ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	7 (ΜΕΤΑΠΤΥΧΙΑΚΟ)		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	Mscict113	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**2ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ		

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
Φροντιστήριο	-	
Εργαστηριακές ασκήσεις	-	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης, γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	Ειδίκευσης, Ανάπτυξης Δεξιοτήτων
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	-
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uniwa.gr/courses/MSCICT107/

(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 το Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης*
- *Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και το Παράρτημα Β*
- *Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων*

Το μάθημα καλύπτει το γενικό μέρος της Ασφάλειας της Πληροφορίας και των Συστημάτων. Σκοπός του μαθήματος είναι η δημιουργία ενός βασικού πλαισίου θεωρητικών και εφαρμοσμένων γνώσεων στην ευρύτερη περιοχή της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων σε δύο άξονες, την πληροφορία και το σύστημα. Το πλαίσιο αυτό θα συμπληρώσει επαρκώς το προφίλ του φοιτητή που ολοκληρώνει το μεταπτυχιακό αυτό κύκλο σπουδών στην Πληροφορική και θα αποτελέσει γι' αυτόν σημαντικό εφόδιο στην αγορά εργασίας.

Γνώσεις

Στα πλαίσια του μαθήματος, οι φοιτητές και οι φοιτήτριες:

- Θα αντιλαμβάνονται τα σύγχρονα ζητήματα ασφάλειας πληροφοριών και συστημάτων και τις προκλήσεις σε σύγχρονες επιχειρήσεις και οργανισμούς
- Θα κατανοούν το πλαίσιο ανάπτυξης ενός συστήματος διοίκησης για την ασφάλεια των πληροφοριών
- Θα γνωρίζουν τα προβλήματα ασφάλειας σε Πληροφοριακά και Επικοινωνιακά Συστήματα
- Θα αναγνωρίζουν τις ευπάθειες των πληροφοριακών και επικοινωνιακών συστημάτων
- Θα εφαρμόζουν βασικές αρχές σχεδιασμού πολιτικών ασφαλείας
- Θα γνωρίζουν τα χαρακτηριστικά και τους μηχανισμούς ασφαλείας που υλοποιούν τις πολιτικές αυτές
- Θα επιδεικνύουν κριτική κατανόηση της μεθοδολογίας της διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών
- Θα έχουν εξοικειωθεί με παραδείγματα που υλοποιούν και εφαρμόζουν μηχανισμούς ασφάλειας σε διαφορετικά Λειτουργικά Συστήματα
- Θα έχουν γνώσεις στην περιοχή της Ασφάλειας Βάσεων Δεδομένων
- Θα γνωρίζουν τα διαφορετικά είδη firewalls και πώς αυτά χρησιμοποιούνται και εφαρμόζονται
- Θα γνωρίζουν μηχανισμούς αυθεντικοποίησης, το ρόλο και τη σπουδαιότητά τους
- Θα έχουν εξοικειωθεί με τα Computer Forensics και θα έχει γνώση των εργαλείων που τα υποστηρίζουν
- Θα γνωρίζουν στοιχεία κρυπτογραφίας και κρυπτανάλυσης σε συμμετρικούς και ασύμμετρους κρυπτογραφικούς αλγόριθμους
- Θα έχουν κατανοήσει τα Συστήματα Ανίχνευσης Εισβολών, τον τρόπο λειτουργίας τους και τις τεχνικές που χρησιμοποιούνται στις μηχανές ανίχνευσης αυτών
- Θα επιδεικνύουν κριτική κατανόηση του πλαισίου σχεδιασμού, εφαρμογής και αξιολόγησης των επιδόσεων των κατάλληλων αντιμέτρων: οργανωτικών, τεχνολογικών, φυσικής ασφάλειας, ανθρώπινου παράγοντα
- Θα κατανοούν τα σύγχρονα προβλήματα που εγείρονται κατά την επεξεργασία προσωπικών δεδομένων και να γνωρίζουν τις μεθοδολογίες προστασίας δεδομένων ήδη από τον σχεδιασμό
- Θα διαθέτουν αυξημένη κριτική αντίληψη της εξελικτικής δυναμικής του γνωστικού πεδίου της κυβερνοασφάλειας και της προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων.

Στο μάθημα αξιοποιούνται τα πιο σύγχρονα διεθνή πρότυπα και μεθοδολογίες για την υλοποίηση αντιμέτρων, με χαρακτήρα είτε προληπτικό, είτε ανιχνευτικό, είτε διορθωτικό. Για το σύγχρονο πλαίσιο λειτουργίας των επιχειρήσεων και οργανισμών του ιδιωτικού και του δημόσιου τομέα, στο μάθημα προσφέρονται, κατά το δυνατό, γνώσεις κατάλληλες για την αναγνωριση των σημαντικών ζητημάτων ασφάλειας πληροφοριαών και συστημάτων και προστασίας της ιδιωτικότητας.

Δεξιότητες

Το πρόγραμμα διαλέξεων και πρακτικών ασκήσεων είναι δομημένο με τρόπο ώστε να συναντώνται οι state-of-the-art επιστημονικές γνώσεις, με το πλαίσιο αποτελεσματικής και αποδοτικής εφαρμογής τους, ώστε να εφοδιαστούν φοιτητές και φοιτήτριες με δεξιότητες απαραίτητες για τη σύγχρονη αγορά

εργασίας στην Ελλάδα και διεθνώς και κατ' αποτέλεσμα να ενισχυθεί η δυνατότητα επαγγελματικής τους αποκατάστασης.

Με βάση τις ανωτέρω αρχές και ανάγκες, ολοκληρώνοντας το μάθημα οι φοιτητές και φοιτήτριες αναμένεται να δύνανται:

- Να εφαρμόζουν με ευχέρεια θεωρίες και μεθοδολογίες από τον χώρο της ασφάλειας πληροφοριών και συστημάτων, με έμφαση σε θέματα διαχείρισης κινδύνων της ασφάλειας των πληροφοριών σε επιχειρήσεις και οργανισμούς, ανεξαρτήτως του πεδίου δραστηριοποίησής τους
- Να αξιολογούν συγκριτικά ποικίλες μεθόδους και εργαλεία που αξιοποιούνται για την ασφάλεια πληροφοριών και συστημάτων
- Να αρθρώνουν επαγωγικά, με επιστημονικά τεκμηριωμένο τρόπο, λύσεις στα σύνθετα προς επίλυση προβλήματα από τον χώρο της ασφάλειας πληροφοριών και συστημάτων και της προστασίας προσωπικών δεδομένων

Ικανότητες

Οι φοιτητές και φοιτήτριες θα μπορούν:

- Να αναπτύσσουν με αυτονομία τις γνώσεις και ικανότητες τους
- Να επιλύουν προβλήματα και να λαμβάνουν στρατηγικές αποφάσεις με αφετηρία την επαγωγική σκέψη
- Να συνεισφέρουν στην ανάπτυξη γνώσεων και πρακτικών στον επαγγελματικό χώρο και να διαθέτουν επιχειρησιακή ικανότητα κατά τη διαχείριση κρίσεων

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	*Σχεδιασμός και διαχείριση έργων*
	Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα
	Σεβασμός στο φυσικό περιβάλλον
Προσαρμογή σε νέες καταστάσεις	*Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας*
Λήψη αποφάσεων	*και ευαισθησίας σε θέματα φύλου*
Αυτόνομη εργασία	*Άσκηση κριτικής και αυτοκριτικής*
Ομαδική εργασία	*Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης*
Εργασία σε διεθνές περιβάλλον	*……*
Εργασία σε διεπιστημονικό περιβάλλον	*Άλλες…*
Παράγωγή νέων ερευνητικών ιδεών	*…….*

Οι γενικές ικανότητες που θα πρέπει να έχουν αποκτήσει οι φοιτητές και οι φοιτήτριες είναι:

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση των κατάλληλων τεχνολογιών
- Λήψη αποφάσεων
- Αυτόνομη εργασία
- Αποτελεσματική λειτουργία σε περιβάλλον ομάδας
- Δυνατότητα προσαρμογής σε νέες καταστάσεις
- Σχεδιασμός και διαχείριση έργων για διασφάλιση ποιότητας (iron triangle: time, cost, scope)
- Δραστηριοποίηση σε διαθεματικό και διεπιστημονικό περιβάλλον
- Παραγωγή νέων ερευνητικών ιδεών

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα καλύπτει γενικά θέματα Ασφάλειας Πληροφορίας και Συστημάτων. Το περίγραμμα του μαθήματος περιλαμβάνει θεμελιώδεις έννοιες και ορολογία στην Ασφάλεια Πληροφορίας και Συστημάτων, θέματα κλασικής και ασφαλούς Κρυπτογράφησης (ασύμμετρης: RSA), ανεκτικότητα κρυπτογραφικών αλγόριθμων, προστασία Λειτουργικών Συστημάτων, ασφάλεια Βάσεων Δεδομένων, Έλεγχο Πρόσβασης, ασφάλεια Δικτύων και Κατανεμημένων Συστημάτων, Ανίχνευση Επιθέσεων, Ανάλυση Επικινδυνότητας, Computer Forensics.

Περίγραμμα μαθήματος

1. Εννοιολογική θεμελίωση της Ασφάλειας Πληροφορίας και Συστημάτων
   - Επιτιθέμενοι και ειδικές κατηγορίες (εσωτερικά επιτιθέμενοι)
   - Ευπάθειες Εφαρμογών και Συστημάτων
   - Είδη Απειλών και Μέθοδοι Επίθεσης
   - Υπηρεσίες και Μηχανισμοί Ασφάλειας (Έλεγχοι)

2. Κρυπτογραφία
   - Κλασσικά Κρυπτοσυστήματα
   - Αλγόριθμοι Μονοαλφαβητικής Αντικατάστασης
   - Αλγόριθμοι Πολυαλφαβητικής Αντικατάστασης
   - Αλγόριθμοι Μετάθεσης
   - Ανεκτικότητα Συμμετρικών Κρυπτογραφικών Αλγορίθμων

3. Ασύμμετρη Κρυπτογραφία και Ψηφιακές Υπογραφές
   - Κρυπτογράφηση δημοσίου κλειδιού (Diffie-Hellman, RSA)
   - Ψηφιακές Υπογραφές
   - Παραδείγματα και εφαρμογές

4. Προστασία Λειτουργικών Συστημάτων, Αυθεντικοποίηση και Έλεγχος Πρόσβασης
   - Αντικείμενα και μέθοδοι προστασίας
   - Προστασία μνήμης και διευθυνσιοδότησης
   - Μηχανισμοί Ελέγχου Πρόσβασης
   - Μηχανισμοί προστασίας αρχείων
   - Μηχανισμοί Αυθεντικοποίησης

5. Ασφάλεια Βάσεων Δεδομένων
   - Απαιτήσεις ασφάλειας
   - Αξιοπιστία και ακεραιότητα ΒΔ
   - Ευαίσθητα δεδομένα
   - Το πρόβλημα λήψης πληροφοριών

6. Ανάλυση Επικινδυνότητας
   - Λόγοι που οδηγούν σε Ανάλυση Επικινδυνότητας
   - Βήματα της Ανάλυσης Επικινδυνότητας
   - Εξοικονόμηση προγράμματος.
   - Λόγοι κατά της Ανάλυσης Επικινδυνότητας

7. Ασφάλεια, Προστασία Ιδιωτικότητας, Απόρρητο Επικοινωνιών και Λήψη αποφάσεων με αλγορίθμους
   - Ψηφιακή πρόοδος στην Ελλάδα και την ΕΕ
   - Κυβερνοασφάλεια
   - Απόρρητο ηλεκτρονικών επικοινωνιών
   - Προστασία δεδομένων
   - Προστασία προσωπικών δεδομένων
   - Λήψη αποφάσεων με αλγορίθμους
   - Οι μείζονες κίνδυνοι

8. Εννοιολογική θεμελίωση όρων ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων και ISO 27000:2018

- Η ανάγκη προστασίας των πληροφοριών
- Εννοιολογική Θεμελίωση και το πρότυπο ISO27000:2018

9. Σύστημα Διοίκησης για την Ασφάλεια των Πληροφοριών και ISO 27001:2022
   - Η ανάγκη προστασίας των πληροφοριών
   - Προτυποποίηση: Πιστοποίηση και Διαπίστευση
   - Το πρότυπο ISO 27001:2022

10. Κανόνες Καλής Πρακτικής για τη Διοίκηση για την Ασφάλεια των Πληροφοριών και ISO 27002:2022
   - Το πρότυπο ISO 27002:2022

11. Καθοδήγηση για τη Διοίκηση Επικινδυνότητας της Ασφάλειας των Πληροφοριών και ISO 27005:2022
   - Εισαγωγή και βασικές έννοιες
   - Η αναγκαιότητα Διοίκησης της Επικινδυνότητας
   - Το πρότυπο ISO 27005:2022
   - Μέθοδοι Διοίκησης της Επικινδυνότητας

12. Πλαίσιο Ιδιωτικότητας και ISO 29100:2011/2017
   - Περίληψη του ISO 29100:2011
   - Αντικείμενο και Ορισμοί στο ISO 29100:2011
   - Αρκτικόλεξα στο ISO 29100:2011
   - Βασικά στοιχεία του Πλαισίου Ιδιωτικότητας στο ISO 29100:2011
   - Οι αρχές Ιδιωτικότητας στο ISO 29100:2011

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Σύγχρονη εξ αποστάσεως εκπαίδευση
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Υποστήριξη της μαθησιακής διαδικασίας μέσω της εκπαιδευτικής πλατφόρμας Eclass, της πλατφόρμας εξ' αποστάσεως εκπαίδευσης MS-Teams, και άλλων ηλεκτρονικών υπηρεσιών (ηλεκτρονικού ταχυδρομείου κ.λπ.) του Πανεπιστημίου.
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 σύμφωνα με τις αρχές του ECTS*	***Δραστηριότητα Φόρτος Εργασίας Εξαμήνου*** Διαλέξεις 39 Φροντιστήριο - Εργαστηριακή άσκηση - Ατομικές εργασίες εξάσκησης 71 Αυτοτελής μελέτη 90 ***Σύνολο Μαθήματος 200*** (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)

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.*	Η τελική βαθμολογία προκύπτει από: I. Εκπόνηση εργασίας (40%) II. Προφορική τελική εξέταση (60%) που περιλαμβάνει: - Ερωτήσεις ανάπτυξης - Επίλυση προβλημάτων - Συγκριτική αξιολόγηση στοιχείων θεωρίας

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- Stallings William και Brown Lawrie, Ασφάλεια Υπολογιστών – Αρχές και Πρακτικές, 3/E, 2016, Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ.
- Stallings William, Κρυπτογραφία και Ασφάλεια Δικτύων: Αρχές και Εφαρμογές, 5/E, 2012, Εκδοτικός Όμιλος Ίων.
- Κάτσικας Σ. Γκρίτζαλης Σ. Λαμπρινουδάκης Κ., (eds.) Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, Εκδόσεις Νέων Τεχνολογιών, 2021
- Bishop M., Introduction to Computer Security, Addison-Wesley,2005.
- Fourouzan B., "Cryptography and Network Security", 2008, Mc Graw-Hill.
- Menezes A., Van Oorschot P., Vanstone S., Handbook of Applied Cryptography, HAC (free).
- Mitnick K.D., Simon W.L., The Art of Deception, John Wiley & Sons, 2002.
- Pfleeger C.P., Lawrence Pfleeger S., Security in Computing, Prentice Hall, 2003.
- Stallings William, Cryptography and Network Security: Principles and Practice, 5/E (free), 2012, Prentice Hall.
- Young S., Aitel D., The Hacker's Handbook – The Strategy behind Breaking into and Defending Networks, Auerbach, 2004.

- Συναφή επιστημονικά περιοδικά:

- IEEE Communications Surveys and Tutorials, IEEE Press
- IEEE Transactions on Information Forensics and Security, IEEE Press
- ACM Transactions on Privacy and Security, ACM Press
- International Journal of Information Security, Springer
- Computers and Security, Elsevier
- Information and Computer Security, Emerald