ΑΣΦΑΛΕΙΑ ΥΛΙΚΟΥ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB201	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**2ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΥΛΙΚΟΥ**		

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	1	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.	**4**	**8**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Υποχρεωτικό, Εξειδικευμένες γενικές γνώσεις*
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	Cscyb.uniwa.gr and eclass (UNIWA Open eClass | Επιλογή μαθημάτων)

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 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*

Σκοπός αυτού του μαθήματος είναι να παρέχει στους μεταπτυχιακούς φοιτητές τις κατάλληλες γνώσεις και δεξιότητες σχετικά με τα κύρια θέματα της ασφάλειας υλικού, συμπεριλαμβανομένων των τρωτών σημείων του υλικού, των επιθέσεων και των κατάλληλων μηχανισμών προστασίας. Με την επιτυχή ολοκλήρωση αυτού του μαθήματος, οι φοιτητές θα είναι σε θέση να:

- Διατυπώνουν τις απαιτήσεις ασφάλειας υλικού για ένα σύστημα.
- Περιγράφουν τους τύπους σφαλμάτων, ελαττωμάτων και κινδύνων σε ένα σύστημα και τον τρόπο αντιμετώπισής τους και να επιλέγουν τις κατάλληλες μεθόδους για την αντιμετώπισή τους.
- Περιγράφουν και εφαρμόζουν μεθόδους ανάλυσης της ασφάλειας υλικού.
- Περιγράφουν και εφαρμόζουν μεθόδους αξιολόγησης της ασφάλειας υλικού.
- Σχεδιάζουν ψηφιακά κυκλώματα για κρυπτογραφικές εφαρμογές.

- Σχεδιάζουν κυκλώματα που θα περιέχουν ενσωματωμένες δοκιμαστικές δομές για εύκολο έλεγχο.
- Ελέγχουν τα κυκλώματα για ελαττώματα ή επιβλαβείς πρόσθετες συνιστώσες υλικού.

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	

Το μάθημα στοχεύει στις ακόλουθες γενικές ικανότητες:

- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών με τη χρήση της απαραίτητης τεχνολογίας
- Ατομική εργασία
- Ομαδική εργασία
- Εργασία σε διεθνές περιβάλλον
- Λήψη απόφασης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Η περιγραφή περιέχει το υλικό που θα καλυφθεί κατά τη διάρκεια 13 διαλέξεων.
Διαλέξεις 1-2: Εισαγωγή και βασικές έννοιες, εξέλιξη της ασφάλειας υλικού, επισκόπηση και επίπεδα ενός υπολογιστικού συστήματος, τύποι ηλεκτρονικού υλικού, ασφάλεια υλικού έναντι εμπιστοσύνης υλικού, ασφάλεια και δοκιμή/εντοπισμός σφαλμάτων, ηλεκτρονική αλυσίδα εφοδιασμού.
Διαλέξεις 3-4: Εισαγωγή στην κρυπτογράφηση και ασφάλεια δεδομένων, πρότυπα κρυπτογράφησης δεδομένων (DES, AES) και κρυπταλγόριθμοι τμήματος, κρυπτογράφηση δημόσιου κλειδιού και αλγόριθμος ασύμμετρου κλειδιού RSA.
Διάλεξη 5: Βασικά στοιχεία σχεδίασης και δοκιμής VLSI
Διάλεξη 6: Φυσικές επιθέσεις
Διάλεξη 7: Πειρατεία πνευματικής ιδιοκτησίας υλικού και αντίστροφη μηχανική
Διάλεξη 8: Επιθέσεις πλευρικού καναλιού
Διάλεξη 9: Δούρειοι Ίπποι Υλικού
Διάλεξη 10: Επιθέσεις σε PCB, RFID και JTAG
Διαλέξεις 11-12: Βασικές τεχνολογίες ασφάλειας υλικού, φυσικές μη κλωνοποιήσιμες συναρτήσεις (PUF) και γεννήτριες πραγματικά τυχαίων αριθμών (TRNG)
Διάλεξη 13: Μέτρηση υλικού και ψηφιακή υδατοσήμανση

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Αυτό το μάθημα διδάσκεται μέσω ενός συνδυασμού διαλέξεων, ασκήσεων, συνεδριών

<table>
<tr><td></td><td>εργαστηρίου υπολογιστών και ασκήσεων.</td></tr>
<tr><td>ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές</td><td>• 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</td></tr>
<tr><td>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</td><td>
<table>
<tr><th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr>
<tr><td>Lectures</td><td>39</td></tr>
<tr><td>Ασκήσεις Πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών και ανάλυση μελετών</td><td>30</td></tr>
<tr><td>Εκπόνηση εργασίας</td><td>41</td></tr>
<tr><td>Αυτοτελής Μελέτη</td><td>90</td></tr>
<tr><td>Total Course Load
(25 hours per credit)</td><td>200</td></tr>
</table>
</td></tr>
<tr><td>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.</td><td>I. Εργασία 1 (50%) και
II. Εργασία 2 (50%)</td></tr>
</table>

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- S. Bhuniaand, M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Morgan Kaufmann–Elsevier, 1st edition, 2018.
- Introduction to Hardware Security and Trust, First Edition, Mohammad Tehranipoor and Cliff Wang (Ed.) (2012), Springer, ISBN-13: 978-1-4419-8079-3 or ISBN-10: 1-4419-8079-2 or e-ISBN: 978-1-4419-8080-9.
- Towards Hardware-Intrinsic Security, First Edition, Ahmad-Reza Sadeghi and David Naccache (Eds.) (2010), Springer, ISBN-13: 978-3-642-14451-6 or ISBN-10: 3-642-14451-9 or e-ISBN: 978-3-642-14452-3.
- Fault-Tolerant Systems, First Edition, Israel Koren and C. Mani Krishna (2007),

Elsevier Morgan Kaufmann Publishers, ISBN-13: 978-0-12-088525-1 or ISBN-10: 0-12-088525-5

- Fundamentals of Dependable Computing for Software Engineers, John Knight, CRC press, 2012.
- Fault-Tolerant Design, Elena Dubrova, Springer, 2013.
- Building Dependable Distributed Systems, Wenbing Zhao, Willey publications.
- Developing Green Software, Dr. Bob Steigerwald and Abhishek Agrawal, Intel Corporation.
- Dependability benchmarking for Computer Systems, Karama Kanoun and Lisa Spainhower (eds), Willey publications & IEEE Computer Society.
- Dependable Computing: Design and Assessment, Ravishankar K. Iyer, Zbigniew T. Kalbarczyk, Nithin M. Nakka, Wiley, 2016.
- Dependable computer systems, Assen V. Krumov, CreateSpace Independent Publishing Platform, 2013.
- Computer Architecture Techniques For Power-Efficiency, Stefanos Kaxiras and Margaret Martonosi, Morgan & Claypool, 2008.
- System-Level Design Techniques For Energy-Efficient Embedded Systems, Marcus T. Schmitz, Bashir M. Al-Hashimi and Petru Eles, Springer 2009.
- Power-efficient System Design, Preeti Ranjan Panda, B. V. N. Silpa, Aviral Shrivastava, Krishnaiah Gummidipudi, Springer 2010.
- Low power design essentials, J. Rabaey, Springer 2009.