

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ (7)		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB1 01	ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	Α'
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ 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	ΕΒΔΟΜΑΔΙΑΙ ΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑ Σ	ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ	
Διαλέξεις	3		
Ασκήσεις Πράξης	2		
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).	5	8	
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης, γενικών γνώσεων, ανάπτυξης δεξιοτήτων	Ανάπτυξης δεξιοτήτων		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΚΑΝΕΝΑ		
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική και Αγγλική		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	Cscyb.uniwa.gr and eclass (UNIWA Open eClass Επιλογή μαθημάτων)		

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

<p>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</p> <ul style="list-style-type: none"> • 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
<p>Γνώσεις Στο πλαίσιο του μαθήματος, οι φοιτητές και οι φοιτήτριες θα μπορούν:</p> <ul style="list-style-type: none"> • Να αντιλαμβάνονται τα σύγχρονα ζητήματα ασφάλειας πληροφοριακών συστημάτων και τις προκλήσεις σε σύγχρονες επιχειρήσεις και οργανισμούς • Να κατανοούν το πλαίσιο ανάπτυξης ενός συστήματος διοίκησης για την ασφάλεια των πληροφοριών • Να επιδεικνύουν κριτική κατανόηση του πλαισίου σχεδιασμού, εφαρμογής και αξιολόγησης των επιδόσεων των κατάλληλων αντιμέτρων: οργανωτικών, τεχνολογικών, φυσικής ασφάλειας, ανθρώπινου παράγοντα • Να διαθέτουν αυξημένες γνώσεις των ιδιαίτερων χαρακτηριστικών που εμφανίζουν τα αντίμετρα σε περιβάλλον νέφους • Να επιδεικνύουν κριτική κατανόηση της μεθοδολογίας της διαχείρισης κινδύνων για την ασφάλεια των πληροφοριών

- Να κατανοούν τα σύγχρονα προβλήματα που εγείρονται κατά την επεξεργασία προσωπικών δεδομένων και να γνωρίζουν τις μεθοδολογίες προστασίας δεδομένων ήδη από τον σχεδιασμό
- Να 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 αναγνώριση των σημαντικών ζητημάτων ασφάλειας πληροφοριακών 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 πληροφοριακών 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 πληροφοριακών συστημάτων
- Να αρθρώνουν επαγωγικά, με επιστημονικά τεκμηριωμένο τρόπο, λύσεις στα σύνθετα προς επίλυση προβλήματα από τον χώρο της ασφάλειας πληροφοριακών 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

Προσαρμογή σε νέες καταστάσεις

Λήψη αποφάσεων

Αυτόνομη εργασία

Ομαδική εργασία

Εργασία σε διεθνές περιβάλλον

Εργασία σε διεπιστημονικό περιβάλλον

Παραγωγή 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

.....

Άλλες...

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

<p><u>Θεωρητικό Μέρος Μαθήματος</u></p> <p>Διάλεξη 1 Εισαγωγή σε θέματα Ασφάλειας (security) πληροφοριακών και επικοινωνιακών συστημάτων. Ορολογία και ISO 27000:2018.</p> <p>Διάλεξη 2 Αυθεντικοποίηση (authentication) οντοτήτων. Εξουσιοδότηση (authorization) και Έλεγχος προσπέλασης (access control): Mandatory Access Control, Discretionary Access Control (Access Control Matrix, Access Control List, Capabilities List), Role-based Access Control (Core, Hierarchical, Constrained).</p> <p>Διάλεξη 3 Σύστημα Διοίκησης για την Ασφάλεια Πληροφοριών (Information Security Management System ISMS) και ISO 27001:2022.</p> <p>Διάλεξη 4 Αντίμετρα (controls) και ISO 27002:2022.</p> <p>Διάλεξη 5 Οδηγίες υλοποίησης ISMS και ISO 27003:2017.</p> <p>Διάλεξη 6 Καλές πρακτικές για υλοποίηση αντιμέτρων στο Νέφος (cloud) και ISO 27017: 2015.</p> <p>Διάλεξη 7 Καθοδήγηση για τη Διοίκηση Επικινδυνότητας της Ασφάλειας των Πληροφοριών (information security risk management) και ISO 27005:2022.</p> <p>Διάλεξη 8 Οδηγίες διοίκησης για την ασφάλεια πληροφοριών στην Κυβερνοασφάλιση (cyberinsurance) και ISO 27102:2019.</p> <p>Διάλεξη 9 Ετοιμότητα τεχνολογιών πληροφορικής και επικοινωνιών (ICT readiness) και ISO 27031:2011 για την επιχειρησιακή συνέχεια (business continuity).</p> <p>Διάλεξη 10 Νομοθετικό και κανονιστικό πλαίσιο για την προστασία προσωπικών δεδομένων: General Data Protection Regulation και ISO 29100:2017.</p> <p>Διάλεξη 11 Οδηγία e-Privacy 2002/58. Οδηγία περί διατήρησης δεδομένων (data retention) 2006/24.</p> <p>Διάλεξη 12 Νομοθετικό και κανονιστικό πλαίσιο για το απόρρητο των ηλεκτρονικών επικοινωνιών. Σύνταγμα της Ελλάδος, άρθρο 19. Εθνική νομοθεσία: ν.5002/2022, ν.3115/2003. Κατασκοπευτικό λογισμικό (spyware) και τρόποι αντιμετώπισης.</p> <p><u>Εργαστηριακό Μέρος Μαθήματος</u></p> <p>Διάλεξη 13 Μελέτες περίπτωσης σε θέματα Enterprise Risk Management, Personal Data Protection, Electronic Communication Security</p>	
---	--

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

<p>ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ <i>Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.</i></p>	<p>Πρόσωπο με πρόσωπο</p>	
<p>ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ <i>Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές</i></p>	<ul style="list-style-type: none"> • Προβολικό σύστημα και δυνατότητα παρουσίασης με την εφαρμογή προγράμματος Power Point • Internet connection • Χρήση HEAL-LINK, scopus, google scholar κ.α. • Χρήση ηλεκτρονικού ταχυδρομείου και της ιστοσελίδας του Τμήματος για την επικοινωνία με τους φοιτητές και την ενημέρωσή τους • Χρήση του eclass του μαθήματος 	
<p>ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ <i>Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας. Διαλέξεις, Σεμινάρια, Εργαστηριακή</i></p>	<p>Δραστηριότητα</p>	<p>Φόρτος Εργασίας Εξαμήνου</p>

<p>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.</p> <p>Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης σύμφωνα με τις αρχές του ECTS</p>	Διαλέξεις	39
	Ασκήσεις πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών, καθώς και ανάλυση μελέτων	51
	Εκπόνηση εργασίας	50
	Αυτοτελής μελέτη	60
	Σύνολο Μαθήματος (25 ώρες ανά πιστωτική μονάδα)	200
<p>ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ</p> <p>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</p> <p>Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.</p>	<p>Γραπτή τελική εξέταση (100%) ή 2 Εξετάσεις Προόδου (30% +30%) και Τελική Εξέταση (40%) που περιλαμβάνουν επίλυση προβλημάτων της ύλης</p> <p>Κάθε άσκηση/πρόβλημα των εξετάσεων έχει διαφορετική βαθμολογία, η οποία ανακοινώνεται στους φοιτητές κατά την εξέταση</p>	

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

<p>Προτεινόμενη Βιβλιογραφία</p> <p>ΑΓΓΛΙΚΗ</p> <ul style="list-style-type: none"> • <i>Security Engineering A Guide to Building Dependable Distributed Systems</i>, R. Anderson, J. Wiley & Sons, 3rd edition, 2020 • <i>The Cyber Security Handbook</i>, A. Calder, ITGP, 2020 • <i>Cybersecurity</i>, E. Lewis, 2020 • <i>The Age of Surveillance Capitalism</i>, S. Zuboff, Profile Books, 2019 • <i>Computer Security</i>, D. Gollmann, J. Wiley & Sons, 3rd edition, 2018 <p>ΕΛΛΗΝΙΚΗ</p> <ul style="list-style-type: none"> • <i>Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο</i>, Σ. Κάτσικας, Σ. Γκρίτζαλης, Κ. Λαμπρινουδάκης (Επισ. Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών, 2021 • <i>Διαχείριση της Ασφάλειας Πληροφοριών</i>, Σ. Κάτσικας, Εκδόσεις Πεδίο, 2014 • <i>Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών</i>, Κ. Λαμπρινουδάκης, Α. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας (Επισ. Επιμέλεια), Εκδόσεις Παπασωτηρίου, 2010 <p>Συναφή επιστημονικά περιοδικά:</p> <ul style="list-style-type: none"> • 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
--

