ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ		
ΤΜΗΜΑ	ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**M107**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**2**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Δικτύων και Τηλεπικοινωνιακών 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**
	3	6
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*	Γενικού υποβάθρου
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	-
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	ΕΛΛΗΝΙΚΗ (ΟΤΑΝ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS, Η ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ ΚΑΙ ΕΞΕΤΑΣΕΩΝ ΕΙΝΑΙ Η ΑΓΓΛΙΚΗ)
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uoa.gr/courses/DIMTEL103/

(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*

Σκοπός του μαθήματος είναι η κατανόηση της ασφάλειας δικτύων και πληροφοριών, με απώτερο σκοπό την απόκτηση γνώσης για τις διαδικασίες, τεχνικές και τεχνολογίες ασφάλειας που εφαρμόζονται για την επίτευξη ενός ασφαλούς δικτύου/συστήματος. Παράλληλα, εξετάζονται και οι πτυχές της προστασίας δεδομένων και ιδιωτικότητας, υπό το φως και του συναφούς νομικού πλαισίου στην ΕΕ.

Ειδικότερα, ο/η φοιτητής/-τρια που θα ολοκληρώσει επιτυχώς το μάθημα, αναμένεται ότι θα είναι σε θέση να:

- Έχει κατανοήσει τη σπουδαιότητα της ασφάλειας πληροφοριών και δικτύων, καθώς επίσης και της προστασίας προσωπικών δεδομένων και ιδιωτικότητας, αναγνωρίζοντας τα κοινά στοιχεία των εν λόγω εννοιών αλλά και πού διαφέρουν
- Έχει κατανοήσει την έννοια της διαχείρισης κινδύνων ασφαλείας
- Συνθέτει κατάλληλα κρυπτογραφικές δομές με τις σωστές παραμέτρους προκειμένου να παράγεται η βέλτιστη κρυπτογραφική λύση για δοθέν πρόβλημα.
- Αναγνωρίζει την αναγκαιότητα της αυθεντικοποιημένης κρυπτογράφησης
- Να αναλύει τη λειτουργία των βασικών πρωτοκόλλων ασφαλείας δικτύων, καθώς και τα επιμέρους χαρακτηριστικά τους που πρέπει να προσεχθούν κατά την υλοποίησή τους προκειμένου να μην εμφανίζεται ευπάθεια
- Να εφαρμόζει στην πράξη εφαρμογές λογισμικού που άπτονται της ασφάλειας δικτύων και πληροφοριών (εργαλεία εκτίμησης ευπαθειών, διαδικτυακά πρωτόκολλα που βασίζονται σε κρυπτογράφηση κ.α.)
- Εφαρμόζει θεωρητικές γνώσεις στην πράξη, επιλύοντας προβλήματα ασφάλειας σε τηλεπικοινωνιακά συστήματα επικοινωνιών.
- Έχει κατανοήσει τα βασικά αντίμετρα που πρέπει να υλοποιούνται για την πρόληψη, ανίχνευση και αντιμετώπιση των διαφόρων τύπων (κυβερνο)επιθέσεων
- Αξιολογεί προτεινόμενες τοπολογίες και ρυθμίσεις δικτύου ως προς το παρεχόμενο επίπεδο ασφάλειας
- Γνωρίζει τις κύριες συναφείς νομικές απαιτήσεις σε επίπεδο Ευρωπαϊκής Ένωσης
- Γνωρίζει τα σύγχρονα ανοιχτά ερευνητικά προβλήματα και τις νέες τάσεις/προκλήσεις στην ασφάλεια πληροφοριών και δικτύων, αλλά και στις τεχνολογίες ενίσχυσης ιδιωτικότητας.

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

Το μάθημα αποσκοπεί στις κάτωθι γενικές ικανότητες:

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- Ανάλυση προβλημάτων, με σκοπό την εύρεση της βέλτιστης λύσης και της λήψης αποφάσεων βάσει των συνθηκών (διαχείριση κινδύνων)

- Αυτόνομη εργασία (αλλά προκρίνεται και η ομαδική εργασία σε κάποιες περιπτώσεις)
- Παραγωγή νέων ερευνητικών ιδεών

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

1) Εισαγωγικές έννοιες της ασφάλειας πληροφοριών και δικτύων
2) Ζητήματα διαχείρισης ασφάλειας / ανάλυσης επικινδυνότητας
3) Νομικό πλαίσιο προστασίας προσωπικών δεδομένων και κυβερνοασφάλειας
4) Κρυπτογραφία (Συμμετρικοί/Ασύμμετροι αλγόριθμοι κρυπτογράφησης)
5) Κρυπτογραφικές συναρτήσεις κατακερματισμού - Ψηφιακές υπογραφές - Ψηφιακά πιστοποιητικά – Αυθεντικοποιημένη κρυπτογράφηση
6) Έλεγχος πρόσβασης - Διαχείριση συνθηματικών
7) Ασφάλεια στο Web – πρωτόκολλο TLS
8) Εικονικά ιδιωτικά δίκτυα - πρωτόκολλο IPSec
9) Ασφάλεια σε ασύρματες επικοινωνίες – πρωτόκολλα WEP, WPA, WPA2
10) Ασφάλεια (διαδικτυακών) εφαρμογών
    1. Κακόβουλα λογισμικά
    2. Επιθέσεις sql injection, buffer overflow, cross-site scripting
    3. Επιθέσεις DDOS
11) Συστήματα ανίχνευσης εισβολών – έλεγχος ανίχνευσης ευπαθειών - «Τείχη» ασφαλείας (Firewalls)
12) Ειδικά θέματα:
    a. Ασφάλεια σε περιβάλλον IoT – ειδικές προκλήσεις και τεχνικές αντιμετώπισης
    b. Ζητήματα προστασίας προσωπικών δεδομένων στο πλαίσιο (κυβερνο)ασφάλειας
    c. Μετα-κβαντική κρυπτογραφία

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Πρόσωπο με πρόσωπο (διαλέξεις σε αίθουσα/αμφιθέατρο). Ταυτόχρονα το μάθημα μεταδίδεται και διαδικτυακά, όπου έχουν πρόσβαση οι εγγεγραμμένοι φοιτητές
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	**1) Το μάθημα μεταδίδεται ταυτόχρονα και διαδικτυακά, για τους εγγεγραμμένους σε αυτό φοιτητές** **2) Υποστήριξη εκπαιδευτικής διαδικασίας μέσω του ιστοχώρου του μαθήματος (e-class),**

	σε συνεχή βάση κατά τη διάρκεια του ακαδημαϊκού εξαμήνου (ανάρτηση εκπαιδευτικού υλικού και ανακοινώσεων, forum συζητήσεων κτλ.) **3) Επικοινωνία με φοιτητές μέσω ηλεκτρονικού ταχυδρομείου**
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***
1. Διαλέξεις	39 (3 x 13)
2. Εργασία (στο σπίτι):	
α) Μελέτη (βιβλιογραφίας, σημειώσεων κτλ.) και ανάλυση θεμάτων	10
β) Επίλυση - Υλοποίηση	15
γ) Συγγραφή	6
3. Αυτοτελής Μελέτη	80
Σύνολο Μαθήματος	***150***

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 αξιολόγηση των φοιτητών γίνεται κατά τον κάτωθι τρόπο: 1) Γραπτή εξέταση στο τέλους του ακαδημαϊκού εξαμήνου (80%), με θέματα που έχουν ως σκοπό την αποτίμηση κριτικής σκέψης και της ικανότητας επίλυσης προβλημάτων. 2) Εργασία (20%), η οποία εκπονείται από τον κάθε φοιτητή ατομικά. Η εργασία προσφέρεται μετά την 7η εβδομάδα των μαθημάτων και υποβάλλεται με το τέλος της εξεταστικής περιόδου. Για κάποια ερωτήματα της εργασίας υπάρχει η παρότρυνση (χωρίς να είναι υποχρεωτικό) να δουλέψουν οι φοιτητές συνεργατικά (να επαληθεύει/επιβεβαιώνει ο ένας τα αποτελέσματα του άλλου και αντίστροφα). Το κάθε θέμα της εργασίας έχει σαφώς προκαθορισμένη μέγιστη βαθμολόγηση που μπορεί να λάβει, ενώ είναι επίσης σαφώς ορισμένο στη διατύπωσή του το τι

	απαιτείται για να θεωρηθεί μία απάντηση πλήρης. Τα ανωτέρω περιγράφονται στο εισαγωγικό υλικό που δίνεται στους φοιτητές κατά την 1η εβδομάδα του μαθήματος.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

1. Cryptography and Network Security, W. Stallings, Prentice Hall, 8th ed., 2020. (http://williamstallings.com/Cryptography/)
2. Cyber-Security Threats, Actors, and Dynamic Mitigation, Kolokotronis N., Shiaeles S. (eds), CRC Press, 2021 (https://www.taylorfrancis.com/books/edit/10.1201/9781003006145/cyber-security-threats-actors-dynamic-mitigation-stavros-shiaeles-nicholas-kolokotronis).
3. Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 3rd editition, 2020 (https://www.cl.cam.ac.uk/~rja14/book.html)
4. Cyberspace Information and Systems Security, Katsikas S., Gritzalis S., Lambrinoudakis K. (eds), NewTech Pubs (in Greek)

- Συναφή επιστημονικά περιοδικά:

1. *IEEE Security & Privacy magazine (https://www.computer.org/csdl/magazine/sp)*
2. *IEEE Transactions on Information Forensics and Security (https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206)*
3. *Computer Networks, Elsevier (https://www.sciencedirect.com/journal/computer-networks)*
4. *Proceedings of USENIX Security Symposiums (available online, on an annual basis: the link for the 2022 Symposium is https://www.usenix.org/conference/usenixsecurity22)*

Τέλος, παρέχονται στους φοιτητές άρθρα από διάφορα επιστημονικά περιοδικά και συνέδρια