟΛΟ	**4**	**5**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων (Μάθημα Ειδικότητας, Υποχρεωτικό)
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Δίκτυα Υπολογιστών, Τεχνολογίες Διαδικτύου, Λειτουργικά Συστήματα Ι, (όχι ως υποχρέωση δήλωσης μαθημάτων στο e-gram, αλλά ως προς την προαπαιτούμενη γνώση)
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ (στην Αγγλική)
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	http://teachers.teicm.gr/chilas/diktya_III.htm http://elearning.teiser.gr/course/view.php?id=179

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Ο σκοπός του μαθήματος είναι η εξοικείωση των φοιτητών με τις θεμελιώδεις αρχές της Ασφάλειας Υπολογιστικών Συστημάτων και Δικτύων και τα προβλήματα ασφάλειας των σύγχρονων υπολογιστικών συστημάτων και δικτύων, τους μηχανισμούς και τις τεχνολογίες προστασίας τους. Επίσης, οι φοιτητές έρχονται σε μια πρώτη επαφή με πρωτόκολλα, πλαίσια και συστήματα Διαχείρισης Δικτύων.

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής / τρια θα είναι σε θέση :

- Να γνωρίζει και να εξηγεί τις θεμελιώδεις έννοιες στην ασφάλεια υπολογιστικών συστημάτων και δικτύων
- Να γνωρίζει και να αναλύει τους κυριότερους κρυπτογραφικούς αλγόριθμους και βασικά χαρακτηριστικά υλοποίησής τους σε προγραμματιστικό περιβάλλον.
- Να διακρίνει και να αναλύει τα βασικά χαρακτηριστικά ασφάλειας δικτύων και δικτυακών εφαρμογών, τις ιδιαίτερες ευπάθειες και απειλές που υφίστανται.
- Να γνωρίζει και να εφαρμόζει τους μηχανισμούς ασφάλειας και τα αντίστοιχα πρωτόκολλα σε όλα τα επίπεδα του TCP/IP και τους μηχανισμούς περιμετρικής άμυνας δικτύων.
- Να εξετάζει και να αξιολογεί τις ευπάθειες, τις απειλές και την εκτίμηση επικινδυνότητας σε ένα υπολογιστικό σύστημα.
- Να γνωρίζει και να εξηγεί τις θεμελιώδεις έννοιες στη διαχείριση υπολογιστικών συστημάτων και δικτύων

Γενικές Ικανότητες

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- Ομαδική Εργασία
- Αυτόνομη Εργασία
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Μέρος Ι

- Βασικές αρχές ασφάλειας δικτύων και πληροφοριακών συστημάτων. Εννοιολογική θεμελίωση. Ακεραιότητα, Αυθεντικοποίηση, Ιδιωτικότητα, Μη-απάρνηση.
- Ανάλυση και Διαχείριση Επικινδυνότητας: δυνατότητες και περιορισμοί των τεχνικών ανάλυσης και διαχείρισης επικινδυνότητας.
- Μοντέλα και πολιτικές ελέγχου πρόσβασης: Lattice, Bell-La Padula, MAC, DAC, RBAC.
- Στοιχεία κρυπτογραφίας. Κλασική και μοντέρνα κρυπτογραφία. Κρυπταλγόριθμοι τμήματος και ροής, κρυπτογραφία Δημοσίου κλειδιού, κρυπτογραφικές συναρτήσεις σύνοψης, κρυπτανάλυση.
- Αυθεντικοποίηση Οντοτήτων: Πρωτόκολλα και Τεχνολογίες αυθεντικοποίησης, Έξυπνες κάρτες, Βιομετρία, Ψηφιακά πιστοποιητικά, Ψηφιακή Υπογραφή, Υποδομή Δημοσίου Κλειδιού.
- Ιομορφικό λογισμικό: Μοντέλα και κατηγορίες κακόβουλου λογισμικού
- Ασφάλεια Βάσεων Δεδομένων: βασικές έννοιες, μοντέλα και πολιτικές ελέγχου πρόσβασης ΒΔ και μεθοδολογικό πλαίσιο σχεδιασμού ασφαλών ΒΔ.
- Μοντέλα Ασφάλειας κινητού κώδικα: Το μοντέλο ασφάλειας της Java και οι δυνατότητες υλοποίησης μηχανισμών ασφάλειας και κρυπταλγορίθμων.
- Ασφάλεια στο Διαδίκτυο: Απειλές και ευπάθειες, μηχανισμοί και πρωτόκολλα ασφάλειας δικτύου στα επίπεδα του TCP/IP. Ασφάλεια Δικτύων. Kerberos, PGP, IPsec, Web Security (TLS/SSL).
- Περιμετρική άμυνα δικτύου και ασφαλής διαχείρισή του: Firewalls, secure SNP. Εικονικά δίκτυα (VPN). Ανίχνευση εισβολών και φίλτρα.

Μέρος ΙΙ

- Διαχείριση Δικτύων. Συστήματα διαχείρισης – πλατφόρμες, Διαλειτουργικότητα, Διαχείριση διαφορετικών τεχνολογιών, alarms – troubles – warnings, performance – traffic – ticketing, distributed management, προϊόντα, γενικά εργαλεία.
- Πρότυπα Διαχείρισης & Τεχνολογίες. OSI management (X.7xx), TMN Framework, Internet management (SNMP, RMON, …), Inernetworking (MIB's), Εφαρμογές (Corba, OMG), TINA, Web Based Management.

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	Θεωρητική από έδρας διδασκαλία με συζήτηση και ενεργή συμμετοχή των φοιτητών. Κατά την διάρκεια του μαθήματος γίνονται παρουσιάσεις σε power point. Εργαστηριακές Ασκήσεις. Προσομοιώσεις δικτύων με το OPNET. Αλγόριθμοι κρυπτογράφησης με το CryptTool. Επίδειξη λειτουργίας πρωτοκόλλου SNMP σε πραγματικό περιβάλλον.
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	Χρήση εξειδικευμένων λογισμικών. Υποστήριξη Μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας Moodle (elearning.teicm.gr) ή/και e-class.

	Ηλεκτρονικές Ασκήσεις Αυτοαξιολόγησης
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	26
Ασκήσεις πράξης	13
Εργαστηριακές Ασκήσεις	13
Συγγραφή εργαστηριακών αναφορών, *Εκπόνηση μελέτης (project)*	21
Αυτοτελής Μελέτη	52
Σύνολο Μαθήματος	***125***

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Ο τελικός βαθμός του μαθήματος διαμορφώνεται από τον βαθμό του θεωρητικού μέρους (από γραπτή τελική εξέταση) καθώς και από εργασίες που ανατίθενται στους φοιτητές και αξιολόγηση των εργαστηριακών δεξιοτήτων τους. Απαραίτητη προϋπόθεση για τη συμμετοχή στην τελική εξέταση είναι η επιτυχής απόκριση στην εργαστηριακή συνιστώσα του μαθήματος. 1. Η γραπτή τελική εξέταση του θεωρητικού μέρους περιλαμβάνει: - Ερωτήσεις πολλαπλής επιλογής - Επίλυση προβλημάτων εφαρμογής των γνώσεων που αποκτήθηκαν. - Ερωτήσεις σύντομης απάντησης - Συγκριτική αξιολόγηση στοιχείων θεωρίας.

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία (μέσω του συστήματος ΕΥΔΟΞΟΣ):

- ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ: ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ, Έκδοση: 3η Αμερικανική/2016, WILLIAM STALLINGS, LAWRIE BROWN, ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ ΕΠΕ
- "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Γ. Πάγκαλος & Ι.Μαυρίδης, Εκδόσεις ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη, 2002
- "Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης ", Σ. Γκρίτζαλης , Σ. Κάτσικας , Δ. Γκρίτζαλης, Εκδόσεις Παπασωτηρίου, Αθήνα, 2003
- Χειλάς, Κ., Πολίτης, Α., Βακαλούδης, Α. 2016. Εργαστηριακές Ασκήσεις Δικτύων Η/Υ. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. Διαθέσιμο ελεύθερα στο: http://hdl.handle.net/11419/1763

Συμπληρωματικές πηγές:

- Τα RFCs (Request for Comments) που αφορούν στις διάφορες εκδόσεις και εφαρμογές του πρωτοκόλλου SNMP και των MIBs. Όλα διατίθενται ελεύθερα και δωρεάν στο www.ietf.org καθώς και στο www.snmp.com