E603 Ασφάλεια Ψηφιακών Συστημάτων

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	Τεχνολογίας		
ΤΜΗΜΑ	Ψηφιακών Συστημάτων		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	E603	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	6ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Ψηφιακών Συστημάτων		

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, Φροντιστήρια και Εργαστήρια	4	5
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	Επιστημονικής Περιοχής Επιλογής
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uth.gr/courses/DS_U_157/

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*

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

- Σχηματίσει μια συνολική εικόνα του χώρου της ασφάλειας των πληροφορικών συστημάτων
- Κατανοεί τους βασικούς κρυπτογραφικούς αλγορίθμους σε γνωστά πρωτόκολλα ασφάλειας
- Εφαρμόζει τεχνικές κρυπτανάλυσης και επιθέσεων πλευρικού καναλιού
- Αντιλαμβάνεται την πολυπλοκότητα υλοποίησης ασφαλών κρυπτοσυστημάτων
- Εντοπίζει και να διορθώνει κενά ασφάλειας σε ενσύρματες και ασύρματες επικοινωνίες
- Περιγράφει τους κινδύνους και τις ευπάθειες που μπορεί να υπόκειται ένα πληροφορικό σύστημα και να μπορεί να προβαίνει στην σχετική εκτίμηση του ρίσκου με την χρήση επιστημονικών μεθοδολογιών
- Ορίζει τις βασικές μεθοδολογίες και τεχνικές ανάπτυξης ασφαλούς λογισμικού
- Αναγνωρίζει πως να αποτρέπει και να διορθώσει τυχόν ευπάθειες και επιθέσεις σε ένα πληροφορικό σύστημα καθώς και να εντοπίζει ενδεχόμενες παραβιάσεις των μηχανισμών ασφαλείας του

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*

- Εφαρμογή της γνώσης στην πράξη
- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- Προσαρμογή σε νέες καταστάσεις
- Λήψη αποφάσεων
- Αυτόνομη εργασία
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή και εννοιολογική θεμελίωση της ασφάλειας ψηφιακών συστημάτων
- Βασικές αρχές και αλγόριθμοι κρυπτογραφίας
- Σύγχρονοι κρυπτογραφικοί αλγόριθμοι
- Τύποι επιθέσεων
- Ψηφιακές υπογραφές και συναρτήσεις κατακερματισμού
- Μαθηματική θεμελίωση κρυπτογραφίας
- Πρωτόκολλα ασφάλειας και επιθέσεις σε Ενσύρματα Δίκτυα
- Πρωτόκολλα ασφάλειας και επιθέσεις σε Ασύρματα Δίκτυα
- Τύποι καλόβουλου λογισμικού
- Ασφάλεια πληροφοριών
- Ανάπτυξη Ασφαλούς Λογισμικού
  - Ασφαλείς Μεθοδολογίες Ανάπτυξης Λογισμικού
  - Ασφάλεια Λειτουργικών Συστημάτων
  - Ασφάλεια Υλικού
- Ασφάλεια Πληροφοριών
  - Πολιτικές Ασφάλειας
  - Διαχείριση Ρίσκου
  - Επιθεώρηση και Πρότυπα Ασφάλειας
  - Αυθεντικοποίηση και Έλεγχος Πρόσβασης
  - Διαχείριση Ταυτότητας
- Διασφάλιση και Αξιολόγηση Ασφάλειας Συστημάτων και Προϊόντων

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο

ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Διαλέξεις με τη χρήση προβολικού και διαφανειών τύπου ppt/pdf. Υποστήριξη μαθησιακής διαδικασίας μέσω ηλεκτρονικής αλληλογραφίας, σχετικής ηλεκτρονικής λίστας και του eclass.
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	39
Εργαστήρια & Φροντιστήρια	13
Αυτοτελής Εκπόνηση Εργασίας	23
Αυτοτελής Μελέτη	50
Σύνολο Μαθήματος ***(25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)***	**125**

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.*	I. Γραπτή τελική εξέταση (70%): - Ερωτήσεις Θεωρίας - Ερωτήσεις πολλαπλής επιλογής - Επίλυση προβλημάτων - Παρουσίαση και σύγκριση μεθόδων II. Εκπόνηση Εργασίας (15%) III. Εργαστηριακές ασκήσεις (15%)

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

-Προτεινόμενη Βιβλιογραφία :

- Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, 2003
- Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004
- William Stallings, Ασφάλεια υπολογιστών - Αρχές και πρακτικές, Εκδόσεις Κλειδάριθμος
- 2016