

## ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

### 1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ICE-6002	ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	6 <sup>ο</sup>
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ		
<b>ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ</b> 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		<b>ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ</b>	<b>ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ</b>
Διαλέξεις		3	
Εργαστήριο		1	
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο 4.		4	5
<b>ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ</b> Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων	Επιστημονικής Περιοχής, Ανάπτυξης δεξιοτήτων		
<b>ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:</b>	Λειτουργικά Συστήματα		
<b>ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:</b>	Ελληνική		
<b>ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS</b>	Όχι		
<b>ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)</b>			

### 2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

<p><b>Μαθησιακά Αποτελέσματα</b> 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.</p> <p>Συμβουλευτείτε το Παράρτημα Α</p> <ul style="list-style-type: none"> <li>• Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης</li> <li>• Περιγραφικοί Δείκτες Επιπέδων 6, 7 &amp; 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και Παράρτημα Β</li> <li>• Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων</li> </ul> <p>Το μάθημα καλύπτει το γενικό μέρος της επιστημονικής περιοχής της Ασφάλειας στην Τεχνολογία της Πληροφορίας. Σκοπός του μαθήματος είναι η δημιουργία ενός ευρύτατου πλαισίου θεωρητικών και πρακτικών γνώσεων, το οποίο θα αποτελέσει για το φοιτητή εφόδιο στην αγορά εργασίας στον τομέα της Ασφάλειας στην Τεχνολογία της Πληροφορίας.</p> <p>Με την επιτυχή ολοκλήρωση του μαθήματος αυτού, ο φοιτητής:</p>
--

- Θα γνωρίζει τα προβλήματα ασφάλειας σε Πληροφοριακά και Επικοινωνιακά Συστήματα,
- Θα αναγνωρίζει τις ευπάθειες των πληροφοριακών και επικοινωνιακών συστημάτων,
- Θα είναι σε θέση να εφαρμόσει βασικές αρχές σχεδιασμού πολιτικών ασφαλείας,
- Θα γνωρίζει τα χαρακτηριστικά και τους μηχανισμούς ασφαλείας που υλοποιούν τις πολιτικές αυτές,
- Θα έχει εξοικειωθεί με παραδείγματα που υλοποιούν και εφαρμόζουν μηχανισμούς ασφαλείας σε διαφορετικά Λειτουργικά Συστήματα,
- Θα έχει γνώσεις από Ασφάλεια Βάσεων Δεδομένων,
- Θα γνωρίζει τα διαφορετικά είδη firewalls και πώς αυτά χρησιμοποιούνται και εφαρμόζονται,
- Θα γνωρίζει μηχανισμούς αυθεντικοποίησης, το ρόλο και τη σπουδαιότητά τους,
- Θα έχει εξοικειωθεί με τα ComputerForensics και θα έχει γνώση των εργαλείων που τα υποστηρίζουν,
- Θα γνωρίζει κρυπτογραφία και κρυπτανάλυση, και τέλος,
- Θα έχει κατανοήσει τα Συστήματα Ανίχνευσης Εισβολών, τον τρόπο λειτουργίας τους και τις τεχνικές που χρησιμοποιούνται σε αυτά.

#### **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;*

<i>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</i>	<i>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</i>
--	--

- Αυτόνομη Εργασία,
- Ομαδική Εργασία,
- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών και εργαλείων,
- Προγραμματισμός απλών μηχανισμών ασφαλείας,
- Παραγωγή νέων ερευνητικών ιδεών.

### **3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ**

- Γενικά Θέματα Ασφάλειας στην Τεχνολογία της Πληροφορίας (IT Security)
- Κρυπτογραφία I (Cryptography I)
- Κρυπτογραφία II (Cryptography II)
- Προστασία Λειτουργικών Συστημάτων (Operating Systems Protection)
- Ασφάλεια Βάσεων Δεδομένων (Data Base Security)
- Έλεγχος Πρόσβασης (Access Control)
- Ασφάλεια Δικτύων και Κατανεμημένων Συστημάτων (Network and Distributed Systems Security)
- Ασφάλεια Διαδικτύου (InternetSecurity)
- Ανίχνευση ΕπιθέσεωνI (Intrusion Detection I)
- Ανίχνευση ΕπιθέσεωνII (Intrusion Detection II)
- Computer Forensics
- Ανάλυση Επικινδυνότητας (RiskAnalysis)
- Διαχείριση Ασφάλειας (SecurityManagement)

- Νομικά Θέματα (Legal and Ethical Issues)

#### 4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

<p><b>ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ</b> Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.</p>	<p>Πρόσωπο με πρόσωπο (στην τάξη)</p>													
<p><b>ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ</b> Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές</p>	<p>Εξειδικευμένο λογισμικό για ανίχνευση ευπαθειών, για κρυπτογραφικούς αλγόριθμους, για Computer Forensics, για ασφάλεια Βάσεων Δεδομένων, για Ανίχνευση Εισβολών, για Έλεγχο Πρόσβασης. Υποστήριξη μαθησιακής διαδικασίας μέσω της πλατφόρμας ηλεκτρονικής μάθησης του Πανεπιστημίου.</p>													
<p><b>ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ</b> Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας. Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη &amp; 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 ώστε ο συνολικός φόρτος εργασίας σε επίπεδο εξαμήνου να αντιστοιχεί στα standards του ECTS</p>	<table border="1" data-bbox="699 555 1359 920"> <thead> <tr> <th data-bbox="699 555 1029 629">Δραστηριότητα</th> <th data-bbox="1034 555 1359 629">Φόρτος Εργασίας Εξαμήνου</th> </tr> </thead> <tbody> <tr> <td data-bbox="699 636 1029 667">Διαλέξεις</td> <td data-bbox="1034 636 1359 667">39</td> </tr> <tr> <td data-bbox="699 674 1029 705">Εργαστηριακές ασκήσεις</td> <td data-bbox="1034 674 1359 705">13</td> </tr> <tr> <td data-bbox="699 712 1029 743">Ατομικές εργασίες</td> <td data-bbox="1034 712 1359 743">20</td> </tr> <tr> <td data-bbox="699 750 1029 781">Αυτοτελής Μελέτη</td> <td data-bbox="1034 750 1359 781">53</td> </tr> <tr> <td data-bbox="699 788 1029 920"><b>Σύνολο Μαθήματος</b> (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)</td> <td data-bbox="1034 788 1359 920"><b>125</b></td> </tr> </tbody> </table>		Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου	Διαλέξεις	39	Εργαστηριακές ασκήσεις	13	Ατομικές εργασίες	20	Αυτοτελής Μελέτη	53	<b>Σύνολο Μαθήματος</b> (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	<b>125</b>
Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου													
Διαλέξεις	39													
Εργαστηριακές ασκήσεις	13													
Ατομικές εργασίες	20													
Αυτοτελής Μελέτη	53													
<b>Σύνολο Μαθήματος</b> (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	<b>125</b>													
<p><b>ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ</b> Περιγραφή της διαδικασίας αξιολόγησης</p> <p>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>I. Γραπτή τελική εξέταση θεωρίας (80%) που περιλαμβάνει: Ερωτήσεις συνδυασμού γνώσεων και κρίσεως, με ζητούμενο την κατάλληλη επιχειρηματολογία μέσα από την οποία διαπιστώνεται το βάθος της κατανόησης των θεμάτων που έχουν αποτελέσει αντικείμενο των διαλέξεων της θεωρίας.</p> <p>II. Εργαστηριακές ασκήσεις και γραπτή τελική εξέταση εργαστηρίου (20%) που περιλαμβάνει.</p> <p>III. Επιπλέον (20%) βαθμολογία από τις προαιρετικές ατομικές εργασίες εξάσκησης επί του προβιβασίμου βαθμού γραπτής τελικής εξέτασης θεωρίας.</p>													

Αναφέρονται ρητά  
προσδιορισμένα κριτήρια  
αξιολόγησης και εάν και που είναι  
προσβάσιμα από τους φοιτητές.

## 5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία :

1. Stallings και Brown, Ασφάλεια Υπολογιστών: αρχές και Πρακτικές, 2016, ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ ΕΠΕ, ISBN: 978-960-461-668-8.
2. Γκριτζαλης Σ., Γκριτζαλης Δ., Κάτσικας Σ., Ασφάλεια Δικτύων Υπολογιστών, Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ ΟΕ, 2003, ISBN: 978-960-7530-45-5.
3. Stallings, Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, ΜΑΡΙΑ ΠΑΡΙΚΟΥ & ΣΙΑ ΕΠΕ, 2011, ISBN: 9789604117307.
4. Σουρή Α., Πατσός Δ., Γρηγοριάδης Ν., Ασφάλεια της Πληροφορίας, ΕΚΔΟΣΕΙΣ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΜΟΝ. ΕΠΕ, 2004, ISBN: 960-8105-66-8.
5. Κάτσικας Σ.Κ., Γκριτζαλης Δ., Γκριτζαλης Σ., Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004.
6. Κάττος Β., Στεφανίδης Γ., Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης, ΖΥΓΟΣ, 2003.
7. Bishop M., Computer Security – Art and Science, Addison-Wesley, 2003.
8. Bishop M., Introduction to Computer Security, Addison-Wesley, 2005.
9. Buchmann J., Introduction to Cryptography, 2nd Ed., Springer, 2004.
10. Casey E., Handbook of Computer Crime Investigation – Forensic Tools and Technology, Academic Press, 2002.
11. Mitnick K.D., Simon W.L., The Art of Deception, John Wiley & Sons, 2002.
12. Oppliger R., Security Technologies for the World Wide Web, Artech House Inc., 2000.
13. Pfleeger C.P., LawrencePfleeger S., Security in Computing, Prentice Hall, 2003.
14. Pieprzyk J., Hardjono T., Seberry J., Fundamentals of Computer Security, Springer, 2003.
15. Proctor P.E., The Practical Intrusion Detection Handbook, Prentice Hall, 2001.
16. Riggs G., Network Perimeter Security – Building Defense In-Depth, Auerbach, 2004.
17. Schultz E.E., Shumway R., Incident Response – A Strategic Guide to Handling System and Network Security Breaches, New Riders Publishing, 2002.
18. Spitzner L., Honeypots – Tracking Hackers, Addison Wisley, 2003.
19. Young S., Aitel D., The Hacker’s Handbook – The Strategy behind Breaking into and Defending Networks, Auerbach, 2004.

## 6. ΒΙΒΛΙΑ ΕΥΔΟΞΟΣ

1. Βιβλίο [94701556]: Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο, Σωκράτης Κάτσικας, Στέφανος Γκριτζαλης, Κωνσταντίνος Λαμπρινουδάκης [Λεπτομέρειες](#)
2. Βιβλίο [50656354]: ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ: ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ, WILLIAM STALLINGS, LAWRIE BROWN [Λεπτομέρειες](#)
3. Βιβλίο [9675]: Ασφάλεια Δικτύων Υπολογιστών, Γκριτζαλης Στέφανος, Γκριτζαλης Δημήτρης Α., Κάτσικας Σωκράτης [Λεπτομέρειες](#)