ΚΑΝΟΝΕΣ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB102	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**1ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΚΑΝΟΝΕΣ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ**		

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	
Ασκήσεις Πράξης	2	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.	**5**	**7**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Ανάπτυξης Δεξιοτήτων, Υποβάθρου*
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	Cscyb.uniwa.gr UNIWA Open eClass | ΚΑΝΟΝΕΣ και ΠΡΩΤΟΚΟΛΛΑ ΚΥΒΕΡΝΟΑΣ...

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*
Οι φοιτητές μπορούν να - να κατανοήσουν το σκοπό, το πεδίο εφαρμογής και τη σημασία των διαφόρων κανόνων - απομνημονεύουν βασικούς όρους, ορισμούς και θεμελιώδεις αρχές των προτύπων κυβερνοασφάλειας. Αυτό το επίπεδο βοηθά στην οικοδόμηση μιας θεμελιώδους κατανόησης των εννοιών ασφάλειας των προτύπων κυβερνοασφάλειας. - αναλύουν τη δομή, τα συστατικά στοιχεία και τις απαιτήσεις των προτύπων κυβερνοασφάλειας - αξιολογούν τα πρότυπα κυβερνοασφάλειας, λαμβάνοντας υπόψη τα δυνατά και αδύνατα σημεία τους και τη συνάφεια με συγκεκριμένες οργανωτικές ανάγκες.

- εφαρμόζουν τα πρότυπα κυβερνοασφάλειας σε πραγματικές καταστάσεις
- Περιγράφουν, τις μεθόδους που χρησιμοποιούνται για την έναρξη ενός πρωτοκόλλου
- επιδεικνύουν, την ικανότητα επιλογής του κατάλληλου πρωτοκόλλου
- τροποποιούν ένα πρωτόκολλο προκειμένου να επικαιροποιεί το περιεχόμενό του.
- συγκρίνουν παρόμοια πρωτόκολλα.
- αναπτύσσουν από την αρχή ένα πρωτόκολλο με όλες τις αρμόδιες επιτροπές.
- αποφασίζουν, σχετικά με την επιλογή πρωτοκόλλου σε ένα δεδομένο έργο που πρόκειται να αναλάβουν

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	
Παραγωγή νέων ερευνητικών ιδεών	

Ανάκληση βασικών γεγονότων και εννοιών σχετικά με τα πρότυπα κυβερνοασφάλειας
Χρήση προτύπων κυβερνοασφάλειας σε συγκεκριμένα πλαίσια ή σενάρια
Εξετάζουν και να αναλύουν τα πρότυπα κυβερνοασφάλειας για να κατανοούν τα συστατικά τους στοιχεία.
Αξιολογούν την αποτελεσματικότητα και την καταλληλότητα των προτύπων ασφάλειας στον κυβερνοχώρο Να αναπτύσσουν καινοτόμες λύσεις ή στρατηγικές με βάση τα πρότυπα ασφάλειας στον κυβερνοχώρο.
Κατανοούν το νόημα και τη σημασία των προτύπων ασφάλειας στον κυβερνοχώρο.

ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Θεωρητικό Μέρος Μαθήματος:
Η περιγραφή περιέχει την ύλη που θα καλυφθεί κατά τη διάρκεια των 13 εβδομάδων

1) Περιγραφή των πρωτοκόλλων και των προτύπων
2) Επικεφαλής οργανισμοί στα πρωτόκολλα κυβερνοασφάλειας, Η ιεραρχία στην παραγωγή πρωτοκόλλων
3) Βασικά στοιχεία BOT, Πρωτόκολλα για την αυτοκινητοβιομηχανία (π.χ. FlexRay, SAE J2735)
4) Πρωτόκολλα τηλεπικοινωνιών
5) Πρωτόκολλα και πρότυπα ναυτιλιακής ασφάλειας στον κυβερνοχώρο, κώδικας δεοντολογίας της TN
6) FIPS, ILIT
7) Διακυβέρνηση, κίνδυνος και συμμόρφωση (ERNEST YOUNG) και αξιόπιστη ασφάλεια υπολογιστών, Medi Seciurity
8) ΓΚΠΔ, προστασία προσωπικών δεδομένων GRC ()
9) CERT, NIST, NIS, NERC
10) Κοινά κριτήρια (ISO 15408) και Πορτοκαλί βιβλίο

11) Πρωτόκολλα δικτύου
12) Πρωτόκολλα και πρότυπα κινητής τηλεφωνίας για την ασφάλεια στον κυβερνοχώρο
13) Πρωτόκολλα και πρότυπα νοσοκομειακής κυβερνοασφάλειας

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*	• Προβολικό σύστημα και δυνατότητα παρουσίασης με την εφαρμογή του Προγράμματος Power Point, • Δυνατότητα σύνδεσης με internet, • Χρήση μηχανών αναζήτησης βιβλιογραφίας HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR • Χρήση ηλεκτρονικού ταχυδρομείου και της ιστοσελίδας του Τμήματος για την επικοινωνία με τους φοιτητές και την ενημέρωσή τους • Χρήση του eclass του μαθήματος
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***
Lectures	39
Ασκήσεις Πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών και ανάλυση μελετών	26
Εκπόνηση εργασίας	*50*
Αυτοτελής Μελέτη	60
Total Course Load (25 hours per credit)	**175**

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. Multiple choice questions (40%) II. Class Participation (20%) III. Research work on a standard (40%)

ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- *Προτεινόμενη Βιβλιογραφία:*

1) *Cybersecurity Risk Management - Mastering the Fundamentals Using the NIST, Cynthia Brumfield, Brian Haugli, WILEY, 2021*
2) *5G Cybersecurity Standards, ENISA, 2022*

3) *"NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations" by Ron Ross, Stu Katzke, Arnold Johnson, National Institute of Standards and Technology, 2020*
4) *ISO 27001/27002: A Pocket Guide" by Alan Calder, IT Governance Publishing, 2008*
5) *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide" by Mike Chapple, James Michael Stewart, and Darril Gibson, 7th ed. John Wiley and Sons, 2015*
6) *Cybersecurity for Hospitals and Healthcare Facilities, Ayala Luis, Apress, 2016*
7) *Biometric-Based Physical and Cybersecurity Systems, Obaidat, Traore, Wouhgang (eds), Springer Nature Switzerland AG, 2018*
8) *Effective Cybersecurity: a Guide to Using Best Practices and Standards, William Stallings, 2018*
9) *Automotive Cyber Security: Introduction, Challenges, and Standardization, Kim S., Shrestha R., Springer, 2020*
10) *The Ultimate Guide to Cybersecurity Planning for Businesses, 2020*
11) *Derived Test Requirements for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (Author), 2011*
12) *Cybercrime and Cyber Warfare, Igor Bernik, ISTE Ltd and John Wiley & Sons Inc, 2013*
13) *Cyber Security Essentials, Rick Howard, Taylor & Francis Inc, 2010*
14) *Handbook of Biometrics for Forensic Science (Advances in Computer Vision and Pattern Recognition), 2018, Massimo Tistarelli (Editor), Christophe Champod (Editor)*
15) *Handbook of Vascular Biometrics (Advances in Computer Vision and Pattern Recognition), 2019, Andreas Uhl (Editor), Christoph Busch (Editor), Sébastien Marcel (Editor), Raymond Veldhuis (Editor)*

Webliography
https://www.itgovernanceusa.com/cybersecurity-standards
https://www.enisa.europa.eu