ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	Επιστήμης και Τεχνολογίας		
ΤΜΗΜΑ	Επιστήμης και Τεχνολογίας		
ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ	ΠΜΣ «Msc in Cybersecurity»		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Μεταπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CC01	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	1
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Πληροφοριακών Συστημάτων		
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Επιλογής, υποχρεωτικό*	Υποχρεωτικό		
ΔΙΔΑΣΚΩΝ/ΟΥΣΑ (ΔΙΔΑΣΚΟΝΤΕΣ/ΟΥΣΕΣ)	Θεωρία: Αν. Καθ. Κωνσταντίνος Ράντος		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ σε περίπτωση που οι πς 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**
	3,75	6
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).		

ΑΝΑΛΥΣΗ ΔΙΔΑΚΤΙΚΩΝ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ**
Θεωρία	3,75 (Σύνολο: 30 ώρες)
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*	Ειδικού Υπόβαθρου
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	-
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Αγγλική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://elearn-ucips.ihu.gr/

(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*

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

- Κατανοεί τον ρόλο των πλαισίων κυβερνοασφάλειας.
- Προτείνει μηχανισμούς προστασίας σύμφωνα με διεθνή πλαίσια και βέλτιστες πρακτικές.
- Εξηγεί την μεθοδολογία της διαχείρισης κινδύνων.
- Κατανοεί πώς να εφαρμόζει κάποια μέθοδο αξιολόγησης κινδύνων.
- Γνωρίζει πώς να χρησιμοποιεί κύριους μηχανισμούς κρυπτογραφίας.
- Περιγράφει βέλτιστες πρακτικές διαχείρισης κυβερνοαπειλών.
- Εξηγεί την αρχιτεκτνική της μηδενικής εμπιστοσύνης.

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 Ν*
	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	*…….*

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

(3) ΠΕΡΙΓΡΑΦΗ/ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα παρέχει μια εισαγωγή στις θεμελιώδεις έννοιες της ασφάλειας στον κυβερνοχώρο και της ασφάλειας των υπολογιστών. Οι περισσότεροι σύγχρονοι οργανισμοί αντιμετωπίζουν κινδύνους ασφάλειας και ιδιωτικότητας που απειλούν τα πολύτιμα περιουσιακά τους στοιχεία. Είναι επιτακτική ανάγκη να σχεδιαστούν συστήματα πληροφοριών με επίγνωση στην ασφάλεια πληροφοριών και την προστασία της ιδιωτικότητας, που προστατεύουν από αυτές τις απειλές. Το μάθημα παρέχει ένα ευρύ φάσμα δεξιοτήτων και γνώσεων σχετικά με τις υπάρχουσες τεχνολογίες, αρχές ασφάλειας και απορρήτου για την ανάπτυξη των επαγγελματικών δεξιοτήτων που απαιτούνται για την ασφάλεια των πληροφοριακών συστημάτων. Τα θέματα που καλύπτονται περιλαμβάνουν:

- Βασικά στοιχεία για την ασφάλεια στον κυβερνοχώρο.
- Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών.
- Πλαίσια Κυβερνοασφάλειας.
- Διαχείριση Κινδύνων Ασφάλειας Πληροφοριών.
- Απειλές και ευπάθειες.
- Πληροφορίες για Κυβερνοαπειλές.
- Εφαρμοσμένη Κρυπτογραφία.
- Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Υβριδική διδασκαλία: Πρόσωπο με πρόσωπο, ασύγχρονο εξ αποστάσεως εκπαιδευτικό υλικό και σύγχρονη εξ αποστάσεως εκπαίδευση

ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές

Χρήση Τ.Π.Ε. στη Διδασκαλία

Κατά τη διάρκεια της εκπαιδευτικής διαδικασίας, χρησιμοποιούνται διάφορα εργαλεία διαχείρισης κινδύνου και εφαρμοσμένης κρυπτογραφίας, μαζί με εκπαιδευτικό υλικό από τον κλάδο και άλλο υλικό που διατίθεται στην πλατφόρμα e-learning.

Η υβριδική μέθοδος διδασκαλίας περιλαμβάνει σύγχρονη μάθηση με την υποστήριξη του εργαλείου τηλεδιάσκεψης Zoom.

Οι μαθητές διδάσκονται μια ποικιλία εργαλείων που σχετίζονται με το περιεχόμενο και το υλικό του μαθήματος, που σχετίζονται κυρίως με τη διαχείριση κινδύνων ασφάλειας πληροφοριών και την εφαρμοσμένη κρυπτογραφία.

Χρήση Τ.Π.Ε. στην Επικοινωνία με τους φοιτητές

- Ανάρτηση εκπαιδευτικού υλικού (διαφάνειες, επιστημονικά άρθρα, ασκήσεις, κτλ.) στη σελίδα του μαθήματος στην ηλεκτρονική πλατφόρμα (Moodle).
- Χρήση ανακοινώσεων μέσω Forum στο Moodle.
- Ζωντανές συναντήσεις μέσω Zoom.
- Επικοινωνία μέσω email.

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	30 ώρες
Ασύγχρονο εξ αποστάσεως εκπαιδευτικό υλικό	30 ώρες
Εργασίες	20 ώρες
Εξετάσεις	2 ώρες
Μη Καθοδηγούμενη Μελέτη	78 ώρες
Σύνολο Μαθήματος	***150 ώρες***

ΚΑΤΑΝΟΜΗ ΥΛΗΣ

Θεωρία/Φροντιστήριο	
Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών.	2 ώρες
Πλαίσια Κυβερνοασφάλειας.	2 ώρες
Διαχείριση Κινδύνων Ασφάλειας Πληροφοριών.	8 ώρες
Απειλές και ευπάθειες.	3 ώρες
Πληροφορίες για Κυβερνοαπειλές.	3 ώρες
Εφαρμοσμένη Κρυπτογραφία.	8 ώρες
Αρχιτεκτονικές Μηδενικής Εμπιστοσύνης.	4 ώρες

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 αξιολόγησης: Αγγλική Η αξιολόγηση συνίσταται σε: ● Επιτυχή παρακολούθηση ασύγχρονου εξ αποστάσεως εκπαιδευτικού υλικού (20%) ● Ατομική εργασία (20%): ○ Διαχείριση Κινδύνων Ασφάλειας Πληροφοριών (10%) ○ Εφαρμοσμένη κρυπτογραφία (10%) ● Γραπτή εξέταση στο τέλος του εξαμήνου (60%). Μέθοδοι Γραπτής Αξιολόγησης: ○ Ερωτήσεις Ανοιχτού Τύπου ○ Ερωτήσεις Πολλαπλής Επιλογής Οι φοιτητές θα πρέπει να επιτύχουν προβιβάσιμο βαθμό στις εργασίες και στην γραπτή εξέταση προκειμένου να ολοκληρώσουν επιτυχώς τις υποχρεώσεις τους για το μάθημα. Τα κριτήρια αξιολόγησης ανακοινώνονται στους φοιτητές κατά την πρώτη διάλεξη και είναι προσβάσιμα στην πλατφόρμα τηλεκπαίδευσης καθ' όλη τη διάρκεια του εξαμήνου.	
ΥΠΟΧΡΕΩΣΕΙΣ ΦΟΙΤΗΤΩΝ *Υποχρεωτική: παρακολούθηση διαλέξεων, εργαστηρίων, φροντιστηρίων, συμμετοχή σε προόδους, εξετάσεις, παράδοση ασκήσεων, παράδοση εργασιών (project) κ.λπ.*		● Υποχρεωτική παρακολούθηση διαλέξεων ● Υποχρεωτική παρακολούθηση ασύγχρονου εξ αποστάσεως εκπαιδευτικού υλικού ● Υποχρεωτική παράδοση εργασιών ● Υποχρεωτική συμμετοχή σε εξετάσεις		

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

1. Security standards applying to all European Commission information systems https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en
2. ENISA Threat and Risk Management https://www.enisa.europa.eu/topics/threat-risk-management
3. NIST Computer Security Resource Center https://www.nist.gov/cyberframework https://csrc.nist.gov/Projects/riskmanagement
4. Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 –Project 645421, D5.4, ECRYPT-CSA, 02/2018. https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf
5. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5
6. Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-021021.pdf?__blob=publicationFile
7. Block Cipher Modes, NIST. https://csrc.nist.gov/projects/block-cipher-techniques/bcm
8. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7, October 1996, 816 pages.

9. Cybersecurity and Infrastructure Security Agency (CISA) -Cybersecurity Division, Zero Trust Maturity Model, June 2021, Version 1.0, https://www.cisa.gov/zero-trust-maturity-model
10. Scott W. Rose, Oliver Borchert, Stuart Mitchell, Sean Connelly, NIST SP 800-207, Zero Trust Architecture, August 2020, https://doi.org/10.6028/NIST.SP.800-207
11. Implementing a Zero Trust Architecture (2nd Preliminary Draft), https://csrc.nist.gov/publications/detail/sp/1800-35/draft