ΕΦΗΜΕΡΙΔΑ
ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ
ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

7 Φεβρουαρίου 2024 | ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ | Αρ. Φύλλου **878**

ΑΠΟΦΑΣΕΙΣ

Αριθμ. 5275

Έγκριση Τροποποίησης του Κανονισμού Λειτουργίας του Ξενόγλωσσου Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με: Ελληνικό Τίτλο: «Κυβερνοασφάλεια» και Αγγλικό Τίτλο: «Cybersecurity», μεταξύ: του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, του Πανεπιστημίου USARB (Universitatea de Stat "Alecu Russo" din Balti) (Balti-Μολδαβία), του Πανεπιστημίου UTM (The Technical University of Moldova) Chisinau- Μολδαβία), του Πανεπιστημίου USM (Moldova State University) (Chisinau - Μολδαβία) και της Ακαδημίας ASEM (Academy of Economic Studies of Moldova) (Chisinau-Μολδαβία).

Η ΣΥΓΚΛΗΤΟΣ ΤΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

Λαμβάνοντας υπόψη:

1. Τις διατάξεις του ν. 4521/2018 «Ίδρυση Πανεπιστημίου Δυτικής Αττικής και Άλλες Διατάξεις» (Α' 38).

2. Τις διατάξεις του ν. 4610/2019 «Συνέργειες Πανεπιστημίων και Τ.Ε.Ι., πρόσβαση στην τριτοβάθμια εκπαίδευση, πειραματικά σχολεία, Γενικά Αρχεία του Κράτους και λοιπές διατάξεις» (Α' 70).

3. Τις διατάξεις του ν. 4957/2022 «Νέοι Ορίζοντες στα Ανώτατα Εκπαιδευτικά Ιδρύματα: Ενίσχυση της Ποιότητας, της Λειτουργικότητας και της Σύνδεσης των Α.Ε.Ι. με την Κοινωνία και Λοιπές Διατάξεις» (Α' 141) και ιδίως των άρθρων 79 έως 88.

4. Τον Εσωτερικό Κανονισμό λειτουργίας του Πανεπιστημίου Δυτικής Αττικής, με τις τροποποιήσεις του (Β' 4621/2020).

5. Τον Πρότυπο Κανονισμό Σπουδών των Π.Μ.Σ. του Πα.Δ.Α. «Έγκριση Κανονισμού Λειτουργίας των Προγραμμάτων Μεταπτυχιακών Σπουδών του Πανεπιστημίου Δυτικής Αττικής» (Β' 4861/2023).

6. Την υπό στοιχεία 135557/Ζ1/1-11-2022 εγκύκλιο του Υπουργείου Παιδείας και Θρησκευμάτων, σχετικά με την: «Εφαρμογή των διατάξεων του ν. 4957/2022 «Νέοι Ορίζοντες στα Ανώτατα Εκπαιδευτικά Ιδρύματα: Ενίσχυση της Ποιότητας, της Λειτουργικότητας και της Σύνδεσης των Α.Ε.Ι. με την κοινωνία και λοιπές διατάξεις" για την οργάνωση και λειτουργία προγραμμάτων μεταπτυχιακών σπουδών και λοιπά θέματα».

7. Την υπό στοιχεία 108990/Ζ1/08-09-2022 υπουργική απόφαση του Υφυπουργού Παιδείας και Θρησκευμάτων «Ρύθμιση των θεμάτων σχετικά με τη διαδικασία δωρεάν φοίτησης σε Πρόγραμμα Μεταπτυχιακών Σπουδών με τέλη φοίτησης» (Β' 4899).

8. Την υπό στοιχεία 18137/Ζ1/16-02-2023 κοινή υπουργική απόφαση των Υπουργών Παιδείας και Θρησκευμάτων - Επικρατείας «Καθορισμός των προϋποθέσεων και της διαδικασίας οργάνωσης Προγραμμάτων Μεταπτυχιακών Σπουδών με μεθόδους εξ αποστάσεως Εκπαίδευσης στα Ανώτατα Εκπαιδευτικά Ιδρύματα (Α.Ε.Ι.)» (Β' 1079).

9. Την υπ' αρ. 46969/12-05-2023 διαπιστωτική Πράξη του Αντιπρύτανη Έρευνας και Δια Βίου Εκπαίδευσης του Πανεπιστημίου Δυτικής Αττικής «Εκλογή Πρύτανη του Πανεπιστημίου Δυτικής Αττικής» (Υ.Ο.Δ.Δ. 454).

10. Την υπ' αρ. 77275/1-09-2023 (Υ.Ο.Δ.Δ. 921) πράξη του Πρύτανη του Πανεπιστημίου Δυτικής Αττικής «Ορισμός Αντιπρυτάνεων, Τομέων Ευθύνης Αυτών, Κατανομής Αρμοδιοτήτων και Σ-ειράς Αναπλήρωσης του Πρύτανη του Πανεπιστημίου Δυτικής Αττικής», καθώς και την υπ' αρ. 94297/12-10-2023 (Υ.Ο.Δ.Δ. 1141) τροποποίηση αυτής.

11. Την υπ' αρ. 124685/22-12-2022 απόφαση του Πρύτανη του Πανεπιστημίου Δυτικής Αττικής σχετικά με τη «Συγκρότηση της Επιτροπής Μεταπτυχιακών Σπουδών του Πανεπιστημίου Δυτικής Αττικής» (ΑΔΑ: 66ΥΚ46Μ9ΞΗ-Θ9Ξ), καθώς και την υπ' αρ. 86982/28-9-2023 (ΑΔΑ: 6ΡΡ846Μ9ΞΗ-ΝΞΦ) απόφαση Ανασυγκρότησης αυτού.

12. Την υπ' αρ. 80818/12-09-2023 (ΑΔΑ: 9ΖΥΨ46Μ9ΞΗ-ΘΑΔ) Πράξη του Πρύτανη του Πανεπιστημίου Δυτικής Αττικής «Συγκρότηση της Συγκλήτου του Πανεπιστημίου Δυτικής Αττικής» .

13. Την υπ' αρ. 97386/19-10-2023 (ΑΔΑ: ΨΛΓΧ46Μ9ΞΗ-Ι07) Πράξη του Πρύτανη «Ανασυγκρότηση της Συγκλήτου του Πανεπιστημίου Δυτικής Αττικής».

14. Την υπ' αρ. 121813/18-03-2019 απόφαση της Διοικούσας Επιτροπής του Πανεπιστημίου Δυτικής Αττικής «Έγκριση Δριϊδρυματικού Προγράμματος Με-

ταπτυχιακών Σπουδών με τίτλο «Μεταπτυχιακή Εξειδίκευση στην Κυβερνοασφάλεια» (Β’ 1038) του τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών», όπως αυτή τροποποιήθηκε με την υπ’ αρ. 69633/2-10-2020 (Β’ 4462) απόφαση της Συγκλήτου του Πανεπιστημίου Δυτικής Αττικής.

15. Την υπ’ αρ. 37870/21-07-2019 απόφαση της Διοικούσας Επιτροπής του Πανεπιστημίου Δυτικής Αττικής «Κανονισμός Σπουδών του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Π.Μ.Σ.) με τίτλο “Κυβερνοασφάλεια” του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής» (Β’ 3150), όπως αυτή τροποποιήθηκε με την υπ’ αρ. 69634/02-10-2020 (Β’ 4462) απόφαση της Συγκλήτου του Πανεπιστημίου Δυτικής Αττικής.

16. Τα «Ειδικά Πρωτόκολλα Συνεργασίας» μεταξύ του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστήμιου Δυτικής Αττικής, καθώς και των Ιδρυμάτων της Μολδαβίας και του Καζακστάν, του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο: «Κυβερνοασφάλεια».

17. Το υπ’ αρ. 04/21-12-2023 (θέμα 1ον) απόσπασμα Πρακτικού της απόφασης της Επιτροπής Προγράμματος Σπουδών του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο «Κυβερνοασφάλεια» με θέμα: «Έγκριση τροποποίησης της ίδρυσης και του νέου Κανονισμού Λειτουργίας του ΔΠΜΣ με τίτλο “Κυβερνοασφάλεια” σύμφωνα με τον ν. 4957/2022 και τον πρότυπο Κανονισμό λειτουργίας Μεταπτυχιακών Σπουδών του ΠΑΔΑ».

18. Το υπ’ αρ. 2/15-01-2024 (θέμα 2ο) απόσπασμα Πρακτικού της Επιτροπής Μεταπτυχιακών Σπουδών «Εισήγηση για την έγκριση της τροποποίησης της ίδρυσης και του Εσωτερικού Κανονισμού Λειτουργίας του Διϊδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με τίτλο “Κυβερνοασφάλεια” μεταξύ του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής και των Ιδρυμάτων της Μολδαβίας και του Καζακστάν, σύμφωνα με τον ν. 4957/2022 (Α’ 141) και τον Πρότυπο Κανονισμού Λειτουργίας των Προγραμμάτων Μεταπτυχιακών Σπουδών του Πανεπιστημίου Δυτικής Αττικής (Β’ 4861/2023)».

19. Την υπ’ αρ. 3810/22-01-2024 (θέμα 15ο) απόφαση της Συγκλήτου του Πανεπιστημίου Δυτικής Αττικής, με θέμα: «Έγκριση Τροποποίησης του Κανονισμού Λειτουργίας του Ξενόγλωσσου Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με: Ελληνικό Τίτλο: “Κυβερνοασφάλεια” και Αγγλικό Τίτλο: “Cybersecurity”, Μεταξύ: του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, του Πανεπιστημίου USARB (Universitatea de Stat "Alecu Russo" din Balti) (Balti-Μολδαβία), του Πανεπιστημίου UTM (The Technical University of Moldova) Chisinau-Μολδαβία), του Πανεπιστημίου USM (Moldova State University) (Chisinau-Μολδαβία) και της Ακαδημίας ASEM (Academy of Economic Studies of Moldova) (Chisinau-Μολδαβία)».

20. Το γεγονός ότι με την παρούσα δεν προκαλείται δαπάνη σε βάρους του κρατικού προϋπολογισμού, αποφασίζει:

Την έγκριση τροποποίησης του Κανονισμού Λειτουργίας του Ξενόγλωσσου Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών με: Ελληνικό Τίτλο: «Κυβερνοασφάλεια» και Αγγλικό Τίτλο: «Cybersecurity», μεταξύ: του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, του Πανεπιστημίου USARB (Universitatea de Stat "Alecu Russo" din Balti) (Balti-Μολδαβία), του Πανεπιστημίου UTM (The Technical University of Moldova) Chisinau-Μολδαβία), του Πανεπιστημίου USM (Moldova State University) (Chisinau-Μολδαβία) και της Ακαδημίας ASEM (Academy of Economic Studies of Moldova) (Chisinau-Μολδαβία), ως ακολούθως:

Άρθρο 1
Γενικές Διατάξεις

Το Διϊδρυματικό Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών (Δ.Δ.Π.Μ.Σ.) με ελληνικό τίτλο «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» και αγγλικό τίτλο «Cybersecurity», του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, της Σχολής ΜΗΧΑΝΙΚΩΝ, λειτουργεί με τη συμμετοχή τεσσάρων (4) Ιδρυμάτων της Μολδαβίας: (1) Πανεπιστήμιο USARB (Universitatea de Stat "Alecu Russo" din Balti) (Balti-Μολδαβία), (2) Πανεπιστήμιο UTM (The Technical University of Moldova) Chisinau-Μολδαβία), (3) Πανεπιστήμιο USM (Moldova State University) (Chisinau-Μολδαβία) και (4) Ακαδημία ASEM (Academy of Economic Studies of Moldova) (Chisinau-Μολδαβία) και εντάσσεται στο πλαίσιο των σκοπών και της γενικότερης αποστολής του Πανεπιστημίου Δυτικής Αττικής (Πα.Δ.Α.).

Το Δ.Δ.Π.Μ.Σ. «Κυβερνοασφάλεια» στοχεύει στην παροχή υψηλού επιπέδου επιστημονικών γνώσεων σχετικών με την επιστήμη της Πληροφορικής και ειδικότερα με την ασφάλεια στον κυβερνοχώρο. Η ανάπτυξη τεχνολογιών πληροφοριών και επικοινωνιών και κατά συνέπεια η προστασία από εξωτερικούς κινδύνους αποτελεί, πολιτική προτεραιότητα των χωρών-εταίρων του παρόντος Δ.Δ.Π.Μ.Σ., διότι τα εμπλεκόμενα Πανεπιστήμια παρ’ ότι προσφέρουν βαθιά πανεπιστημιακή μόρφωση σχετική με την επιστήμη των υπολογιστών (Προγραμματισμός, Δίκτυα, Επικοινωνίες, IoT, Υλικό των υπολογιστών), δεν προσφέρουν υψηλή τεχνογνωσία στην ασφάλεια των σχετικών πληροφοριακών συστημάτων. Τα περισσότερα Πανεπιστήμια μέχρι σήμερα παρέχουν μόνο βασικές γνώσεις στον τομέα της ασφάλειας και σίγουρα μη προσανατολισμένες στις σημερινές ανάγκες της αγοράς.

Το πρόγραμμα. δίνει έμφαση στην απόκτηση τόσο θεωρητικών γνώσεων όσο και πρακτικών δεξιοτήτων με στόχο τη δημιουργία αποφοίτων με υψηλή θεωρητική κατάρτιση, τεχνογνωσία και πρακτική εμπειρία, ώστε να ανταποκρίνονται πλήρως στις ανάγκες που επιβάλλουν οι ραγδαίες τεχνολογικές εξελίξεις και η αγορά εργασίας. Απώτερος στόχος του είναι η διαμόρφωση επιστημόνων που θα στελεχώσουν τους Δημόσιους Οργανισμούς και τις Επιχειρήσεις του Ιδιωτικού Τομέα και θα συμβάλουν στον τεχνολογικό εκσυγχρονισμό και την πρόοδο της χώρας.

Άρθρο 2
Σκοπός - Οργάνωση

Σκοπός του Δ.Π.Μ.Σ. «Κυβερνοασφάλεια» είναι να εκπαιδεύσει αποφοίτους σχολών Πανεπιστημίων ή ΤΕΙ, καθώς και στρατιωτικών σχολών, ειδικοτήτων της Πληροφορικής οι οποίοι επιθυμούν να αποκτήσουν γνώσεις και δεξιότητες στο αντικείμενο της Κυβερνοασφάλειας και να διαμορφώσει επιστήμονες που θα στελεχώσουν τους Δημόσιους Οργανισμούς, θεσμικά όργανα όπως υπουργεία και άλλους νευραλγικούς τομείς του Δημοσίου. Επίσης Επιχειρήσεις του Ιδιωτικού Τομέα καθώς και τα Ερευνητικά Κέντρα, και θα συμβάλουν στην πλήρη προστασία των συστημάτων από Κυβερνοεπιθέσεις.

Το Δ.Δ.Π.Μ.Σ. επιτυγχάνει την ανάπτυξη των δεξιοτήτων μέσω της υψηλού επιπέδου εκπαίδευσης. Πιο συγκεκριμένα, ο απόφοιτος του Δ.Δ.Π.Μ.Σ. θα είναι ικανός, μεταξύ άλλων, να:

- Εντοπίζει απειλές.
- Προστατεύει το δίκτυο του έναντι απειλών.
- Ανιχνεύει τυχόν σφάλματα στις θύρες εισόδου του πληροφοριακού συστήματος.
- Καταπολεμά το έγκλημα στον κυβερνοχώρο.
- Συμμετέχει στις παγκόσμιες προκλήσεις της ασφάλειας δικτύων υπολογιστών.
- Λαμβάνει αποφάσεις, που συμβάλλουν στην καλή διαχείριση και ασφάλεια δικτύων και συστημάτων.
- Αναπτύσσει σχέδιο κατάρτισης για δραστηριότητες που εμπλέκονται στην ασφάλεια υπολογιστών.
- Αποκτήσει ικανότητα στους τομείς της ανάπτυξης, διοίκησης και διαχείρισης, των συστημάτων ασφαλείας και των δικτύων υπολογιστών.
- Αντιμετωπίζει τις νέες εξειδικευμένες ανάγκες μεταξύ με γνώσεις και δεξιότητες σχετικές με την Κυβερνοασφάλεια.
- Σχεδιάζει και αναπτύσσει εφαρμογές ασφαλείας των πληροφοριακών συστημάτων.
- Κωδικοποιεί ασφαλώς την πληροφορία του.
- Εντοπίζει τις εφαρμογές που τυχόν απειλούν το Πληροφοριακό του Σύστημα.
- Διακρίνει τις επιβλαβείς λειτουργίας του Διαδικτύου.
- Διαχειρίζεται προγράμματα ασφάλειας των βάσεων δεδομένων και του διαδικτύου των πραγμάτων.

Άρθρο 3
Όργανα ίδρυσης, οργάνωση και
λειτουργία του Δ.Δ.Π.Μ.Σ.

Τα αρμόδια όργανα για την οργάνωση και λειτουργία του Δ.Δ.Π.Μ.Σ. είναι τα ακόλουθα:

Α) η Σύγκλητος του Πα.Δ.Α.

Β) η Επιτροπή Προγράμματος Σπουδών (Ε.Π.Σ.).

Γ) η Συντονιστική Επιτροπή (Σ.Ε.) του Δ.Δ.Π.Μ.Σ.

Δ) ο Διευθυντής του Δ.Δ.Π.Μ.Σ.

Ε) η Επιτροπή Μεταπτυχιακών Σπουδών (Ε.Μ.Σ.).

α) Η Σύγκλητος του Πα.Δ.Α.

Η Σύγκλητος έχει τις ακόλουθες αρμοδιότητες:

1. Εγκρίνει την ίδρυση του Διιδρυματικού Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών (Δ.Δ.Π.Μ.Σ.) ή την τροποποίηση της απόφασης ίδρυσης του,

2. εγκρίνει την παράταση της χρονικής διάρκειας της λειτουργίας των Δ.Δ.Π.Μ.Σ.,

3. συγκροτεί την Επιτροπή Προγράμματος Σπουδών, σε περίπτωση διατμηματικών ή διιδρυματικών ή κοινών Δ.Δ.Π.Μ.Σ.,

4. αποφασίζει την κατάργηση των Δ.Δ.Π.Μ.Σ. που προσφέρονται από το Πανεπιστήμιο Δυτικής Αττικής.

β) Η Επιτροπή Προγράμματος Σπουδών (Ε.Π.Σ.)

Η Επιτροπή Προγράμματος Σπουδών αποτελείται συνολικά από 7 μέλη ΔΕΠ. Η επιτροπή συγκροτείται με απόφαση της Συγκλήτου του Πα.Δ.Α. κατόπιν εισήγησης των Συνελεύσεων των συνεργαζόμενων Τμημάτων (ή των αρμόδιων οργάνων των συνεργαζόμενων φορέων).

Η Επιτροπή Προγράμματος Σπουδών είναι αρμόδια για την οργάνωση, διοίκηση και διαχείριση του Δ.Δ.Π.Μ.Σ. και ασκεί τις ίδιες αρμοδιότητες με αυτές της Συνέλευσης του Τμήματος σύμφωνα με την παρ. 3, άρθρο 81, ν. 4957/2022.

γ) Η Συντονιστική Επιτροπή (Σ.Ε.):

Με απόφαση της Επιτροπής Προγράμματος Σπουδών συγκροτείται η Συντονιστική Επιτροπή, με διετή θητεία, η οποία αποτελείται από τον Διευθυντή του Δ.Δ.Π.Μ.Σ. και τέσσερα (4) μέλη Διδακτικού Ερευνητικού Προσωπικού (Δ.Ε.Π.) του Τμήματος, που έχουν συναφές γνωστικό αντικείμενο με αυτό του Δ.Δ.Π.Μ.Σ. και αναλαμβάνουν διδακτικό έργο στο Δ.Δ.Π.Μ.Σ. Η Σ.Ε. είναι αρμόδια για την παρακολούθηση και τον συντονισμό της λειτουργίας του προγράμματος και ιδίως:

1) Καταρτίζει τον αρχικό ετήσιο προϋπολογισμό του Δ.Δ.Π.Μ.Σ. και τις τροποποιήσεις του, εφόσον το Δ.Δ.Π.Μ.Σ. διαθέτει πόρους σύμφωνα με το άρθρο 84 του ν. 4957/2022, και εισηγείται την έγκρισή του προς την Επιτροπή Ερευνών του Ειδικού Λογαριασμού Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.),

2) καταρτίζει τον απολογισμό του προγράμματος και εισηγείται την έγκρισή του προς την ΕΠΣ,

3) εγκρίνει τη διενέργεια δαπανών του Δ.Δ.Π.Μ.Σ.,

4) εγκρίνει τη χορήγηση υποτροφιών, ανταποδοτικών ή μη, σύμφωνα με όσα ορίζονται στην απόφαση ίδρυσης του Δ.Δ.Π.Μ.Σ. και τον Κανονισμό μεταπτυχιακών και διδακτορικών σπουδών,

5) εισηγείται προς την Ε.Π.Σ. την κατανομή του διδακτικού έργου, καθώς και την ανάθεση διδακτικού έργου στις κατηγορίες διδασκόντων του άρθρου 83 του ν. 4957/2022,

6) εισηγείται προς την Ε.Π.Σ. την πρόσκληση Επισκεπτών Καθηγητών για την κάλυψη διδακτικών αναγκών του Δ.Δ.Π.Μ.Σ.,

7) καταρτίζει σχέδιο για την τροποποίηση του προγράμματος σπουδών, το οποίο υποβάλλει προς την Ε.Π.Σ.,

8) εισηγείται προς τη Συνέλευση του Τμήματος την ανακατανομή των μαθημάτων μεταξύ των ακαδημαϊκών εξαμήνων, καθώς και θέματα που σχετίζονται με την ποιοτική αναβάθμιση του προγράμματος σπουδών. Δύνανται να μεταβιβάζονται προς τη Συντονιστική Επιτροπή συγκεκριμένες αρμοδιότητες της Συνέλευσης του Τμήματος ή της Ε.Π.Σ. για την αποτελεσματικότερη λειτουργία του Δ.Δ.Π.Μ.Σ., κατόπιν έκδοσης σχετικής απόφασης μεταβίβασης αρμοδιοτήτων. Στην Σ.Ε. δύνα-

ται να συμμετέχουν Ομότιμοι Καθηγητές του Τμήματος ή των συνεργαζόμενων Τμημάτων, εφόσον παρέχουν διδακτικό έργο στο Δ.Δ.Π.Μ.Σ.

δ) Ο Διευθυντής Δ.Δ.Π.Μ.Σ.

Ο Διευθυντής του Δ.Δ.Π.Μ.Σ. προέρχεται από τα μέλη Δ.Ε.Π. του Τμήματος κατά προτεραιότητα βαθμίδας Καθηγητή και ορίζεται με απόφαση της Ε.Π.Σ. για διετή θητεία, με δυνατότητα ανανέωσης χωρίς περιορισμό.

Ο Διευθυντής του Δ.Δ.Π.Μ.Σ. έχει τις ακόλουθες αρμοδιότητες:

1) Προεδρεύει της Σ.Ε., καθώς και της Επιτροπής Προγράμματος Σπουδών, σε περίπτωση διατμηματικού ή διιδρυματικού ή κοινού Δ.Δ.Π.Μ.Σ., συντάσσει την ημερήσια διάταξη και συγκαλεί τις συνεδριάσεις της,

2) εισηγείται τα θέματα που αφορούν στην οργάνωση και λειτουργία του Δ.Δ.Π.Μ.Σ. προς την Ε.Π.Σ.,

3) εισηγείται προς τη Σ.Ε. και τα λοιπά όργανα του Δ.Δ.Π.Μ.Σ. και του Α.Ε.Ι. θέματα σχετικά με την αποτελεσματική λειτουργία του Δ.Δ.Π.Μ.Σ.,

4) είναι Επιστημονικός Υπεύθυνος του προγράμματος σύμφωνα με το άρθρο 234 του ν. 4957/2022 και ασκεί τις αντίστοιχες αρμοδιότητες,

5) παρακολουθεί την υλοποίηση των αποφάσεων των οργάνων του Δ.Δ.Π.Μ.Σ. και του Εσωτερικού Κανονισμού μεταπτυχιακών προγραμμάτων σπουδών, καθώς και την παρακολούθηση εκτέλεσης του προϋπολογισμού του Δ.Δ.Π.Μ.Σ.,

6) ασκεί οποιαδήποτε άλλη αρμοδιότητα, η οποία ορίζεται στην απόφαση ίδρυσης του Δ.Δ.Π.Μ.Σ.

Ο Διευθυντής του Δ.Δ.Π.Μ.Σ., καθώς και τα μέλη της Σ.Ε. ή της Ε.Π.Σ. δεν δικαιούνται αμοιβής ή οιασδήποτε αποζημίωσης για την εκτέλεση των αρμοδιοτήτων που τους ανατίθενται και σχετίζεται με την εκτέλεση των καθηκόντων τους.

Ορισμός νέου Διευθυντή ή μέλους της Σ.Ε., σε περίπτωση παραίτησης, μπορεί να πραγματοποιηθεί με απόφαση των αρμοδίων οργάνων, κατόπιν υποβολής αίτησης των μελών και αιτιολογικής έκθεσης του αιτήματος αλλαγής/παραίτησης.

ε) Η Επιτροπή Μεταπτυχιακών Σπουδών:

Με απόφαση της Συγκλήτου, κατόπιν πρότασης των Κοσμητειών των Σχολών του Πανεπιστημίου Δυτικής Αττικής συγκροτείται η Επιτροπή Μεταπτυχιακών Σπουδών. Η Επιτροπή αποτελείται από ένα (1) μέλος Διδακτικού Ερευνητικού Προσωπικού (Δ.Ε.Π.) από κάθε Σχολή του Πα.Δ.Α., ένα (1) μέλος που προέρχεται από τις κατηγορίες μελών Ειδικού Εκπαιδευτικού Προσωπικού (Ε.Ε.Π.), Εργαστηριακού Διδακτικού Προσωπικού (Ε.ΔΙ.Π.), και Ειδικού Τεχνικού Εργαστηριακού Προσωπικού (Ε.Τ.Ε.Π.) του Πα.Δ.Α. και τον/την Αντιπρύτανη, που είναι αρμόδιος/α για ακαδημαϊκά θέματα, ως Πρόεδρο. Τα μέλη της Επιτροπής έχουν εμπειρία στην οργάνωση και συμμετοχή σε προγράμματα σπουδών δεύτερου κύκλου σπουδών. Η θητεία της Επιτροπής είναι δύο (2) ακαδημαϊκά έτη.

Αρμοδιότητα της Επιτροπής είναι:

1) η υποβολή γνώμης προς τη Σύγκλητο του Πα.Δ.Α. για την ίδρυση νέων Προγραμμάτων Μεταπτυχιακών Σπουδών ή την τροποποίηση των ήδη λειτουργούντων Δ.Δ.Π.Μ.Σ., μετά από αξιολόγηση των αιτημάτων των Συνελεύσεων των Τμημάτων για την ίδρυση νέων Δ.Δ.Π.Μ.Σ., των σχετικών εκθέσεων σκοπιμότητας και βιωσιμότητάς τους και την κοστολόγηση της λειτουργίας του Δ.Δ.Π.Μ.Σ., καθώς και η δυνατότητα αναπομπής τους, αν η εισήγηση δεν είναι επαρκώς αιτιολογημένη ή οι συνοδευτικές εκθέσεις δεν είναι πλήρεις,

2) η κατάρτιση σχεδίου Κανονισμού για Δ.Δ.Π.Μ.Σ. του Πα.Δ.Α. και η υποβολή του προς τη Σύγκλητο,

3) η εκπόνηση πρότυπου σχεδίου Κανονισμού λειτουργίας Δ.Δ.Π.Μ.Σ.,

4) ο έλεγχος της τήρησης των Κανονισμών λειτουργίας των Δ.Δ.Π.Μ.Σ.,

5) η παρακολούθηση της εφαρμογής της νομοθεσίας, του Κανονισμού και των αποφάσεων των οργάνων διοίκησης του Πα.Δ.Α. από τα Δ.Δ.Π.Μ.Σ.,

6) η παρακολούθηση της εφαρμογής της διαδικασίας απαλλαγής από την υποχρέωση καταβολής τελών φοίτησης,

7) κάθε άλλη αρμοδιότητα που ορίζεται από τον Εσωτερικό Κανονισμό του εκάστοτε Δ.Δ.Π.Μ.Σ.

Με απόφαση της Συγκλήτου, κατόπιν εισήγησης της Επιτροπής Μεταπτυχιακών Σπουδών, εγκρίνεται ο Κανονισμός προγραμμάτων μεταπτυχιακών σπουδών, ο οποίος αποτελεί διακριτό κεφάλαιο του εσωτερικού κανονισμού λειτουργίας του Πα.Δ.Α.

Άρθρο 4
Αριθμός Εισακτέων, Κριτήρια και Τρόπος Επιλογής

Ο αριθμός εισακτέων στο Δ.Δ.Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» ορίζεται κατά ανώτατο όριο σε σαράντα (40) κατ’ έτος και αντίστοιχα ο κατώτατος αριθμός εισακτέων ορίζεται σε δεκαπέντε (15).

Σε περίπτωση ισοψηφίας υποψηφίων αυξάνεται ο αριθμός των εισακτέων μεταπτυχιακών φοιτητών, ώστε να εισαχθεί και ο τελευταίος/α ισοψηφών/ούσα υποψήφιος/α. Επιπλέον του αριθμού των εισακτέων, γίνονται δεκτοί ως υπεράριθμοι υπότροφοι και μέλη των κατηγοριών ΕΕΠ, ΕΔΙΠ και ΕΤΕΠ.

Κριτήρια και Τρόπος Επιλογής Εισακτέων:

Ι. Πρόσκληση εκδήλωσης ενδιαφέροντος

Οι υποψήφιοι/ες ενημερώνονται από την πρόσκληση εκδήλωσης ενδιαφέροντος του Δ.Δ.Π.Μ.Σ., η οποία δημοσιεύεται στις ιστοσελίδες του ΠΜΣ, του Τμήματος, του Πα.Δ.Α. και σε οποιοδήποτε άλλο πρόσφορο μέσο. Στην πρόσκληση εκδήλωσης ενδιαφέροντος αναγράφονται όλες οι σχετικές πληροφορίες (ημερομηνίες και τόπος κατάθεσης της αίτησης, απαραίτητα δικαιολογητικά που πρέπει να τη συνοδεύουν), καθώς και τα κριτήρια αξιολόγησης των αιτήσεων των υποψηφίων για τα απαραίτητα δικαιολογητικά, τη διαδικασία υποβολής αίτησης και την καταληκτική ημερομηνία υποβολής αιτήσεων.

Στην πρόκληση εκδήλωσης ενδιαφέροντος αναφέρονται:

α) Οι προϋποθέσεις συμμετοχής υποψηφίων μεταπτυχιακών φοιτητών στη διαδικασία επιλογής,

β) οι κατηγορίες πτυχιούχων και ο αριθμός εισακτέων,

γ) η διαδικασία και τα κριτήρια επιλογής των μεταπτυχιακών φοιτητών,

δ) οι προθεσμίες υποβολής αιτήσεων,

ε) τα απαιτούμενα δικαιολογητικά,

στ) κάθε άλλη λεπτομέρεια που κρίνεται απαραίτητη, η οποία διευκολύνει τη διαδικασία επιλογής των υποψηφίων μεταπτυχιακών φοιτητών.

Οι αιτήσεις και τα απαιτούμενα δικαιολογητικά κατατίθενται στην Γραμματεία του Δ.Δ.Π.Μ.Σ., σε έντυπη ή σε ηλεκτρονική μορφή, σε προθεσμία που ορίζεται στην πρόσκληση εκδήλωσης ενδιαφέροντος και μπορεί να παραταθεί με απόφαση της Συνέλευσης του Τμήματος ή της Επιτροπής Προγράμματος Σπουδών.

ΙΙ. Επιτροπή Αξιολόγησης Υποψηφίων (Ε.Α.Υ.)

Η επιλογή των εισακτέων από την Ελλάδα, ανεξαρτήτως εθνικότητας, γίνεται από τριμελή Επιτροπή Αξιολόγησης υποψηφίων (Ε.Α.Υ.).

Η Επιτροπή έχει τις παρακάτω αρμοδιότητες:

i. Αξιολόγηση όλων των υποβληθέντων δικαιολογητικών. Ο έλεγχος της πληρότητας των δικαιολογητικών ενεργείται από τη Γραμματεία του Δ.Δ.Π.Μ.Σ.

ii. Έλεγχος της γλωσσικής επάρκειας.

iii. Διενέργεια προσωπικών συνεντεύξεων.

Τα δικαιολογητικά συμμετοχής των υποψηφίων είναι: (ενδεικτικά αναφέρονται)

1. Αίτηση υποψηφιότητας στο Δ.Δ.Π.Μ.Σ.

2. Αντίγραφο πτυχίου/διπλώματος ή βεβαίωση περάτωσης σπουδών.

3. Πιστοποιητικό αναλυτικής βαθμολογίας.

4. Αναλυτικό βιογραφικό σημείωμα, στο οποίο θα αναφέρονται αναλυτικά οι τίτλοι σπουδών και ενδεχόμενες ερευνητικές ή επαγγελματικές δραστηριότητες.

5. Αποδεικτικά ερευνητικής ή επαγγελματικής δραστηριότητας (εφόσον υπάρχουν).

6. Συστατικές επιστολές (εφόσον υπάρχουν).

7. Αντίγραφο μεταπτυχιακού τίτλου (εφόσον υπάρχει),.

8. Δημοσιεύσεις σε περιοδικά με κριτές (εφόσον υπάρχουν).

9. Φωτοτυπία δύο όψεων της αστυνομικής ταυτότητας.

10. αντίγραφο πιστοποιητικού γνώσης της αγγλικής γλώσσας. Η γνώση πιστοποιείται με αναγνωρισμένο τίτλο σπουδών (π.χ. Τίτλο σπουδών από Εκπαιδευτικό Ίδρυμα αγγλόφωνης χώρας ή αγγλόφωνου προγράμματος σπουδών, Πιστοποιητικό επιπέδου C1, Πιστοποιητικό TOEFL με βαθμολογία τουλάχιστον 500 μόρια (ή 300 με το νέο τρόπο αξιολόγησης), Πιστοποιητικό IELTS με βαθμό τουλάχιστον 6,5.

11. Επιπρόσθετα προσόντα, υποτροφίες, ειδικά σεμινάρια, μεταπτυχιακοί τίτλοι, πτυχία συμπληρωματικής εκπαίδευσης κ.λπ. (εφόσον υπάρχουν).

Οι πτυχιούχοι αγγλόφωνων πανεπιστημίων απαλλάσσονται από την υποχρέωση προσκόμισης πιστοποιητικού γλωσσομάθειας.

(Σε περίπτωση που δεν υπάρχουν οι ανωτέρω προϋποθέσεις για την καλή γνώση της αγγλικής γλώσσας, η Σ.Ε. του Δ.Δ.Π.Μ.Σ. διαπιστώνει την επάρκεια στην αγγλική γλώσσα με τίτλο γλωσσομάθειας αντίστοιχο του επιπέδου C1. Θετικά συνυπολογίζεται και η γνώση και άλλων ξένων γλωσσών).

Με την ολοκλήρωση των διαδικασιών αξιολόγησης, η αρμόδια Ε.Α.Υ. συντάσσει τον πίνακα των επιτυχόντων και επιλαχόντων κατά σειρά κατάταξης, σύμφωνα με τα κριτήρια επιλογής και τους συντελεστές βαρύτητας ανά κριτήριο. Ως επιτυχόντες θεωρούνται οι υποψήφιοι/ες που έλαβαν βαθμολογική θέση στη σειρά κατάταξης μέχρι του ανώτατου ορίου εισαγωγής φοιτητών/τριών. Η Ε.Α.Υ. μπορεί να θεωρήσει επιτυχόντες και όσους από τους/τις υποψήφιους/ες ισοβάθμησαν με τον τελευταίο επιτυχόντα. Ως επιλαχόντες/χούσες θεωρούνται οι υποψήφιοι/ες οι οποίοι έλαβαν βαθμολογική θέση στη σειρά κατάταξης, πέραν του ανώτατου ορίου εισαγωγής φοιτητών, έχοντας δικαίωμα εγγραφής στην περίπτωση που οι πρωθύστεροι στην κατάταξη δεν αποδεχθούν τη θέση ή δεν εγγραφούν εμπρόθεσμα.

Σε περίπτωση ισοβαθμίας εισάγονται όλοι οι ισοβαθμήσαντες υποψήφιοι με την προϋπόθεση ότι δεν υπερβαίνουν το μέγιστο αριθμό εισακτέων που έχει οριστεί στην Πρόσκληση Εκδήλωσης Ενδιαφέροντος. Στην περίπτωση που συμπληρωθεί ο μέγιστος αριθμός εισακτέων στο 2, εισάγεται ο υποψήφιος που έχει τον μεγαλύτερο βαθμό πτυχίου.

Η τελική κατάταξη των υποψηφίων με βάση τη λίστα κριτηρίων του Προγράμματος και η πρόταση επιλογής υποψηφίων με βάση την κατάταξη αυτή, υποβάλλονται προς επικύρωση στην Επιτροπή Προγράμματος Σπουδών.

ΙΙΙ. Κριτήρια επιλογής των υποψηφίων:

ΚΩΔΙΚΟΣ	ΠΕΡΙΓΡΑΦΗ	ΒΑΡΥΤΗΤΑ
Κ1	Βαθμός πτυχίου Βαθμολογία σε μαθήματα σχετικά με το γνωστικό αντικείμενο του Δ.Δ.Π.Μ.Σ. Διπλωματική εργασία, όπου αυτή προβλέπεται στον α’ κύκλο σπουδών	25%
Κ2	Γνώση Αγγλικής γλώσσας σε επίπεδο τουλάχιστον C1	10%
Κ3	Τυχόν συγγραφική ή/και ερευνητική δραστηριότητα του υποψηφίου στο αντικείμενο του προγράμματος	10%
Κ4	Ερευνητική ή Επαγγελματική εμπειρία του υποψηφίου ή τεκμηριωμένη ενασχόλησή του σε αντίστοιχο τομέα ή σε συναφές αντικείμενο	20%
Κ5	Συνέντευξη	30%
Κ6	Επαρκής γνώση μιας τουλάχιστον ξένης γλώσσας πέραν της γλώσσας διεξαγωγής του ΠΜΣ	5%

Βαθμός = Κ1 Χ 0,25 + Κ2 Χ 0,10 + Κ3 Χ 0,10 + Κ4 Χ 0,2+…

Επιλέγονται οι υποψήφιοι που θα συγκεντρώνουν την υψηλότερη συνολική βαθμολογία και μέχρι της κάλυψης του μέγιστου αριθμού εισακτέων του Προγράμματος.

ΙV. Διαδικασία επιλογής

Τα απαιτούμενα δικαιολογητικά υποβάλλονται εντός των προθεσμιών που ορίζονται στην αντίστοιχη πρόσκληση εκδήλωσης ενδιαφέροντος.

Η Γραμματεία του Δ.Δ.Π.Μ.Σ. παραλαμβάνει τις αιτήσεις και τα απαραίτητα δικαιολογητικά που υποβάλλουν οι υποψήφιοι/ες μεταπτυχιακοί/ες φοιτητές/τριες, τα οποία προβλέπονται από την πρόσκληση εκδήλωσης

ενδιαφέροντος κάθε φορά και συντάσσει πίνακα υποψηφίων μεταπτυχιακών φοιτητών, τον οποίο διαβιβάζει στην Ε.Α.Υ. Τα δικαιολογητικά που κατατίθενται από τους υποψήφιους πρέπει να έχουν υποβληθεί εμπρόθεσμα, όπως αυτά προβλέπονται στη σχετική πρόσκληση εκδήλωσης ενδιαφέροντος. Εκπρόθεσμες αιτήσεις δεν γίνονται δεκτές.

Η διαδικασία αξιολόγησης των υποψηφίων περιλαμβάνει δύο στάδια:

Στο πρώτο, αξιολογούνται οι αιτήσεις με βάση την πληρότητα και την εγκυρότητα των απαιτούμενων δικαιολογητικών που υποβλήθηκαν, το οποίο αποτελεί απαραίτητη προϋπόθεση πρόκρισης στο επόμενο στάδιο.

Κατά το δεύτερο στάδιο της διαδικασίας, οι υποψήφιοι/ες καλούνται σε συνέντευξη ενώπιον της Ε.Α.Υ. Στόχος είναι να διαπιστωθεί ποιοι/ές υποψήφιοι/ες είναι ικανοί/ές να ανταποκριθούν ουσιαστικά στις απαιτήσεις του Δ.Δ.Π.Μ.Σ., συνεκτιμώντας το κίνητρο και το ενδιαφέρον, αλλά και τη συνολικότερη συγκρότηση και επιστημονική τους επάρκεια σε σχέση με το αντικείμενο του μεταπτυχιακού προγράμματος.

Με την ολοκλήρωση των διαδικασιών αξιολόγησης, η Ε.Α.Υ. καταρτίζει πλήρη κατάλογο με όλους τους υποψηφίους, ιεραρχεί τους υποψηφίους, προβαίνει στην τελική επιλογή και καταρτίζει τον προσωρινό πίνακα των επιτυχόντων, ο οποίος επικυρώνεται από την Ε.Π.Σ.. Η ανάρτησή του πραγματοποιείται σύμφωνα με τις διατάξεις περί προστασίας προσωπικών δεδομένων, στην ιστοσελίδα του Δ.Δ.Π.Μ.Σ. και στις ανακοινώσεις του Τμήματος.

Σε περίπτωση που δυο ή περισσότεροι υποψήφιοι συγκεντρώσουν συνολικά τον ίδιο αριθμό μορίων, γίνονται δεκτοί ως ισοβαθμήσαντες.

Ένσταση κατά του προσωρινού πίνακα επιτυχόντων μπορεί να γίνει μέσα σε πέντε (5) εργάσιμες ημέρες από την ημερομηνία ανακοίνωσης των πινάκων. Η ένσταση, πρέπει να είναι συγκεκριμένη και κρίνεται τελεσίδικα από Τριμελή Επιτροπή μελών Δ.Ε.Π. των αντίστοιχων Τμημάτων των Πανεπιστημίων συμμετεχόντων Φορέων σε περίπτωση διατμηματικού ή διιδρυματικού ή κοινού Π.Μ.Σ.) που έχουν αναλάβει μεταπτυχιακό έργο, η οποία ορίζεται με απόφαση της Ε.Π.Σ..

Μετά την λήξη της προθεσμίας ενστάσεων (εάν υπάρχουν) και την τελεσίδικη απόφαση της επιτροπής ενστάσεων, αναρτάται ο τελικός πίνακας επιτυχόντων, σύμφωνα με την διαδικασία ανάρτησης του προσωρινού πίνακα.

Οι επιτυχόντες υποψήφιοι καλούνται να απαντήσουν γραπτώς ή ηλεκτρονικώς (e-mail) εντός 5 ημέρων το αργότερο από την ανάρτηση του τελικού πίνακα όπως ορίζεται στην πρόσκληση εκδήλωσης ενδιαφέροντος για την αποδοχή της ένταξης τους στο Π.Μ.Σ και τους όρους λειτουργίας του, όπως αυτοί περιγράφονται στον παρόντα κανονισμό λειτουργίας.

Εφόσον υπάρξουν αρνήσεις, η Γραμματεία ενημερώνει τους αμέσως επόμενους υποψήφιους στη σειρά αξιολόγησης από τον τελικό πίνακα επιτυχόντων/επιλαχόντων.

ν. Εγγραφή στο Δ.Δ.Π.Μ.Σ.

Οι επιτυχόντες θα πρέπει να εγγραφούν στη γραμματεία του Δ.Δ.Π.Μ.Σ. το αργότερο την τελευταία εργάσιμη ημέρα της προτελευταίας εβδομάδας του Σεπτεμβρίου του εκάστοτε έτους. Για λόγους εξαιρετικής ανάγκης είναι δυνατή η εγγραφή μεταπτυχιακού φοιτητή μετά από τη λήξη της προθεσμίας με απόφαση της Συντονιστικής Επιτροπής ύστερα από αιτιολογημένη αίτηση του ενδιαφερομένου. Οι εισακτέοι μεταπτυχιακοί φοιτητές μπορούν να ενημερώνονται από την ιστοσελίδα του Τμήματος ή/και από τη Γραμματεία του Δ.Δ.Π.Μ.Σ.

Άρθρο 5
Κατηγορίες Υποψηφίων.

Στο Π.Μ.Σ γίνονται δεκτοί πτυχιούχοι Ιδρυμάτων Τριτοβάθμιας Εκπαίδευσης της ημεδαπής ή ομοταγών Ιδρυμάτων της αλλοδαπής σύμφωνα με τις διατάξεις της κείμενης νομοθεσίας Υποψηφιότητα θέτουν όλοι οι πτυχιούχοι των ΑΕΙ καθώς επίσης και οι πτυχιούχοι των Σχολών των Ενόπλων Δυνάμεων (τετραετούς φοιτήσεως) ή γενικώς πτυχιούχοι που έχουν τουλάχιστον 210 ECTS στον τίτλο σπουδών τους από Ελληνικά ΑΕΙ ή 180 ECTS για πτυχιούχους της αλλοδαπής.

Αίτηση μπορούν να υποβάλουν και τελειόφοιτοι Τμημάτων, υπό την προϋπόθεση ότι θα έχουν προσκομίσει Βεβαίωση Περάτωσης των Σπουδών τους πριν την ημερομηνία επικύρωσης του πίνακα των επιτυχόντων. Στην περίπτωση αυτή, αντίγραφο του πτυχίου ή του διπλώματός τους προσκομίζεται πριν από την ημερομηνία έναρξης του προγράμματος.

Αίτηση δύναται να υποβάλλουν και τελειόφοιτοι αλλοδαπών Ιδρυμάτων τα οποία δεν είναι ακόμα ενταγμένα στο Εθνικό Μητρώο Αναγνωρισμένων Ιδρυμάτων της αλλοδαπής του ΔΟΑΤΑΠ. Σε περίπτωση που Ίδρυμα της Αλλοδαπής δεν βρίσκεται αναρτημένο στον ιστότοπο του ΔΟΑΤΑΠ, το Τμήμα εφαρμόζει τη διαδικασία σύμφωνα με όσα ορίζονται στην κείμενη νομοθεσία. Σε διαφορετική περίπτωση, γίνεται διαγραφή του φοιτητή, χωρίς να υπάρχει αξίωση από τον φοιτητή επιστροφής των χρημάτων που ενδεχομένως κατέθεσε.

Τα μέλη των κατηγοριών Ε.Ε.Π., καθώς και Ε.ΔΙ.Π. και Ε.Τ.Ε.Π. και διοικητικοί υπάλληλοι του χώρου της Πληροφορικής μπορούν μετά από αίτησή τους να εγγραφούν ως υπεράριθμοι/ες και μόνο ένας κατ’ έτος, χωρίς τέλη φοίτησης, εφόσον έχει αποφασισθεί από την Σ.Ε..

Η αρμόδια Γραμματεία του Τμήματος ελέγχει αν το ίδρυμα απονομής του τίτλου αλλοδαπού ιδρύματος ανήκει στο Εθνικό Μητρώο Αναγνωρισμένων Ιδρυμάτων της αλλοδαπής και αν ο τύπος του τίτλου αυτού ανήκει στο Εθνικό Μητρώο Τύπων Τίτλων Σπουδών Αναγνωρισμένων Ιδρυμάτων που είναι αναρτημένα στον ιστότοπο του ΔΟΑΤΑΠ.

Άρθρο 6
Διάρκεια Σπουδών - Μερική Φοίτηση - Αναστολή Φοίτησης

6.1. Χρονική διάρκεια φοίτησης

Η χρονική διάρκεια για τις σπουδές που οδηγούν στην απονομή του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ) του Προγράμματος ορίζεται σε τρία(3) Ακαδη-

μαϊκά εξάμηνα και ο προσαυξημένος χρόνος διαρθρώνεται σε έξι (6) εξάμηνα, έκαστο διάρκειας δεκατριών (13) εβδομάδων διδασκαλίας στα οποία περιλαμβάνεται και ο χρόνος για την εκπόνηση και υποβολή προς κρίση της Μεταπτυχιακής Διπλωματικής Εργασίας (Μ.Δ.Ε.).

Η επιτρεπόμενη διάρκεια ολοκλήρωσης των υποχρεώσεων για την λήψη του διπλώματος μεταπτυχιακών σπουδών είναι από τρία (3) εξάμηνα το λιγότερο έως και πέντε (5) Ακαδημαϊκά εξάμηνα το μέγιστο. Ωστόσο, σε εξαιρετικές περιπτώσεις, μπορεί να δοθεί αναστολή φοίτησης με εισήγηση της Συντονιστικής Επιτροπής και απόφαση της Συνέλευσης Τμήματος και ο χρόνος αυτός δεν υπολογίζεται στην συνολική απαιτούμενη διάρκεια απονομής του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ).

Η διάρκεια των μαθημάτων του Δ.Δ.Π.Μ.Σ. ανά εξάμηνο σπουδών, είναι τουλάχιστον δεκατρείς (13) εβδομάδες. Τα υποχρεωτικά μαθήματα δεν υπολείπονται των 39 διδακτικών ωρών. Το σύνολο των προσφερόμενων μαθημάτων ανά εξάμηνο αντιστοιχεί σε 30 ECTS. Ο χρόνος συγγραφής της διπλωματικής εργασίας δεν μπορεί να είναι μικρότερος από έξι (6) μήνες και μεγαλύτερος από δεκαοκτώ (18) μήνες.

Το Δ.Δ.Π.Μ.Σ. ολοκληρώνεται με την απονομή Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.), επίπεδο επτά (7) του Εθνικού και Ευρωπαϊκού Πλαισίου Προσόντων, σύμφωνα με το άρθρο 47 του ν. 4763/2020.

Η επιτυχής ολοκλήρωση φοίτησης διαπιστώνεται από την επιτυχή επίδοση στα μαθήματα του Π.Μ.Σ και την επιτυχή εκπόνηση Διπλωματικής Εργασίας.

6.2. Μερική Φοίτηση

Στους μεταπτυχιακούς φοιτητές/τριες που αδυνατούν να ανταποκριθούν στις ελάχιστες απαιτήσεις του προγράμματος πλήρους φοίτησης, προβλέπεται σύμφωνα με την κείμενη νομοθεσία, η δυνατότητα μερικής φοίτησης.

Δικαιούνται μερική φοίτηση:

α) Οι φοιτητές που αποδεδειγμένα εργάζονται τουλάχιστον 40 ώρες την εβδομάδα,

β) οι φοιτητές με αναπηρία και ειδικές εκπαιδευτικές ανάγκες,

γ) για σοβαρούς οικογενειακούς λόγους υγείας,

δ) λόγοι ανωτέρας βίας. Ως λόγοι ανωτέρας βίας θεωρούνται ο πόλεμος, το πραξικόπημα, οι απρόβλεπτες κυβερνητικές απαγορεύσεις και αφορούν τους ένστολους φοιτητές.

Η υποβολή των αιτήσεων για ένταξη σε καθεστώς μερικής φοίτησης πραγματοποιείται στη Γραμματεία του Τμήματος φοίτησης και οι ενδιαφερόμενοι ταυτόχρονα με την αίτηση καταθέτουν ως επισυναπτόμενα, έγγραφα που αποδεικνύουν τις προϋποθέσεις οι οποίες συντρέχουν για τη δυνατότητα μερικής φοίτησης. Στη μερική φοίτηση η διάρκεια σπουδών δεν μπορεί να υπερβαίνει το διπλάσιο της κανονικής φοίτησης.

6.3. Αναστολή φοίτησης

Ο μεταπτυχιακός φοιτητής μπορεί με αίτησή του να ζητήσει αιτιολογημένα αναστολή φοίτησης (π.χ. στρατιωτική θητεία, ασθένεια, απουσία στο εξωτερικό ή σοβαροί οικογενειακοί λόγοι), εφόσον προσκομίσει τα σχετικά δικαιολογητικά. Η απόφαση λαμβάνεται από την Ε.Π.Σ. κατόπιν εισήγησης της Συντονιστικής Επιτροπής. Τα εξάμηνα αναστολής της φοιτητικής ιδιότητας δεν προσμετρώνται στην προβλεπόμενη μέγιστη διάρκεια κανονικής φοίτησης. Το δικαίωμα αναστολής σπουδών δύναται να ασκηθεί άπαξ ή τμηματικά για χρονικό διάστημα κατ’ ελάχιστον ενός (1) ακαδημαϊκού εξαμήνου, αλλά η συνολική διάρκεια της αναστολής δεν δύναται να υπερβαίνει αθροιστικά τα δύο (2) ακαδημαϊκά εξάμηνα. Οι φοιτητές που βρίσκονται σε αναστολή φοίτησης, χάνουν την φοιτητική ιδιότητα καθ’ όλο το χρονικό διάστημα της αναστολής. Ο/Η φοιτητής/τρια με την επάνοδό του/της στη φοίτηση εξακολουθεί να υπάγεται στο καθεστώς φοίτησης του χρόνου εγγραφής του/της ως μεταπτυχιακός/ης φοιτητής/τριας.

Άρθρο 7
Πρόγραμμα Σπουδών

Το Δ.Δ.Π.Μ.Σ. ξεκινά το χειμερινό ή/και εαρινό εξάμηνο κάθε Ακαδημαϊκού έτους. Η επιτυχής εξέταση σε όλα τα μαθήματα του προγράμματος σπουδών, η επιτυχής εκπόνηση της διπλωματικής εργασίας, είναι απαραίτητες προϋποθέσεις για την απονομή Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.).

Το αναλυτικό πρόγραμμα μαθημάτων ανά εξάμηνο ως εξής:

Α΄ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ			
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Υ: Υποχρεωτικό Ε: Επιλογής	ECTS
Cscyb 101	Information Systems Security Ασφάλεια Πληροφοριακών Συστημάτων	Υ	8
Cscyb 102	Cybersecurity protocols and standards Κανόνες και Πρωτόκολλα Κυβερνοασφάλειας	Υ	7
Cscyb 103	Applied Cryptography Εφαρμοσμένη Κρυπτογραφία	Υ	8
Cscyb 104	Information Security Ασφάλεια Πληροφορίας	Υ	3
Cscyb 105	Τεχνολογίες Αλυσίδας Συστοιχιών & Κατανεμημένου Καθολικού Blockchain & Distributed Ledger technologies	Υ	4
	ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ ΕΞΑΜΗΝΟΥ		30

Β’ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ			
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Υ: Υποχρεωτικό Ε: Επιλογής	ECTS
Cscyb 201	Hardware Security Ασφάλεια Υλικού	Υ	8
Cscyb 204	Ψηφιακή Εγκληματολογία και έλεγχος διείσδυσης Digital Forensics and Penetration Testing	Υ	8
Cscyb 205	Software and Database Security Ασφάλεια Λογισμικού και Βάσεων Δεδομένων	Υ	7
Cscyb 206	Ασφάλεια Διαδικτύου Network security	Υ	7
Cscyb 202	IoT security and Cloud security Ασφάλεια διαδικτύου των πραγμάτων και Νεφουπολογιστικής	ΕΥ	3
Cscyb 203	Mobile computing Security Ασφάλεια κινητής υπολογιστικής	ΕΥ	4
Cscyb 207	Physical Layer Security Ασφάλεια φυσικού επιπέδου	ΕΥ	3
Cscyb 208	IT project management Διαχείριση Έργων Πληροφορικής	ΕΥ	4
Cscyb 209	Ασφάλεια Ηλεκτρονικών Συναλλαγών Security of electronic transactions	ΕΥ	3
	ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ ΕΞΑΜΗΝΟΥ		30

Γ’ ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ			
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	Μ.Δ.Ε.	Υ: Υποχρεωτικό Ε: Επιλογής	ECTS
Cscyb 300	Διπλωματική Εργασία Master Thesis	Υ	30
	ΣΥΝΟΛΟ ΠΙΣΤΩΤΙΚΩΝ ΜΟΝΑΔΩΝ ΕΞΑΜΗΝΟΥ		30

Άρθρο 8
Μεταπτυχιακή Διπλωματική Εργασία (Μ.Δ.Ε.)

Ο/Η μεταπτυχιακός φοιτητής/τρια υποχρεούται να εκπονήσει και να υποστηρίξει με επιτυχία τη μεταπτυχιακή διπλωματική του/της εργασία στο αντίστοιχο εξάμηνο σπουδών που αναφέρεται στον παρόντα Εσωτερικό Κανονισμό. Ο μεταπτυχιακός φοιτητής έχει δικαίωμα αίτησης ανάληψης Μ.Δ.Ε εφόσον έχει ολοκληρώσει την παρακολούθηση των μαθήματων του προγράμματος σπουδών. Το θέμα της Μ.Δ.Ε. πρέπει να εντάσσεται στο αντικείμενο του Δ.Δ.Π.Μ.Σ.

Ειδικότερα θέματα εκπόνησης Μ.Δ.Ε. ορίζονται από τον Οδηγό Μεταπτυχιακής Διπλωματικής Εργασίας του Δ.Δ.Π.Μ.Σ., ο οποίος ενδεικτικά μπορεί περιλαμβάνει τα ακόλουθα:

1. Τον εκπαιδευτικό σκοπό της Μ.Δ.Ε.,
2. τα στάδια υποβολής της Μ.Δ.Ε.,
3. τα πεδία ερευνητικού ενδιαφέροντος,
4. τα στάδια διενέργειας της Μ.Δ.Ε.,
5. την αλλαγή τίτλου Μ.Δ.Ε.
6. τις καλές πρακτικές σύνταξης του κειμένου και της ηλεκτρονικής ή έντυπης ανάγνωσης της Μ.Δ.Ε.,
7. την μελέτη και εύρεση βιβλιογραφικών πηγών,
8. την σύνταξη των ερευνητικών εργασιών,
9. τα κριτήρια αξιολόγησης της Μ.Δ.Ε.,
10. την αλλαγή επιβλέποντα, κ.τ.λ.

Άρθρο 9
Οργάνωση του Δ.Δ.Π.Μ.Σ. με τη χρήση μεθόδων σύγχρονης και ασύγχρονης εξ αποστάσεως εκπαίδευσης

Στις συνθήκες που έχουν διαμορφωθεί, είναι επιτακτική η ανάγκη του εκσυγχρονισμού του μαθησιακού μοντέλου. Το σχέδιο περιλαμβάνει και την υποστήριξη της εκπαιδευτικής διαδικασίας με σύγχρονα ψηφιακά μέσα και τεχνολογίες.

Προβλέπεται συνεπώς και η δυνατότητα σύγχρονης και ασύγχρονης εξ αποστάσεως εκπαίδευση, η δε διαδικασία υλοποίησής της υπόκειται στα προβλεπόμενα του ν. 4957/2022, του άρθρου 9 του Πρότυπου Κανονισμού Σπουδών των ΠΜΣ του Πα.Δ.Α. (Β’ 4861) και την υπό στοιχεία 18137/Ζ1/16-2-2023 (Β’ 1079) κοινή υπουργική απόφαση.

Η διδασκαλία πραγματοποιείται με όλες τις μεθόδους Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) που διαθέτει το ΠαΔΑ για τη σύγχρονη, ασύγχρονη και μικτή εξ αποστάσεως εκπαίδευση.

Μέρος της εκπαιδευτικής διαδικασίας δύναται να οργανώνεται και με μεθόδους ασύγχρονης εξ αποστάσεως εκπαίδευσης, εφόσον ο συνολικός αριθμός των πιστωτικών μονάδων των εκπαιδευτικών δραστηριοτήτων που οργανώνονται με την εν λόγω μέθοδο δεν υπερβαίνει το είκοσι πέντε τοις εκατό (25%) των συνολικών πιστωτικών μονάδων του Δ.Δ.Π.Μ.Σ..

Η εκπαιδευτική διαδικασία δύναται να διεξάγεται με τη χρήση μεθόδων σύγχρονης ή ασύγχρονης εξ αποστάσεως εκπαίδευσης, και σε περιπτώσεις:

Ι. Ανωτέρας βίας ή έκτακτες συνθήκες, όπου δεν καθίσταται δυνατή η διά ζώσης διεξαγωγή της εκπαιδευτικής διαδικασίας ή η χρήση των υποδομών του Πανεπιστημίου Δυτικής Αττικής για τη διεξαγωγή των εκπαιδευτικών δραστηριοτήτων του,

ΙΙ. οργάνωσης μαθημάτων εμβάθυνσης και φροντιστηριακών ασκήσεων, πέραν των υποχρεωτικών ωρών διδακτικού έργου ανά μάθημα.

Το ποσοστό της σύγχρονης και ασύγχρονης εξ αποστάσεως εκπαίδευσης στο σύνολο δεν θα υπερβαίνει το 80% των πιστωτικών μονάδων του Δ.Δ.Π.Μ.Σ.

Η οργάνωση της εκπαιδευτικής διαδικασίας με μεθόδους εξ αποστάσεως εκπαίδευσης εξασφαλίζει απόλυτα την προσβασιμότητα των ατόμων με αναπηρία και ειδικές εκπαιδευτικές ανάγκες.

Το σύνολο του υλικού των μαθημάτων που προσφέρονται στο μεταπτυχιακό πρόγραμμα για τη διεξαγωγή της εξ αποστάσεως εκπαίδευσης μέσω είτε των ασύγχρονων είτε των σύγχρονων μεθόδων (Open eclass, Moodle, MS Teams κ.α.), συμπεριλαμβανομένων ενδεικτικά κειμένων, γραφημάτων, φωτογραφιών, απεικονίσεων, προσομοιώσεων και γενικά κάθε είδους αρχείων, υπόκειται στον νόμο περί πνευματικής ιδιοκτησίας και διέπεται από τις εθνικές και διεθνείς διατάξεις της, με εξαίρεση τα ρητώς αναγνωρισμένα δικαιώματα τρίτων.

Σε περίπτωση πρόθεσης βιντεοσκόπησης ηλεκτρονικής διάλεξης ή άλλης σύγχρονης εκπαιδευτικής δραστηριότητας (ασκήσεις πράξης, εργαστηριακή ομάδα) εκ μέρους του διδάσκοντα θα πρέπει, πριν την έναρξη της καταγραφής, να ενημερώνονται οι συμμετέχοντες φοιτητές ώστε να συναινούν όλοι.

ΑΠΑΓΟΡΕΥΣΕΙΣ κατά την διάρκεια των εξ αποστάσεως μαθημάτων

Απαγορεύεται ρητά η με οποιονδήποτε τρόπο καταγραφή, βιντεοσκόπηση, ηχογράφηση, καθώς και η αναπαραγωγή, αναδημοσίευση, αντιγραφή, μετάδοση, έκδοση, μετάφραση, τροποποίηση του υλικού των μαθημάτων που διεξάγονται από απόσταση, τμηματικά ή περιληπτικά, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του διδάσκοντα. Σε περίπτωση παράβασης της παραπάνω απαγόρευσης, εκκινεί η διαδικασία επιβολής των νόμιμων κυρώσεων κατά του υπαιτίου, σύμφωνα με τις διατάξεις περί Πνευματικής ιδιοκτησίας.

Των ανωτέρω εξαιρείται η απλή παρακολούθηση και «τηλεφόρτωση» (download) του μαθησιακού υλικού για προσωπική χρήση των φοιτητών.

Άρθρο 10
Αξιολόγηση φοιτητών - Εξετάσεις

Στην αρχή κάθε εξαμήνου και πριν την έναρξη των μαθημάτων του Δ.Δ.Π.Μ.Σ. ανακοινώνεται στους μεταπτυχιακούς φοιτητές το ακαδημαϊκό ημερολόγιο του Π.Μ.Σ, το οποίο καθορίζεται με απόφαση της Ε.Π.Σ., μετά από εισήγηση της Σ.Ε. Στο ακαδημαϊκό ημερολόγιο του Δ.Δ.Π.Μ.Σ. αναγράφονται οι ημερομηνίες έναρξης και λήξης των εξαμήνων, οι αργίες, καθώς και οι ημερομηνίες των εξετάσεων.

Η Συντονιστική Επιτροπή καταρτίζει και ανακοινώνει εγκαίρως το ωρολόγιο πρόγραμμα των εξετάσεων κάθε εξεταστικής περιόδου και όχι αργότερα από δέκα (10) ημέρες πριν από την έναρξη των εξετάσεων.

Επαναληπτική εξεταστική περίοδος παρέχεται στον Σεπτέμβριο εκάστου έτους.

Η αξιολόγηση των μεταπτυχιακών φοιτητών και η επίδοσή τους στα μαθήματα που υποχρεούνται να παρακολουθήσουν στο πλαίσιο του Δ.Δ.Π.Μ.Σ. πραγματοποιείται με γραπτές ή προφορικές εξετάσεις ή με εκπόνηση εργασιών καθ’ όλη τη διάρκεια του εξαμήνου. Ο τρόπος αξιολόγησης περιγράφεται στο περίγραμμα του κάθε μαθήματος. Η επίδοση σε κάθε μάθημα αξιολογείται από τον/ους διδάσκοντα/ες και βαθμολογείται με την ισχύουσα, για τους προπτυχιακούς φοιτητές, κλίμακα βαθμολογίας. Συγκεκριμένα, οι βαθμοί που δίδονται, κυμαίνονται από μηδέν (0) μέχρι δέκα (10). Προβιβάσιμοι βαθμοί είναι το πέντε (5) και οι μεγαλύτεροί του. Για την αντιμετώπιση έκτακτων αναγκών ή συνθηκών που ανάγονται σε λόγους ανωτέρας βίας δύναται η χρήση ηλεκτρονικών μέσων για την αξιολόγηση των μαθημάτων, υπό την προϋπόθεση ότι εξασφαλίζεται το αδιάβλητο της διαδικασίας της αξιολόγησης.

Για την αξιολόγηση φοιτητών με αναπηρία και ειδικές εκπαιδευτικές ανάγκες παρέχονται όλες οι δυνατές υποδομές π.χ. (πενήντα τοις εκατό) 50% επιπλέον χρόνος στους έχοντες προβλήματα δυσλεξίας, η εξέταση κατά μόνας στους αγοραφοβικούς, δυνατότητα εξέτασης με την χρήση ατόμου που γνωρίζει την νοηματική σε περίπτωση κωφαλάλων και τέλος προφορική εξέταση στους έχοντες μειωμένη όραση.

Για τη βελτίωση της βαθμολογίας των μεταπτυχιακών φοιτητών, δύναται η επανεξέταση σε ένα μόνο μάθημα, στο οποίο έχει εξεταστεί επιτυχώς, σε οποιαδήποτε εξεταστική περίοδο.

Αν ο/η μεταπτυχιακός/η φοιτητής/τρια αποτύχει περισσότερες από τρεις (3) φορές στο ίδιο μάθημα, δύναται να ζητήσει, με αίτησή του προς τον Διευθυντή του ΠΜΣ, να αξιολογηθεί από τριμελή επιτροπή, η οποία αποτελείται από διδακτικό προσωπικό του ίδιου ή άλλου Τμήματος του Πα.Δ.Α., με γνωστικό αντικείμενο ίδιο ή συναφές με αυτό του προς εξέταση μαθήματος, στην οποία δεν μπορεί να συμμετέχει ο/η διδάσκων/ούσα του μαθήματος. Αν ο Διευθυντής του Δ.Δ.Π.Μ.Σ. δεν ορίσει τα μέλη της επιτροπής εντός ενός (1) μηνός από την υποβολή της αίτησης, ο φοιτητής δύναται να ζητήσει τον ορισμό τους από τον Πρόεδρο του Τμήματος.

Η αξιολόγηση των φοιτητών, στο πλαίσιο της εξ αποστάσεως εκπαίδευσης Μεταπτυχιακών Προγραμμάτων Σπουδών (Δ.Δ.Π.Μ.Σ.), διενεργείται με γραπτές ή προφορικές εξετάσεις που διενεργούνται δια ζώσης ή με γραπτές ή προφορικές εξετάσεις που διενεργούνται με μεθόδους εξ αποστάσεως, καθώς και με εναλλακτικές μεθόδους, όπως η υποβολή εργασιών.

ΑΞΙΟΛΟΓΗΣΗ

1. Η αξιολόγηση των φοιτητών, στο πλαίσιο της εξ αποστάσεως εκπαίδευσης Μεταπτυχιακών Προγραμμάτων Σπουδών (Δ.Δ.Π.Μ.Σ.), διενεργείται με γραπτές ή προφορικές εξετάσεις που διενεργούνται δια ζώσης ή με γραπτές ή προφορικές εξετάσεις που διενεργούνται με μεθόδους εξ αποστάσεως, καθώς και με εναλλακτικές μεθόδους, όπως η υποβολή εργασιών.

2. Το ΠαΔΑ λαμβάνει τα κατάλληλα και αναγκαία μέτρα ώστε να διασφαλίζεται η αξιοπιστία και το αδιάβλητο της διαδικασίας. Ειδικώς, η γραπτή ή η προφορική εξ αποστάσεως εξέταση δύναται να πραγματοποιηθεί μέσω τεχνολογικής διαμεσολάβησης και αντίστοιχων συστημάτων/εφαρμογών εξ αποστάσεως εξέτασης, που διασφαλίζει την αυθεντικοποίηση του χρήστη, τη φυσική ταυτοποίησή του και την επιτήρηση της διαδικασίας εξέτασης, όπου αυτή κρίνεται αναγκαία.

3. Η επεξεργασία των προσωπικών δεδομένων κατά τη διαδικασία της εξ αποστάσεως εξέτασης πραγματοποιείται με τρόπο ώστε να επιτυγχάνεται το κατάλληλο επίπεδο ασφάλειας έναντι κινδύνων, όπως τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση,

άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ’ άλλο τρόπο σε επεξεργασία. Το διδακτικό προσωπικό, οι επιτηρητές/τριες και πρόσωπα που παρέχουν τεχνική ή/και διοικητική υποστήριξη (όπως ο/η διαχειριστής/τρια πλατφόρμας) δεσμεύονται από υποχρεώσεις εμπιστευτικότητας. Η επιλογή της ηλεκτρονικής πλατφόρμας για την πραγματοποίηση της εξέτασης με εξ αποστάσεως μεθόδους πραγματοποιείται με κριτήριο την αξιοπιστία και την παροχή εγγυήσεων ως προς την προστασία των προσωπικών δεδομένων.

Άρθρο 11
Δικαιώματα και Υποχρεώσεις φοιτητών - Διαγραφή Μεταπτυχιακού Φοιτητή.

11.1. Δικαιώματα Φοιτητή

Οι μεταπτυχιακοί/ες φοιτητές/τριες έχουν όλα τα δικαιώματα και τις παροχές που προβλέπονται και για τους φοιτητές του πρώτου κύκλου σπουδών, πλην του δικαιώματος παροχής δωρεάν διδακτικών συγγραμμάτων. Οι μεταπτυχιακοί/κές φοιτητές/τριες δύνανται να χρησιμοποιούν την υπάρχουσα υλικοτεχνική υποδομή του Πανεπιστημίου Δυτικής Αττικής, η οποία περιλαμβάνει χώρους διδασκαλίας κατάλληλα εξοπλισμένους με σύγχρονα μέσα διδασκαλίας και Η/Υ, τη Βιβλιοθήκη, και τις εγκαταστάσεις του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών.

Οι μεταπτυχιακοί φοιτητές που δεν έχουν άλλη ιατροφαρμακευτική και νοσοκομειακή περίθαλψη, δικαιούνται πλήρη ιατροφαρμακευτική και νοσοκομειακή περίθαλψη στο Εθνικό Σύστημα Υγείας (Ε.Σ.Υ.) με κάλυψη των σχετικών δαπανών από τον Εθνικό Οργανισμό Παροχής Υπηρεσιών Υγείας (Ε.Ο.Π.Υ.Υ.) κατ’ ανάλογη εφαρμογή του άρθρου 33 του ν. 4368/2016 (Α’ 83).

Οι μεταπτυχιακοί φοιτητές δικαιούνται δωρεάν σίτιση με βάση την ατομική και οικογενειακή οικονομική τους κατάσταση και την εντοπιότητά τους.

Οι μεταπτυχιακοί/ες φοιτητές/τριες δύνανται να διεκδικήσουν εξωτερική χρηματοδότηση των σπουδών τους από διάφορα Ιδρύματα ή φορείς του δημοσίου και ιδιωτικού τομέα και Ερευνητικά Ινστιτούτα.

Οι μεταπτυχιακοί/ες φοιτητές/τριες δύνανται να καλύπτονται οικονομικά από χρηματοδοτούμενα προγράμματα έρευνας στα οποία συμμετέχουν. Οι σχετικές λεπτομέρειες ορίζονται με απόφαση της Σ.Ε. ή την Ε.Π.Σ., ύστερα από εισήγησή του/της Διευθυντή/ντριας του Δ.Δ.Π.Μ.Σ.

Οι μεταπτυχιακοί/ες φοιτητές/τριες μπορούν να συμμετάσχουν στα προγράμματα ανταλλαγής φοιτητών/τριών (π.χ. ERASMUS) του Πανεπιστημίου ή σε άλλα ερευνητικά προγράμματα αλλοδαπών Α.Ε.Ι., στο πλαίσιο διακρατικών συμφωνιών του Τμήματος με ομοταγή ιδρύματα και να εγγράφονται σε αυτά ως φιλοξενούμενοι φοιτητές/τριες.

Το Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών οφείλει να εξασφαλίζει υποχρεωτικά στους/στις μεταπτυχιακούς/κές φοιτητές/τριες με αναπηρία ή/και ειδικές εκπαιδευτικές ανάγκες προσβασιμότητα στα προτεινόμενα προγράμματα και την διδασκαλία ή άλλες διευκολύνσεις. Οι διευκολύνσεις αυτές σύμφωνα με την κείμενη νομοθεσία, θα πρέπει να ορισθούν από το Τμήμα αναλυτικά.

Παράλληλα δίνεται η δυνατότητα εξ αποστάσεως εκπαίδευσης με όλα τα διατιθέμενα μέσα ώστε ο φοιτητής ακόμα και αν παρακολουθεί από απόσταση να είναι ωσεί παρών (χρήση bluetooth ηχείων και μικροφώνου συνδεδεμένων στο Η.Υ του διδάσκοντα.

11.2. Υποχρεώσεις Φοιτητή

Οι μεταπτυχιακοί φοιτητές έχουν τις κάτωθι υποχρεώσεις:

- Να παρακολουθούν ανελλιπώς τα μαθήματα του ισχύοντος προγράμματος σπουδών.
- Να υποβάλλουν τις απαιτούμενες εργασίες μέσα στις καθορισμένες προθεσμίες.
- Να προσέρχονται στις προβλεπόμενες εξετάσεις.
- Να δηλώνουν υπεύθυνα, ότι η διπλωματική εργασία δεν αποτελεί προϊόν λογοκλοπής ούτε στο σύνολο ούτε σε επιμέρους τμήματα αυτής.
- Να καταβάλλουν τα προβλεπόμενα τέλη φοίτησης όπως ορίζεται στον Εσωτερικό Κανονισμό του Δ.Δ.Π.Μ.Σ..
- Να σέβονται και να τηρούν τον Κανονισμό Μεταπτυχιακών Σπουδών, τις αποφάσεις των οργάνων του Δ.Δ.Π.Μ.Σ., του Τμήματος και του Πανεπιστημίου Δυτικής Αττικής, καθώς και την ακαδημαϊκή δεοντολογία.

Οι μεταπτυχιακοί φοιτητές καλούνται να συμμετέχουν και να παρακολουθούν σεμινάρια, συζητήσεις, συνέδρια/ημερίδες με γνωστικό αντικείμενο συναφές με αυτό του Δ.Δ.Π.Μ.Σ., διαλέξεις ή άλλες επιστημονικές εκδηλώσεις του Δ.Δ.Π.Μ.Σ. Οι μεταπτυχιακοί φοιτητές δύναται να ασκούν επικουρικό διδακτικό έργο σε προγράμματα σπουδών πρώτου κύκλου με απόφαση αρμοδίου οργάνου του Δ.Δ.Π.Μ.Σ. Οι μεταπτυχιακοί φοιτητές εκδίδουν ακαδημαϊκή ταυτότητα υποχρεωτικά μέσω της Ηλεκτρονικής Υπηρεσίας Απόκτησης Ακαδημαϊκής Ταυτότητας του Υπουργείου Παιδείας και Θρησκευμάτων.

11.3. Διαγραφή Μεταπτυχιακού Φοιτητή

Η διαγραφή μεταπτυχιακού/κής φοιτητή/τριας γίνεται κατόπιν σχετικής εισήγησης της Σ.Ε. του Δ.Δ.Π.Μ.Σ. προς την Ε.Π.Σ. και λήψης σχετικής απόφασης. Η απόφαση κοινοποιείται εντός 15 ημερών στον/ην ενδιαφερόμενο/νη μεταπτυχιακό/κη φοιτητή/τρια και έχει δικαίωμα υποβολής ένστασης εντός δέκα πέντε (15) ημέρων από την ημερομηνία έκδοσης της. Η ένσταση κρίνεται τελεσίδικα από τα ανωτέρω όργανα.

Η Συνέλευση του Τμήματος ή η Ε.Π.Σ. μετά την εισήγηση της Σ.Ε., δύναται να αποφασίσει τη διαγραφή μεταπτυχιακών φοιτητών για τους παρακάτω λόγους:

α. Πλημμελής εκπλήρωση των υποχρεώσεων του/της μεταπτυχιακού/ης φοιτητή/τριας, όπως αυτές περιγράφονται στον Εσωτερικό Κανονισμό Δ.Δ.Π.Μ.Σ.

β. Μη καταβολή των προβλεπόμενων τελών φοίτησης (σε κάθε περίπτωση, φοιτητής, ο οποίος δεν έχει ανταποκριθεί στις οικονομικές του υποχρεώσεις, δε δικαιούται να λάβει ούτε βεβαίωση ολοκλήρωσης σπουδών, ούτε το Δίπλωμα Μεταπτυχιακών Σπουδών),

γ. Πειθαρχικά παραπτώματα, όπως παράβαση ακαδημαϊκής δεοντολογίας και γενικότερα κάθε παράβαση της κείμενης νομοθεσίας και του Εσωτερικού Κανονισμού του Πα.Δ.Α.

δ. Αίτηση διαγράφης του/της ίδιου/ας του μεταπτυχιακού/κής φοιτητή/τριας.

ε. Έχουν επανειλημμένως αποτύχει στην εξέταση μαθήματος ή μαθημάτων όπως ορίζεται στον Εσωτερικό Κανονισμό.

στ. Δεν ανανέωσαν την εγγραφή τους ή δεν παρακολούθησαν μαθήματα για δύο (2) συνεχόμενα εξάμηνα ζ. Έχουν υποπέσει στο παράπτωμα της λογοκλοπής ή σε παράπτωμα που εμπίπτει στο δίκαιο περί πνευματικής ιδιοκτησίας (ν. 2121/1993).

η) Για οποιαδήποτε άλλο λόγο κρίνεται απαραίτητη.

Σε περίπτωση οριστικής διακοπής φοίτησης ή διαγραφής μεταπτυχιακού/κής φοιτητή/τριας για οποιοδήποτε λόγο, τα ήδη καταβληθέντα δίδακτρα δεν επιστρέφονται.

Άρθρο 12
Τέλη φοίτησης

Το ύψος των τελών φοίτησης για το Δ.Δ.Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» ανέρχεται στο ποσό των 2900 (δύο χιλιάδων και εννιακοσίων) ευρώ. Στα τέλη φοίτησης που καταβάλλονται εφάπαξ, χορηγείται έκπτωση 10%. Το τέλος εγγραφής ανέρχεται στο ποσό των 200 € και καταβάλλεται με την αποδοχή της θέσεως από τον υποψήφιο εντός 20 ημερολογιακών ημέρων από την ανακοίνωση των αποτελεσμάτων. Η μέγιστη διάρκεια καταβολής του υπολειπόμενου ποσού είναι εννέα (9) ισόποσες δόσεις που καταβάλλονται κατά την διάρκεια του κάθε εξαμήνου και η τελευταία καταβάλλεται με την υποβολή της διπλωματικής εργασίας του φοιτητή.

Οι μεταπτυχιακοί φοιτητές του Δ.Δ.Π.Μ.Σ., υποχρεούνται στην καταβολή αυτών. Το ύψος των προβλεπόμενων τελών φοίτησης για το σύνολο του προγράμματος καθορίζεται στο ΦΕΚ ίδρυσης του Δ.Δ.Π.Μ.Σ..

Στις περιπτώσεις διακοπής της φοίτησης το συνολικό καταβληθέν ποσό δεν επιστρέφεται.

Η καταβολή των διδάκτρων γίνεται στον Ειδικό Λογαριασμό Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.) του Πανεπιστημίου Δυτικής Αττικής, ο οποίος είναι αρμόδιος για τη διαχείρισή τους.

Οι μεταπτυχιακοί φοιτητές οφείλουν να έχουν εξοφλήσει όλες τις οικονομικές τους υποχρεώσεις πριν την χορήγηση βεβαίωσης ολοκλήρωσης σπουδών και την απονομή του Διπλώματος Μεταπτυχιακών Σπουδών.

Στο Δ.Δ.Π.Μ.Σ «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» παρέχεται η δυνατότητα απαλλαγής των τελών φοίτησης, σύμφωνα με την ισχύουσα νομοθεσία και όπως περιγράφεται στο άρθρο 14 του Πρότυπου Κανονισμού Σπουδών των Δ.Δ.Π.Μ.Σ. του Πα.Δ.Α. (Β’ 4861) και του παρόντος κανονισμού.

Άρθρο 13
Υποτροφίες

Το Δ.Δ.Π.Μ.Σ. «ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ» δύναται να χορηγεί ανταποδοτικές υποτροφίες και μη, ή βραβεία αριστείας σε μεταπτυχιακούς/κές φοιτητές/τριες πλήρους φοίτησης, σύμφωνα με απόφαση της Ε.Π.Σ.

Οι υποτροφίες χορηγούνται βάσει αντικειμενικών κριτηρίων, ακαδημαϊκών, οικονομικών και κοινωνικών, τα οποία είναι:

1. Ακαδημαϊκά:

α) Ο μέσος όρος βαθμολογίας του προηγούμενου εξάμηνου.

β) Πρόσφατες ακαδημαϊκές επιδόσεις (βραβεία και τιμητικές διακρίσεις).

2. Οικονομικά:

Εγγεγραμμένοι φοιτητές Δ.Δ.Π.Μ.Σ. δύνανται να φοιτούν δωρεάν σε Δ.Δ.Π.Μ.Σ., αν προβλέπεται η καταβολή τελών φοίτησης, εφόσον πληρούν τα οικονομικά ή κοινωνικά κριτήρια σύμφωνα με τις διατάξεις του άρθρου 86 του ν. 4957/2022 και της υπό στοιχεία 108990/Ζ1/8-9-2022 υπουργικής απόφασης (Β’ 4899).

3. Κοινωνικά:

α) Διαζευγμένος/η με προστατευόμενα μέλη (παιδιά).

β) Αναπηρία υποψηφίου/ας.

γ) Μονογονεϊκή οικογένεια.

δ) Ορφανός/η από δυο γονείς που δεν έχει υπερβεί το 25ο έτος της ηλικίας του/της.

ε) Τέκνο πολύτεκνης οικογένειας.

στ) Μέλη ίδιας οικογενείας.

Διαδικασία:

Μετά από εισήγηση της Συντονιστικής Επιτροπής του Δ.Δ.Π.Μ.Σ., προκηρύσσεται πρόσκληση υποβολής αιτήσεως για τη χορήγηση υποτροφίας. Οι υποψήφιοι/ες οφείλουν να συμπληρώσουν όλα τα υποχρεωτικά πεδία της αίτησης με τα απαιτούμενα κατά περίπτωση δικαιολογητικά και τα υποβάλλουν στην Γραμματεία του Τμήματος στις ημερολογιακές προθεσμίες που ορίζονται στην πρόσκληση. Η αίτηση επέχει θέση Υπεύθυνης Δήλωσης του ν. 1599/1986.

Το αρμόδιο όργανο αξιολογεί και κατατάσσει τις υποψηφιότητες βάσει των κριτηρίων που έχουν οριστεί στον εσωτερικό Κανονισμό λειτουργίας του Δ.Δ.Π.Μ.Σ. και εισηγείται τον κατάλογο ονομάτων των υποψηφίων προς την Ε.Π.Σ.

Ο ανώτατος αριθμός υποτροφιών στο Δ.Δ.Π.Μ.Σ. ορίζεται σε μια (1) ανά έτος εισαγωγής εφόσον υπάρχει διαθέσιμο ποσό συνυπολογίζοντας τους τυχόν υποτρόφους και τους τυχόν δικαιούχους μειωμένων διδάκτρων σύμφωνα με το παρακάτω σχετικό, θεωρώντας ως μέγιστο ποσό παροχών το 20% του ετησίου θεωρητικού μεγίστου ποσού παροχών, όπου θεωρητικό μέγιστο είναι το 70% του 30% του καταβλητέου ποσού απο το σύνολο των φοιτούντων ανά Ακαδημαϊκό έτος.

Μείωση διδάκτρων δύναται να παρέχεται, με ομόφωνη απόφαση της Ε.Π.Σ., σε φοιτητές οι οποίοι υπηρετούν στην ίδια μονάδα σωμάτων ασφαλείας ή ενόπλων δυνάμεων της χώρας ή δημοσίων οργανισμών με συναφείς αρμοδιότητες και το ποσοστό μείωσης των διδάκτρων υπολογίζεται σε ποσοστό κατά μέγιστο 20% εφόσον ο αριθμός τους είναι μεγαλύτερος του τρία (3) και εφόσον υπάρχει διαθέσιμο με βάση το ανωτέρω σκεπτικό (δεν έχει καλυφθεί το όριο των παρεχόμενων υποτροφιών).

Υποτροφία δεν χορηγείται στην περίπτωση που ο μεταπτυχιακός φοιτητής λαμβάνει ήδη υποτροφία από άλλη πηγή.

Άρθρο 14
Δίπλωμα Μεταπτυχιακών Σπουδών (Δ.Μ.Σ)

Το Δίπλωμα Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) είναι δημόσιο έγγραφο. Στον/Στην απόφοιτο/η του Δ.Δ.Π.Μ.Σ. μπορεί να χορηγείται, πριν από την απονομή, βεβαίωση ότι έχει περατώσει επιτυχώς την παρακολούθηση του Δ.Δ.Π.Μ.Σ. και αναλυτική βαθμολογία με τις αντίστοιχες πιστωτικές μονάδες (ECTS). Στο Δίπλωμα Μεταπτυχιακών Σπουδών επισυνάπτεται Παράρτημα Διπλώματος το οποίο είναι επεξηγηματικό έγγραφο και δεν υποκαθιστά τον επίσημο τίτλο σπουδών ή την αναλυτική βαθμολογία των μαθημάτων. Το Παράρτημα Διπλώματος επισυνάπτεται στο Δ.Μ.Σ. και παρέχει πληροφορίες σχετικά με τη φύση, το επίπεδο, το γενικότερο πλαίσιο εκπαίδευσης, το περιεχόμενο και το καθεστώς των σπουδών, οι οποίες ολοκληρώθηκαν με επιτυχία από το άτομο που αναγράφεται ονομαστικά στο πρωτότυπο του τίτλου. Στο Παράρτημα δεν γίνονται αξιολογικές κρίσεις και δεν υπάρχουν δηλώσεις ισοτιμίας ή αντιστοιχίας ή προτάσεις σχετικά με την αναγνώριση του Δ.Μ.Σ. στο εξωτερικό. Το Παράρτημα Διπλώματος εκδίδεται αυτομάτως και χωρίς καμία οικονομική επιβάρυνση στην ελληνική και στην αγγλική γλώσσα, και πρέπει να πληροί τις προϋποθέσεις γνησιότητας που απαιτούνται για τον χορηγούμενο τίτλο σπουδών. Η ημερομηνία έκδοσης του Παραρτήματος δεν συμπίπτει υποχρεωτικά με την ημερομηνία χορήγησης του Δ.Μ.Σ., αλλά δεν μπορεί ποτέ να είναι προγενέστερη από αυτή.

Ο βαθμός του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) προκύπτει από τον βαθμό αξιολόγησης στα μαθήματα και στη Μεταπτυχιακή Διπλωματική Εργασία (Μ.Δ.Ε.).

Αναλυτικότερα σε κάθε εξάμηνο ο φοιτητής/τρια λαμβάνει βαθμολογία σε κάθε μάθημα που εξετάζεται και εάν αξιολογηθεί επιτυχώς, πιστώνεται αναλογικά τις πιστωτικές μονάδες που αντιστοιχούν. Ο τελικός βαθμός του Δ.Μ.Σ. προκύπτει από τον βαθμό αξιολόγησης:

α) Στα μαθήματα,

β) στη Μεταπτυχιακή Διπλωματική Εργασία.

Ο βαθμός του Διπλώματος Μεταπτυχιακών Σπουδών (Δ.Μ.Σ.) εξάγεται με προσέγγιση δύο δεκαδικών ψηφίων και προκύπτει από το 70% του ΜΟ των βαθμών των δύο πρώτων εξαμήνων και κατά 30% από τον βαθμό της πτυχιακής εργασίας η οποία βαθμολογείται με δέκα (10) μόνο εφόσον έχει οδηγήσει σε δημοσίευση.

Ο τύπος που προκύπτει δίνεται από την σχέση:

Β1=(Β1*Π1+Β2*Π2+……..+Βν*Πν)/(Π1+Π2+…..Πν)

Β2 = Βαθμός Πτυχιακής

Τελικός Βαθμός = 0,7*Β1+ 0,3*Β2

όπου Β1,Β2….Βν είναι οι βαθμοί όλων των μαθημάτων που εξετάστηκε επιτυχώς ο φοιτητής/τρια και Π1,Π2….. Πν είναι οι πιστωτικές μονάδες που αντιστοιχούν σε κάθε μάθημα.

Προβιβάσιμοι βαθμοί είναι το πέντε (5) και οι μεγαλύτεροί του. Η βαθμολογική κλίμακα για την αξιολόγηση της επίδοσης των μεταπτυχιακών φοιτητών/τριών ορίζεται από το μηδέν (0) ως το δέκα (10) ως ακολούθως:

- Άριστα: από οκτώ και πενήντα (8,50) μέχρι δέκα (10),

- Λίαν καλώς: από έξι και πενήντα (6,50) ως και οκτώ και σαράντα εννέα (8,49),

- Καλώς: από πέντε (5) ως και έξι και σαράντα εννέα (6,49) ή

- Απορρίπτεται: από μηδέν (0) έως τέσσερα και ενενήντα εννέα (4,99).

Άρθρο 15
Διδάσκοντες Προγραμμάτων
Μεταπτυχιακών Σπουδών

15.1. Το διδακτικό έργο του Προγράμματος Μεταπτυχιακών Σπουδών ανατίθεται, κατόπιν απόφασης της της Ε.Π.Σ. στις ακόλουθες κατηγορίες διδασκόντων:

α) μέλη Διδακτικού Ερευνητικού Προσωπικού (Δ.Ε.Π.), Ειδικού Εκπαιδευτικού Προσωπικού (Ε.Ε.Π.), Εργαστηριακού Διδακτικού Προσωπικού (Ε.ΔΙ.Π.) και Ειδικού Τεχνικού Εργαστηριακού Προσωπικού (Ε.Τ.Ε.Π.) του Τμήματος ή άλλων Τμημάτων του Πα.Δ.Α. ή άλλου Ανώτατου Εκπαιδευτικού Ιδρύματος (Α.Ε.Ι.) ή Ανώτατου Στρατιωτικού Εκπαιδευτικού Ιδρύματος (Α.Σ.Ε.Ι.), με πρόσθετη απασχόληση πέραν των νόμιμων υποχρεώσεών τους.

β) ομότιμους Καθηγητές ή αφυπηρετήσαντα μέλη Δ.Ε.Π. του Τμήματος ή άλλων Τμημάτων του ΠΑΔΑ ή άλλου Α.Ε.Ι.,

γ) συνεργαζόμενους καθηγητές,

δ) εντεταλμένους διδάσκοντες,

ε) επισκέπτες καθηγητές ή επισκέπτες ερευνητές,

στ) ερευνητές και ειδικούς λειτουργικούς επιστήμονες ερευνητικών και τεχνολογικών φορέων του άρθρου 13Α του ν. 4310/2014 (Α’ 258) ή λοιπών ερευνητικών κέντρων και ινστιτούτων της ημεδαπής ή αλλοδαπής,

ζ) επιστήμονες αναγνωρισμένου κύρους, οι οποίοι διαθέτουν εξειδικευμένες γνώσεις και σχετική εμπειρία στο γνωστικό αντικείμενο του Δ.Δ.Π.Μ.Σ.

15.2. Η ανάθεση του διδακτικού έργου του Δ.Δ.Π.Μ.Σ. πραγματοποιείται με απόφαση της Ε.Π.Σ., κατόπιν εισήγησης της Συντονιστικής Επιτροπής του Π.Μ.Σ ή του Διευθυντή του Δ.Δ.Π.Μ.Σ.. Με απόφαση της Ε.Π.Σ δύναται να ανατίθεται επικουρικό διδακτικό έργο στους υποψήφιους διδάκτορες του Τμήματος ή της Σχολής, με αντικείμενο συναφές με το παρεχόμενο επικουρικό διδακτικό έργο του Δ.Δ.Π.Μ.Σ., υπό την επίβλεψη διδάσκοντος του Δ.Δ.Π.Μ.Σ., κατόπιν εισηγήσεως της Σ.Ε.

15.3. Δικαίωμα επίβλεψης διπλωματικών εργασιών έχουν οι διδάσκοντες των περ. α) έως στ) της παρ. 1, υπό την προϋπόθεση ότι είναι κάτοχοι διδακτορικού διπλώματος. Με απόφαση του αρμοδίου οργάνου του Δ.Δ.Π.Μ.Σ., δύναται να ανατίθεται η επίβλεψη διπλωματικών εργασιών και σε μέλη Δ.Ε.Π., Ε.Ε.Π. και Ε.ΔΙ.Π. του Τμήματος, που δεν έχουν αναλάβει διδακτικό έργο στο Δ.Δ.Π.Μ.Σ.

15.4. Όλες οι κατηγορίες διδασκόντων δύνανται να αμείβονται αποκλειστικά από τους πόρους του Δ.Δ.Π.Μ.Σ. Δεν επιτρέπεται η καταβολή αμοιβής ή άλλης παροχής από τον κρατικό προϋπολογισμό ή το πρόγραμμα δημοσίων επενδύσεων. Με απόφαση του αρμόδιου οργάνου του Δ.Δ.Π.Μ.Σ. περί ανάθεσης του διδακτικού έργου, καθορίζεται το ύψος της αμοιβής κάθε διδάσκοντος. Ειδικώς οι διδάσκοντες που έχουν την ιδιότητα μέλους Δ.Ε.Π., δύνανται να αμείβονται επιπρόσθετα για έργο που προσφέρουν προς το Δ.Δ.Π.Μ.Σ., εφόσον εκπληρώνουν τις ελάχιστες εκ του νόμου υποχρεώσεις τους, όπως ορίζονται στην παρ. 2 του άρθρου 155, του

ν. 4957/2022. Το τελευταίο εδάφιο εφαρμόζεται αναλογικά και για τα μέλη Ε.Ε.Π., Ε.ΔΙ.Π. και Ε.Τ.Ε.Π., εφόσον εκπληρώνουν τις ελάχιστες εκ του νόμου υποχρεώσεις τους.

Στις υποχρεώσεις των διδασκόντων περιλαμβάνονται, μεταξύ άλλων, ο καθορισμός και η περιγραφή του μαθήματος, η παράθεση σχετικής βιβλιογραφίας, ο καθορισμός του τρόπου εξέτασης του μαθήματος, η επικοινωνία με τους/τις μεταπτυχιακούς/κες φοιτητές/τριες.

15.5. Στο Δ.Δ.Π.Μ.Σ. με απόφαση της Επιτροπής Προγράμματος Σπουδών (Ε.Π.Σ.) εφαρμόζεται ο θεσμός του Ακαδημαϊκού Συμβούλου. Σκοπός της λειτουργίας του εν λόγω θεσμού είναι η παροχή συμβουλευτικής στους μεταπτυχιακούς φοιτητές κατά τη διάρκεια των σπουδών τους σε ακαδημαϊκά θέματα με εξατομικευμένο τρόπο. Προσδοκώμενο αποτέλεσμα είναι η διευκόλυνση των μεταπτυχιακών φοιτητών στην ολοκλήρωση των σπουδών τους με παράλληλη αξιοποίηση των ιδιαίτερων δεξιοτήτων και ενδιαφερόντων τους στο έδαφος της εκπαιδευτικής και ερευνητικής διαδικασίας. Ο Ακαδημαϊκός Σύμβουλος επιλέγει τον τρόπο προσέγγισης και παροχής συμβουλευτικής στους φοιτητές που του ανατίθενται σε κάθε ακαδημαϊκό έτος.

Άρθρο 16
Επικουρικό διδακτικό έργο
μεταπτυχιακών φοιτητών

Με απόφαση της Ε.Π.Σ. του Δ.Δ.Π.Μ.Σ. είναι δυνατή η έγκριση της συμμετοχής μεταπτυχιακών φοιτητών, υποψηφίων διδακτόρων και μεταδιδακτόρων στην παροχή επικουρικού διδακτικού έργου σε προγράμματα σπουδών πρώτου ή δεύτερου κύκλου.

Το Πα.Δ.Α. δύναται να χορηγεί ανταποδοτικές υποτροφίες σε μεταπτυχιακούς φοιτητές με την υποχρέωση υποστήριξης της εκπαιδευτικής διαδικασίας και παροχής επικουρικού διδακτικού έργου.

Ως επικουρικό διδακτικό έργο ορίζεται η επικουρία των μελών Διδακτικού Ερευνητικού Προσωπικού κατά την άσκηση του διδακτικού τους έργου, η άσκηση των φοιτητών, η διεξαγωγή φροντιστηρίων, εργαστηριακών ασκήσεων, η εποπτεία εξετάσεων και η διόρθωση ασκήσεων.

Άρθρο 17
Χρηματοδότηση - Οικονομική διαχείριση

Η χρηματοδότηση του Δ.Δ.Π.Μ.Σ. προέρχεται από:

α) Τέλη φοίτησης,

β) δωρεές, χορηγίες και πάσης φύσεως οικονομικές ενισχύσεις,

γ) κληροδοτήματα,

δ) πόρους από ερευνητικά έργα ή προγράμματα,

ε) ιδίους πόρους του Πανεπιστημίου Δυτικής Αττικής και

στ) τον κρατικό προϋπολογισμό ή το πρόγραμμα δημοσίων επενδύσεων.

Η καταβολή των τελών φοίτησης, πραγματοποιείται από τον ίδιο τον φοιτητή ή από τρίτο φυσικό ή νομικό πρόσωπο για λογαριασμό του φοιτητή.

Η διαχείριση των πόρων του Δ.Δ.Π.Μ.Σ. πραγματοποιείται από τον Ειδικό Λογαριασμό Κονδυλίων Έρευνας (Ε.Λ.Κ.Ε.) του Πα.Δ.Α.

Οι πόροι του Δ.Δ.Π.Μ.Σ. κατανέμονται ως εξής:

α) Ποσό που αντιστοιχεί στο τριάντα τοις εκατό (30%) των συνολικών εσόδων που προέρχονται από τέλη φοίτησης παρακρατείτε από τον Ε.Λ.Κ.Ε. Στο ποσό αυτό συμπεριλαμβάνεται το ποσοστό παρακράτησης υπέρ του Ε.Λ.Κ.Ε. για την οικονομική διαχείριση των Δ.Δ.Π.Μ.Σ. Στα έσοδα του Δ.Δ.Π.Μ.Σ. των περ. β) έως δ) της παρ. 1 πραγματοποιείται η παρακράτηση υπέρ Ε.Λ.Κ.Ε. που ισχύει για τα έσοδα από αντίστοιχες πηγές χρηματοδότησης.

β) Το υπόλοιπο ποσό των συνολικών εσόδων του Δ.Δ.Π.Μ.Σ. (70%) διατίθεται για την κάλυψη των λειτουργικών δαπανών του Δ.Δ.Π.Μ.Σ.

Μεθοδολογία κατάρτισης προϋπολογισμών εσόδων:

Ως προς τα έσοδα αναγράφονται οι πηγές χρηματοδότησης, σύμφωνα με τις παρ. 1 και 2 του άρθρου 84 του ν. 4957/2022, και τα αντίστοιχα ποσά- αναμενόμενες εισροές από κάθε πηγή χρηματοδότησης.

Έσοδα - χρηματοδότηση	
1	Τέλη φοίτησης
2	Δωρεές, χορηγίες και πάσης φύσεως οικονομικές ενισχύσεις
3	Κληροδοτήματα
4	Πόροι από ερευνητικά έργα ή προγράμματα
5	Ίδιοι πόροι του Πα.Δ.Α.
6	Κρατικός προϋπολογισμός ή Πρόγραμμα Δημοσίων επενδύσεων
Σύνολο	

Αναφέρεται στον προϋπολογισμό ενός πλήρους κύκλου φοίτησης του Δ.Δ.Π.Μ.Σ. για τους εισακτέους του εν λόγω έτους.

Αναλυτικός προϋπολογισμός εξόδων.

Ως προς τα έξοδα, αναγράφονται οι κατηγορίες των λειτουργικών εξόδων και τα αντίστοιχα ποσά - αναμενόμενες εκροές.

Συγκεκριμένα, ποσοστό εβδομήντα τοις εκατό (70%) των λειτουργικών εξόδων του Δ.Δ.Π.Μ.Σ. κατανέμονται σε:

α) Αμοιβές για τη διοικητική - τεχνική υποστήριξη,

β) αμοιβές διδακτικού προσωπικού,

γ) δαπάνες μετακίνησης,

δ) δαπάνες εξοπλισμού και υλικοτεχνικής υποδομής,

ε) δαπάνες χορήγησης υποτροφιών.

στ) λοιπές λειτουργικές δαπάνες (περ. α. της παρ. 4 του άρθρου 80 του ν. 4957/2022).

Οι αμοιβές του τακτικού διδακτικού, τεχνικού και διοικητικού προσωπικού των Ιδρυμάτων αφορά εργασία που υπερβαίνει τις κατά νόμο υποχρεώσεις τους.

Έξοδα - κατηγορίες δαπανών	
1	Αμοιβές για τη διοικητική - τεχνική υποστήριξη
2	Αμοιβές διδακτικού προσωπικού
3	Δαπάνες μετακίνησης
4	δαπάνες εξοπλισμού και υλικοτεχνικής υποδομής
5	Δαπάνες χορήγησης υποτροφιών
6	Λοιπές λειτουργικές δαπάνες
Μερικό Σύνολο (70%)	
7	Λειτουργικά έξοδα Πα.Δ.Α. (30%) ΕΛΚΕ
Σύνολο	

Σύμφωνα με την παρ. 2, του άρθρου 85, του ν. 4957/2022, καθορίζεται ποσοστό δύο τοις εκατό (2%), ως ανώτατο ποσοστό επί των συνολικών ετήσιων εσόδων κάθε Δ.Δ.Π.Μ.Σ. που δύναται να διατίθεται προς Έργο/Πρόγραμμα της παρ. 1 του ίδιου άρθρου.

Άρθρο 18
Λογοκλοπή

Ο/Η μεταπτυχιακός/η φοιτητής/τρια υποχρεούται να αναφέρει με τον ενδεδειγμένο τρόπο αν χρησιμοποίησε το έργο και τις απόψεις άλλων. Επιπλέον, οι μεταπτυχιακοί φοιτητές που έχουν χρησιμοποιήσει τις υπηρεσίες και τη βοήθεια Τεχνητής Νοημοσύνης (Artificial Intelligence, AI) για την εκπόνηση εργασιών που τους ανατίθενται στα πλαίσια του ΠΜΣ ή/και της Μ.Δ.Ε., θα πρέπει στο προοίμιο του κειμένου να περιλάβουν και «Δήλωση σχετικά με τη χρήση δημιουργικής Τεχνητής Νοημοσύνης (generative AI) και τεχνολογιών υποβοηθούμενων από Τεχνητή Νοημοσύνη κατά τη διαδικασία της συγγραφής», όπου θα δηλώνουν ποιο εργαλείο χρησιμοποίησαν και για ποιο λόγο.

Η λογοκλοπή θεωρείται σοβαρό ακαδημαϊκό παράπτωμα. Λογοκλοπή θεωρείται η αντιγραφή εργασίας κάποιου/ας άλλου/ης, καθώς και η χρησιμοποίηση εργασίας άλλου/ης - δημοσιευμένης ή μη - χωρίς τη δέουσα αναφορά. Η αντιγραφή οποιουδήποτε υλικού τεκμηρίωσης, ακόμη και από μελέτες του/της ιδίου/ας του/της υποψηφίου/ας, χωρίς σχετική αναφορά, μπορεί να στοιχειοθετήσει απόφαση της Συνέλευσης του Τμήματος ή της Επιτροπής Προγράμματος Σπουδών, για διαγραφή του/της. Στις παραπάνω περιπτώσεις, η Συνέλευση του Τμήματος ή η Επιτροπή Προγράμματος Σπουδών, μπορεί να αποφασίσει τη διαγραφή του/της, αφού προηγουμένως του/της δοθεί η δυνατότητα να εκθέσει, προφορικώς ή γραπτώς, τις απόψεις του/της επί του θέματος.

Οποιοδήποτε παράπτωμα ή παράβαση ακαδημαϊκής δεοντολογίας παραπέμπεται για αντιμετώπιση του προβλήματος στη Συνέλευση του Τμήματος ή την Ε.Π.Σ. Ως παραβάσεις θεωρούνται και τα παραπτώματα της αντιγραφής ή της λογοκλοπής και γενικότερα κάθε παράβαση των διατάξεων περί πνευματικής ιδιοκτησίας από μεταπτυχιακό/η φοιτητή/τρια κατά τη συγγραφή εργασιών στο πλαίσιο των μαθημάτων ή την εκπόνηση της διπλωματικής εργασίας.

Άρθρο 19
Απονομή πτυχίων - ορκωμοσίες

Φοιτητής που ολοκλήρωσε επιτυχώς τις μεταπτυχιακές σπουδές του, ορκίζεται σε δημόσια τελετή ορκωμοσίας, ενώπιον του/της Πρύτανη/νισσας ή του/της Αντιπρύτανη/ις ως εκπροσώπου του/της Πρύτανη και του/της Προέδρου του Τμήματος, που γίνεται μετά τη λήξη εκάστης εξεταστικής περιόδου, σε ημέρα και ώρα, που ορίζεται από τον/την Πρύτανη σε συνεργασία με τους Προέδρους των Τμημάτων. Ο όρκος δεν αποτελεί συστατικό στοιχείο της επιτυχούς περάτωσης των σπουδών, είναι όμως αναγκαία προϋπόθεση για τη χορήγηση του Μεταπτυχιακού Διπλώματος Σπουδών. Για λόγους ανωτέρας βίας (π.χ. λόγοι υγείας, διαμονή ή εργασία στο εξωτερικό, στρατιωτικές υποχρεώσεις) και με αίτησή του προς τη Γραμματεία του Τμήματος του, ο/η απόφοιτος/η μπορεί να ζητήσει τη χορήγηση του τίτλου σπουδών χωρίς να συμμετάσχει στην τελετή ορκωμοσίας ή να ζητήσει να συμμετάσχει σε επόμενη τελετή ορκωμοσίας. Η εξαίρεση από την υποχρέωση συμμετοχής σε ορκωμοσία εγκρίνεται από τον Πρόεδρο του Τμήματος. Πριν από την ορκωμοσία ή την απαλλαγή από αυτή, μπορεί να δίδεται στους αποφοίτους σχετικό πιστοποιητικό για την επιτυχή περάτωση των σπουδών τους.

Δίπλωμα Μεταπτυχιακών Σπουδών που χορηγήθηκε, είναι δυνατόν να ανακληθεί ή να ακυρωθεί, αν αποδειχθεί ότι δεν συνέτρεχαν την εποχή της απόκτησής του οι εκ του νομικού και θεσμικού πλαισίου προϋποθέσεις κτήσης του. Η ανάκληση ή ακύρωση γίνεται μετά από απόφαση της οικείας Συνέλευσης, η οποία κοινοποιείται στον/στην Πρύτανη του Ιδρύματος.

Άρθρο 20
Αξιολόγηση του Δ.Δ.Π.Μ.Σ.

Στο τέλος κάθε εξαμήνου πραγματοποιείται αξιολόγηση κάθε μαθήματος και κάθε διδάσκοντος/ουσας από τους μεταπτυχιακούς φοιτητές. Η αξιολόγηση γίνεται με τη χρήση ειδικού εντύπου/ερωτηματολογίου αξιολόγησης που συμπληρώνουν οι μεταπτυχιακοί φοιτητές. Τα μαθήματα αξιολογούνται ως προς το περιεχόμενο, τον τρόπο διδασκαλίας, το εκπαιδευτικό υλικό και το βαθμό συσχέτισής τους με τις αρχές και τη φιλοσοφία του μεταπτυχιακού προγράμματος. Οι διδάσκοντες/ουσες αξιολογούνται σε πολλά επίπεδα, τα οποία μπορεί ενδεικτικά να περιλαμβάνουν αξιολόγηση ως προς τις γνώσεις και την ικανότητα μετάδοσής τους στους φοιτητές, την προετοιμασία τους, τη χρήση σύγχρονης βιβλιογραφίας, την προθυμία τους να απαντούν σε ερωτήσεις, την έγκαιρη βαθμολόγηση και επιστροφή εργασιών και γραπτών εξετάσεων και την τήρηση των ωρών διδασκαλίας του μαθήματος.

Η ετήσια εσωτερική αξιολόγηση του Δ.Δ.Π.Μ.Σ. γίνεται σε συνεργασία με τη ΜΟ.ΔΙ.Π. του Πανεπιστημίου Δυτικής Αττικής στο πλαίσιο της εσωτερικής αξιολόγησης του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών και σύμφωνα με την αντίστοιχη διεργασία του εσωτερικού Συστήματος Διασφάλισης Ποιότητας του Πα.Δ.Α.

Η εξωτερική αξιολόγηση του Δ.Δ.Π.Μ.Σ. διενεργείται σε συνεργασία με την ΜΟ.ΔΙ.Π. στο πλαίσιο της πιστοποίησής τους σύμφωνα με την προβλεπόμενη από την ΕΘΑΑΕ διαδικασία.

Στο πλαίσιο αυτό αξιολογείται η συνολική αποτίμηση του έργου που επιτελέστηκε από το Δ.Δ.Π.Μ.Σ., ο βαθμός εκπλήρωσης των στόχων που είχαν τεθεί κατά την ίδρυσή του, η βιωσιμότητά του, η απορρόφηση των αποφοίτων στην αγορά εργασίας, ο βαθμός συμβολής του στην έρευνα, η εσωτερική αξιολόγησή του από τους μεταπτυχιακούς φοιτητές, η σκοπιμότητα παράτασης της λειτουργίας του, καθώς και λοιπά στοιχεία σχετικά με την ποιότητα του έργου που παράγεται και τη συμβολή του στην εθνική στρατηγική για την ανώτατη εκπαίδευση.

Άρθρο 21
Ιστοσελίδα του Π.Μ.Σ

Το Δ.Δ.Π.Μ.Σ. έχει την επίσημη ιστοσελίδα του στη διεύθυνση cscyb.uniwa.gr, στην ελληνική και την αγγλική γλώσσα. Η ιστοσελίδα του Δ.Δ.Π.Μ.Σ. περιέχει όλες τις πληροφορίες και ανακοινώσεις του προγράμματος και αποτελεί τον επίσημο χώρο ενημέρωσης των φοιτητών και φοιτητριών.

Άρθρο 22
Λοιπές Διατάξεις

Οποιοδήποτε θέμα προκύψει στο μέλλον που δεν καλύπτεται από τη σχετική νομοθεσία ή τον παρόντα Κανονισμό, θα αντιμετωπιστεί με αποφάσεις των αρμοδίων οργάνων και όπου απαιτείται με τροποποίηση του Κανονισμού.

ΠΑΡΑΡΤΗΜΑ

Αναλυτική περιγραφή των μαθημάτων (ΕΛΛΗΝΙΚΑ)

1. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ (7)		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**CSCYB101**	**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*	**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 (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

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*

Γνώσεις

Στο πλαίσιο του μαθήματος, οι φοιτητές και οι φοιτήτριες θα μπορούν:

- 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	*Σχεδιασμός και διαχείριση έργων*
Προσαρμογή σε νέες καταστάσεις	*Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα*
	Σεβασμός στο φυσικό περιβάλλον

Λήψη αποφάσεων	*Επίδειξη κοινωνικής, επαγγελματικής και ηθικής*
Αυτόνομη εργασία	*υπευθυνότητας και ευαισθησίας σε θέματα φύλου*
Ομαδική εργασία	*Άσκηση κριτικής και αυτοκριτικής*
Εργασία σε διεθνές περιβάλλον	*Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής*
Εργασία σε διεπιστημονικό περιβάλλον	*σκέψης*
Παράγωγή νέων ερευνητικών ιδεών	*……*
	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

Θεωρητικό Μέρος Μαθήματος

Διάλεξη 1

Εισαγωγή σε θέματα Ασφάλειας (security) πληροφοριακών και επικοινωνιακών συστημάτων. Ορολογία και ISO 27000:2018.

Διαλέξη 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).

Διάλεξη 3

Σύστημα Διοίκησης για την Ασφάλεια Πληροφοριών (Information Security Management System ISMS) και ISO 27001:2022.

Διάλεξη 4

Αντίμετρα (controls) και ISO 27002:2022.

Διάλεξη 5

Οδηγίες υλοποίησης ISMS και ISO 27003:2017.

Διάλεξη 6

Καλές πρακτικές για υλοποίηση αντιμέτρων στο Νέφος (cloud) και ISO 27017: 2015.

Διάλεξη 7

Καθοδήγηση για τη Διοίκηση Επικινδυνότητας της Ασφάλειας των Πληροφοριών (information security risk management) και ISO 27005:2022.

Διάλεξη 8

Οδηγίες διοίκησης για την ασφάλεια πληροφοριών στην Κυβερνοασφάλιση (cyberinsurance) και ISO 27102:2019.

Διάλεξη 9

Ετοιμότητα τεχνολογιών πληροφορικής και επικοινωνιών (ICT readiness) και ISO 27031:2011 για την επιχειρησιακή συνέχεια (business continuity).

Διάλεξη 10

Νομοθετικό και κανονιστικό πλαίσιο για την προστασία προσωπικών δεδομένων: General Data Protection Regulation και ISO 29100:2017.

Διάλεξη 11

Οδηγία e-Privacy 2002/58. Οδηγία περί διατήρησης δεδομένων (data retention) 2006/24.

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.

Εργαστηριακό Μέρος Μαθήματος

Διάλεξη 13 Μελέτες περίπτωσης σε θέματα Enterprise Risk Management, Personal Data Protection, Electronic Communication Security

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

<table>
<tr><td>ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ
Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.</td><td>Πρόσωπο με πρόσωπο</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 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</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 σύμφωνα με τις αρχές του ECTS</td><td>
<table>
<tr><th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr>
<tr><td>Διαλέξεις</td><td>39</td></tr>
<tr><td>Ασκήσεις πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών, καθώς και ανάλυση μελετών</td><td>51</td></tr>
<tr><td>Εκπόνηση εργασίας</td><td>50</td></tr>
<tr><td>Αυτοτελής μελέτη</td><td>60</td></tr>
<tr><td>Σύνολο Μαθήματος (25 ώρες ανά πιστωτική μονάδα)</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>Γραπτή τελική εξέταση (100%) ή 2 Εξετάσεις Προόδου (30%+30%) και Τελική Εξέταση (40%) που περιλαμβάνουν επίλυση προβλημάτων της ύλης

Κάθε άσκηση/πρόβλημα των εξετάσεων έχει διαφορετική βαθμολογία, η οποία ανακοινώνεται στους φοιτητές κατά την εξέταση</td></tr>
</table>

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

Προτεινόμενη Βιβλιογραφία

ΑΓΓΛΙΚΗ

- *Security Engineering A Guide to Building Dependable Distributed Systems, R. Anderson, J. Wiley & Sons, 3rd edition, 2020*
- *The Cyber Security Handbook, A. Calder, ITGP, 2020*
- *Cybersecurity, E. Lewis, 2020*
- *The Age of Surveillance Capitalism, S. Zuboff, Profile Books, 2019*
- *Computer Security, D. Gollmann, J. Wiley & Sons, 3rd edition, 2018*

ΕΛΛΗΝΙΚΗ

- *Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο, Σ. Κάτσικας, Σ. Γκρίτζαλης, Κ. Λαμπρινουδάκης (Επισ. Επιμέλεια), Εκδόσεις Νέων Τεχνολογιών, 2021*
- *Διαχείριση της Ασφάλειας Πληροφοριών, Σ. Κάτσικας, Εκδόσεις Πεδίο, 2014*
- *Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας (Επισ. Επιμέλεια), Εκδόσεις Παπασωτηρίου, 2010*

Συναφή επιστημονικά περιοδικά:

- 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

2. 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*		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**

το σύνολο του μαθήματος αναγράψτε τις εβδομαδιαίες ώρες διδασκαλίας και το σύνολο των πιστωτικών μονάδων		
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 εργαστηρίου υπολογιστών και ασκήσεων.
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*	

Δραστηριότητα	*Φόρτος Εργασίας Εξαμήνου*
Lectures	39
Ασκήσεις Πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών και ανάλυση μελετών	30

(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*	<table><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>
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. Εργασία 1 (50%) και II. Εργασία 2 (50%)

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.

3. Τεχνολογίες Αλυσίδας Συστοιχιών & Κατανεμημένου Καθολικού

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB105	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**1ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Τεχνολογίες Αλυσίδας Συστοιχιών & Κατανεμημένου Καθολικού		

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**	**4**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Ανάπτυξης Δεξιοτήτων, Υποβάθρου*
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	Cscyb.uniwa.gr and eclass (https://eclass.uniwa.gr/courses/CSCYB103/)

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*

Στο μάθημα Τεχνολογίες Αλυσίδας Συστοιχιών & Κατανεμημένου Καθολικού, οι μαθητές θα γνωρίσουν την τεχνολογία του Blockchain και τα χαρακτηριστικά της χωρίς κάποιο προ-απαιτούμενο.

Με την ολοκλήρωση του μαθήματος, οι φοιτητές θα είναι σε θέση:

- Να επιχειρηματολογούν σχετικά με την χρήση (ή όχι) μιας λύσης που βασίζεται στην τεχνολογία Blockchain σε μια δεδομένη περίπτωση χρήσης.
- Να σχεδιάζουν μια λύση που βασίζεται στην τεχνολογία blockchain
- Να κατανοούν πώς η χρήση κρυπτογραφίας και ψηφιακών υπογραφών μπορεί να βελτιώσει την ακεραιότητα και την ασφάλεια των δεδομένων
- Να δημιουργούν ένα πορτοφόλι και να το χρησιμοποιούν για συναλλαγές
- Να συνδέονται και να συναλλάσσονται στα πιο δημοφιλή δίκτυα Blockchain (Ethereum, Bitcoin).
- Να δημιουργούν και να εγκαθιστούν ένα Smart Contract
- Να δημιουργούν ένα NFT

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	

Προσαρμογή σε νέες καταστάσεις
Λήψη αποφάσεων
Αυτόνομη εργασία
Ομαδική εργασία
Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Θεωρητικό Μέρος Μαθήματος:

Το μάθημα χωρίζεται σε 8 ενότητες:

Ενότητα 1: Εισαγωγή στην τεχνολογία Blockchain

Στην Ενότητα αυτή παρουσιάζονται τα βασικά χαρακτηριστικά της τεχνολογίας blockchain και αναλύονται τα προτερήματα και τα μειονεκτήματα της. Επιπλέον, αναλύονται τα είδη των blockchain που υπάρχουν και μελετάται πως μπορεί κάποιος να βρει αν μια λύση blockchain ενδείκνυται σε μια περίπτωση χρήσης και αν ναι ποιος τύπος ταιριάζει καλύτερα.

Ενότητα 2: Δημοφιλείς πλατφόρμες Blockchain

Στην Ενότητα αυτή αναλύονται τα δυο πιο δημοφιλή δίκτυα blockchain, αυτό του Bitcoin και του Ethereum. Εξετάζονται τα βασικά χαρακτηριστικά λειτουργίας τους και σημειώνονται οι ομοιότητες και οι διαφορές τους.

Ενότητα 3: Κλειδιά και Διευθύνσεις

Στην Ενότητα αυτή γίνεται αναλυτική παρουσίαση στον ρόλο της ασύμμετρης κρυπτογραφίας για τη δημιουργία του ζεύγους ιδιωτικού και δημόσιου κλειδιού. Επίσης, αναλύεται πως από το ζεύγος αυτό αποκτάται η διεύθυνση του χρήστη στο Bitcoin δίκτυο και στο Ethereum.

Ενότητα 4: Ψηφιακές Υπογραφές και Πορτοφόλια
Στην Ενότητα αυτή παρουσιάζεται ο τρόπος που δημιουργούνται, με χρήση κρυπτογράφησης ,οι ψηφιακές υπογραφές και εξηγείται ο ρόλος που παίζουν αυτές σε ένα δίκτυο Blockchain. Επιπλέον, αναλύεται ο ρόλος που παίζουν τα πορτοφόλια σε ένα δίκτυο blockchain και μελετώνται οι διαφορετικοί τύποι πορτοφολιών που υπάρχουν.
Ενότητα 5: Συναλλαγές
Στην Ενότητα αυτή εξηγείται ο τρόπος που γίνονται οι συναλλαγές στα δίκτυα του Bitcoin και του Ethereum. Εξηγείται η βασική διαφορά τους και παρουσιάζονται παραδείγματα για την κατανόηση.
Ενότητα 6: Έξυπνες Συμβάσεις (Smart Contracts) και Non-Fungible Tokens (NFTs)
Στην Ενότητα αυτή θα γίνει μια παρουσίαση των έξυπνων συμβάσεων στο δίκτυο του Ethereum. Θα εξηγηθεί ο τρόπος που συντάσσονται και ο ρόλος του gas στην εκτέλεση τους. Επίσης, θα συνταχθεί ένα Smart Contract και θα εγκατασταθεί σε ένα πραγματικό δοκιμαστικό δίκτυο. Επιπλέον, θα παρουσιαστούν τα πρότυπα ERC πάνω στα οποία βασίζονται τα NFTs και τα tokens και θα δοθούν παραδείγματα για το πως μπορεί να δημιουργηθούν NFTs που βασίζονται στο πρότυπο ERC721.
Ενότητα 7: Αποκεντρωμένες Εφαρμογές και Εισαγωγή στο Web 3.0
Στην Ενότητα αυτή θα γίνει μια παρουσίαση του Web3.0 και θα εξηγηθούν οι διαφορές του με το Web 2.0. Κατόπιν, θα εξηγηθεί πως μπορεί να δημιουργηθεί μια αποκεντρωμένη εφαρμογή (Decentralized Application) και πώς συνδέεται με ένα δίκτυο blockchain και τα απαραίτητα Smart Contracts.
Ενότητα 8: Περιπτώσεις Χρήσης
Στην Ενότητα αυτή παρουσιάζονται πολλές περιπτώσεις χρήσης στις οποίες η χρήση της τεχνολογίας του blockchain μπορεί να έχει πολύ καλά αποτελέσματα και να βελτιώσει την απόδοση των σύγχρονων λύσεων. Επιπλέον, αναλύεται τόσο ο λόγος που η τεχνολογία του blockchain μπορεί να βοηθήσει όπως και ποιο είδος λύσης προτείνεται να χρησιμοποιηθεί σε κάθε περίπτωση.

Εργαστηριακό Μέρος Μαθήματος
Το εργαστηριακό μέρος του μαθήματος ακολουθεί το θεωρητικό. Σε αυτό χρησιμοποιούνται εργαλεία όπως το ETH.Build το οποίο προτείνεται από το Ethereum Foundation για την εκπαίδευση του κόσμου στην τεχνολογία του Blockchain. Στο εργαλείο αυτό δίνονται ασκήσεις σχετικές με:

- Την Κρυπτογραφία
- Τις Ψηφιακές Υπογραφές
- Τις Συναλλαγές

Επιπλέον, χρησιμοποιείται το εργαλείο του Remix για την συγγραφή των Smart Contracts αλλά και την εγκατάσταση τους σε ένα πραγματικό Δοκιμαστικό Δίκτυο του Ethereum. Για τον λόγο αυτό, θα γίνει λογαριασμός σε ένα πορτοφόλι (π.χ., Metamask). Το πορτοφόλι θα χρησιμοποιηθεί και για την αποστολή NFTs μεταξύ των φοιτητών/τριων.

4. 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: 21 Εκπόνηση εργασίας: *20* Αυτοτελής Μελέτη: 20 **Total Course Load** (25 hours per credit): **100**
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.*	Θα ανατεθεί μία τελική εργασία και ο βαθμός θα εξαρτηθεί: - Επί της παραδοθείσας γραπτής εργασίας (40%) - Στην προφορική παρουσίαση της εργασίας (60%) Κάθε άσκηση/πρόβλημα της εργασίας έχει διαφορετική βαθμολογία η οποία αναγράφεται στην εκφώνηση

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

ΑΓΓΛΙΚΗ

1. *A. Antonopoulos, “Mastering Bitcoin”, O’Reilly, 2nd edition, 2017.*
2. *A. Antonopoulods, G. Wood, “Mastering Ethereum: Building Smart Contracts and DApps”, O’Relly, 1st Edition, 2018.*

ΕΛΛΗΝΙΚΗ

Πατρικάκης, Χ., Λελίγκου, Ε., & Κόγιας, Δ. (2023). *Αλυσίδες Συστοιχιών (Blockchain)* [Μεταπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. https://dx.doi.org/10.57713/kallipos-171

Ηλεκτρονικές Διευθύνσεις

https://bitcoin.org/bitcoin.pd f

4. Κανόνες και Πρωτόκολλα Κυβερνοασφάλειας

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...		

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*

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.

3. 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 ΤΝ
6) FIPS
7) Διακυβέρνηση, κίνδυνος και συμμόρφωση (ERNEST YOUNG) και αξιόπιστη ασφάλεια υπολογιστών
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

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

5. 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*

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

5. ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧ/ΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ	**CSCYB104**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	1ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ**		

ΚΑΤΑΝΟΜΗ ΜΑΘΗΜΑΤΩΝ	**Εβδομαδιαίες Ώρες Διδασκαλίας**	**ECTS Μονάδες**
Μαθήματα	2	
Ασκήσεις	1	
	3	**3**

ΤΥΠΟΣ ΕΝΟΤΗΤΑΣ ΜΑΘΗΜΑΤΟΣ	Υποχρεωτικές, Εξειδικευμένες και Γενικές γνώσεις
ΓΙΑ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ
ΙΣΤΟΣΕΛΙΔΑ	http://

2 ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ
Το μάθημα στοχεύει στην εκπαίδευση των φοιτητών στον τομέα της ασφάλειας συστημάτων πληροφοριών και επικοινωνιών, καθώς και στις τεχνολογίες προστασίας της ιδιωτικής ζωής. Συνολικά, το μάθημα έχει προγραμματιστεί λαμβάνοντας υπόψη τα ακόλουθα σημεία: Με την επιτυχή ολοκλήρωση αυτού του μαθήματος, ο φοιτητής θα είναι σε θέση: • την εμβάθυνση και εμπέδωση υψηλού επιπέδου γνώσεων στο εύρος του τομέα της Ασφάλειας Πληροφοριών. • Απόκτηση εξειδικευμένων δεξιοτήτων στην επίλυση προβλημάτων Συστημάτων Ασφάλειας Πληροφοριών με στόχο την απόκτηση βάσης για σχεδιασμό έρευνας και καινοτομίας στον τομέα της Ασφάλειας. Ειδικότερα ο φοιτητής θα είναι οικείος με την: • Κατανόηση της δομής και λειτουργίας των Συστημάτων Ασφάλειας Πληροφοριών (στο Διαδίκτυο). • Άριστη γνώση των επιπέδων δικτύου, IPv4, ICMP, ARP, Sniffing, MAC Spoofing, .
• Ασφάλεια των εφαρμογών Διαδικτύου, των αρχιτεκτονικών δικτύων, της σηματοδότησης και των πρωτοκόλλων επικοινωνίας. • Αξιολόγηση των κριτηρίων της Cryptology • Επιλογή των κατάλληλων ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών. • Ανάλυση και τη σύγκριση των σύγχρονων κρυπτογραφικών αλγορίθμων • Δημιουργία και σχεδίαση των Συστημάτων Διαχείρισης Ασφαλείας • Μάθηση του Νομικού πλαισίου του Διαδικτύου Ιδιωτικότητας και του Κυβερνοεγκλήματος
Γενικές Δεξιότητες
• Ανάκτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση των απαραίτητων τεχνολογιών • Ομαδική Εργασία • Προώθηση της ελεύθερης, δημιουργικής και αιτιολογικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

Η περιγραφή περιέχει το υλικό που θα καλυφθεί κατά τη διάρκεια 13 συνεδριών.

1. Βασικές έννοιες και ζητήματα ασφάλειας
2. Δίκτυα και Διαδίκτυο
3. Ασφαλής σύνδεση διεπαφής
4. Προγραμματισμός Διαδικτύου
5. Ασφάλεια Εφαρμογών Διαδικτύου
6. Εισαγωγή στην Κρυπτολογία
7. Σύγχρονοι Κρυπτογραφικοί Αλγόριθμοι
8. Ακεραιότητα και αυθεντικότητα μηνύματος
9. Ψηφιακές Υπογραφές και Ψηφιακά Πιστοποιητικά
10. Εικονικά Ιδιωτικά Δίκτυα
11. Διαχείριση Ασφαλείας
12. Απάντηση σε συμβάντα ασφαλείας & ψηφιακή εγκληματολογία
13. Ιδιωτικό απόρρητο στο Διαδίκτυο και Έγκλημα στον κυβερνοχώρο

4. ΜΕΘΟΔΟΙ ΔΙΔΑΣΚΑΛΙΑΣ - ΕΞΕΤΑΣΗ

ΤΡΌΠΟΣ ΜΑΘΗΜΑΤΟΣ	Δια ζώσης
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	• Χρήση ΤΠΕ στη Διδασκαλία Μαθημάτων • Χρήση του συστήματος Open eClass, με ανεβασμένες σημειώσεις, διαλέξεις, ασκήσεις για εξάσκηση και επικοινωνία με μαθητές.
ΜΕΘΟΔΟΙ ΔΙΔΑΣΚΑΛΙΑΣ	
Εξέταση	I. Γραπτή τελική εξέταση (60%) και II. Ερευνητική εργασία (40%)

Περιγραφή Μεθόδου	***Φόρτος Εξαμήνου***
Διαλέξεις	26
Ασκήσεις	13
Ερευνητική Εργασία	15
Μελέτη	30
Συνολικές ώρες μαθημάτων (φόρτος εργασίας 25 ωρών ανά ECTS)	***75***

5. ΒΙΒΛΙΟΓΡΑΦΊΑ

Προτεινόμενη

- *Κρυπτογραφία & Ασφάλεια Δικτύων Αρχές& Εφαρμογές, William Stallings, Εκδόσεις ΙΩΝ.*
- *Κάτσικα Σ, Γκρίτζαλη Δ., Γκρίτζαλη Σ. Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέες Τεχνολογίες.*
- *Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Δικτύων Υπολογιστών, Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ ΟΕ, 2003.*
- *Business Information Systems: Technology, Development and Management for the Modern Business, Paul Bocij, Andrew Greasley, Simon Hickie, Sixth edition, Pearson 2018*

Επιπλέον

- *Cybersecurity, Mowbray Thomas J.,* Third edition, *John Wiley & Sons In*
- *Anderson R., Security Engineering, Wiley (2nd ed.), USA, 2008.*
- *Gollmann D., Computer Security, 3rd edition, Wiley, March 2011.*
- *Pfleeger C., Security in Computing, Prentice Hall (4th ed.), USA, 2006.*
- *Rhodes-Ousley M. Information security: The complete reference. McGraw-Hill Education. Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., Ασφάλεια της Πληροφορίας, Εκδόσεις Νέες Τεχνολογίες, 2004*

6. Ασφάλεια Δικτύων

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB206	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**2ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**Ασφάλεια Δικτύων**		
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	**7**
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Ανάπτυξης Δεξιοτήτων*		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	Cscyb.uniwa.gr Και 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*
Η Ασφάλεια Δικτύων είναι ένα βασικό μάθημα σε ένα πρόγραμμα Μεταπτυχιακών Σπουδών στο Cybersecurity που ενισχύει τις γνώσεις των φοιτητών σχετικά με την ασφάλεια σε πολλούς διαφορετικούς τύπους δικτύων υπολογιστών. Σκοπός του μαθήματος είναι να εμβαθύνει τις θεωρητικές και πρακτικές δεξιότητες που έχουν ήδη οι φοιτητές στα δίκτυα υπολογιστών και στον τομέα της ασφάλειας υπολογιστών και να καλύψει τα απαιτούμενα συμπληρωματικά θέματα στο πλαίσιο της κυβερνοασφάλειας. Αυτό θα τους προσφέρει πρόσθετη τεχνογνωσία και δεξιότητες υψηλού επιπέδου για την αγορά εργασίας και της έρευνας για να συνεχίσουν τις σπουδές τους στο επόμενο επίπεδο.

Με το τέλος αυτού του μαθήματος, ο φοιτητής θα φτάσει σε επαγγελματικό επίπεδο στην ασφάλεια δικτύων όσον αφορά τις ορολογίες, τις κύριες έννοιες, τις νέες τεχνολογίες και τα πλέον δημοφιλή εργαλεία.
Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής θα είναι σε θέση να:

- να αναγνωρίζει τους παράγοντες που οδηγούν στην ανάγκη για ασφάλεια δικτύων και επικοινωνιών.
- να αναγνωρίζει και να κατηγοριοποιεί συγκεκριμένα παραδείγματα επιθέσεων σε δίκτυα.
- να προσδιορίσει ευπαθή σημεία στις επικοινωνίες και τα δίκτυα.
- να σχεδιάζει και υλοποιεί ασφαλή συστήματα και εφαρμογές δικτύων.
- να διακρίνει τα πλεονεκτήματα και τα μειονεκτήματα εναλλακτικών αρχιτεκτονικών ασφαλών δικτύων και επικοινωνιών.
- να διακρίνει και να συγκρίνει συμμετρικά και ασύμμετρα κρυπτοσυστήματα και να γνωρίζει τα χαρακτηριστικά υβριδικών συστημάτων.
- να γνωρίζει τα εργαλεία και τις τεχνικές για τον εντοπισμό των κενών ασφάλειας των δικτυακών συσκευών και των εφαρμογών και να διακρίνει τα προβλήματα και τα σφάλματα που οφείλονται στην ανεπαρκή εφαρμογή μηχανισμών ασφάλειας των συσκευών και στην ανεπαρκή προστασία της πληροφορίας που μεταδίδεται μέσω των διαδικτυακών εφαρμογών.
- να εφαρμόζει τις γνώσεις του για να προστατεύει τις συσκευές και την μεταδιδόμενη δικτυακά πληροφορία από κακόβουλες ενέργειες υποκλοπής, τροποποίησης, καταστροφής και πλαστογράφησης της πληροφορίας.
- να αξιολογεί την ασφαλή λειτουργία των δικτύων, να εντοπίζει τυχόν κενά ασφάλειας στην πρόσβαση και στη μετάδοση της πληροφορίας, ειδικά σε απομακρυσμένους χρήστες.
- να αντιμετωπίσει τις εξελίξεις στον τομέα της ασφάλειας δικτύων και επικοινωνιών, θέματα στα οποία θα έχει εμβαθύνει τις γνώσεις.
- θα έχει την ικανότητα να καθοδηγεί τις αλλαγές που επιφέρουν οι εξελίξεις στην τεχνολογία στον τομέα αυτό.
- θα έχει την ικανότητα να αξιολογεί και να διακρίνει ασφαλή και μη ασφαλή συστήματα δικτύων και επικοινωνίες μεταξύ των μερών τους.
- θα έχει την ικανότητα να εφαρμόζει μεθοδολογικά την αποκτηθείσα γνώση για την κατανόηση και επίλυση πρακτικών προβλημάτων.
- θα έχει την ικανότητα να χρησιμοποιεί σύγχρονες μεθόδους για την προστασία δικτυακών συστημάτων και συστημάτων επικοινωνιών.

θα έχει την ικανότητα να συνεργάζεται με άλλους για την επίλυση πραγματικών προβλημάτων.

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

Εργασία σε διεπιστημονικό περιβάλλον
Παραγωγή νέων ερευνητικών ιδεών
Αναζήτηση, ανάλυση και σύνθεση δεδομένων
Προσαρμογή σε νέες καταστάσεις
Λήψη αποφάσεων

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το μάθημα οργανώνεται ως εξής: Διάλεξη 1: Εισαγωγή στην Ασφάλεια Δικτύων Διάλεξη 2: Κρυπτογράφηση Διάλεξη 3: Συστήματα Ανίχνευσης Εισβολών Διάλεξη 4: Vehicular Ad-hoc Δίκτυα Διάλεξη 5: WEKA Διάλεξη 6: Επιθέσεις TCP Διάλεξη 7: Απόρρητο Διάλεξη 8: Αποφυγή τείχους προστασίας με χρήση VPN Διάλεξη 9: SNORT Διάλεξη 10: Προχωρημένα Θέματα Ανίχνευσης Εισβολών Διάλεξη 11: Ασφάλεια και Ιδιωτικότητα στο Blockchain Διάλεξη 12: Έμπιστες Αλυσίδες Εφοδιασμού Διάλεξη 13: Παρουσίαση Τελικών εργασιών και δημόσια συζήτηση επ’ αυτών

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	In class face to face
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*	

Περιγραφή Μεθόδου	***Φόρτος Εξαμήνου***
Διαλέξεις	39
Ασκήσεις Πράξης που εστιάζουν στην εφαρμογή μεθοδολογιών και ανάλυση μελετών	26
Ερευνητική Εργασία	60
Μελέτη	50
Συνολικές ώρες μαθημάτων (φόρτος εργασίας 25 ωρών ανά ECTS)	***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.*	Παρουσίαση και εξέταση Τελικής Εργασίας (100%).

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία :

1. W.Stallings, Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, Εκδότης Παρίκου ΕΠΕ, 2011 (Κωδ. Εύδοξος: 12777632)
2. J.F. Kurose, K.W. Ross, “Δικτύωση Υπολογιστών, Προσέγγιση από πάνω προς τα κάτω, 6η Έκδοση 2013”, Εκδόσεις: Γκιούρδα & ΣΙΑ, (Κωδ. Εύδοξος: 33094885)
3. B. Forouzan, Cryptography and Network Security, McGraw Hill, Εκδόσεις Επίκεντρο Α.Ε, 2008 (Κωδ. Εύδοξος: 12562157)
4. J.F. Kizza, “Guide to Computer Network Security”, Springer, 2017
5. L. Ertaul, L.H. Encinas and E. El-Sheikh “Computer and Network Security Essentials”, Springer, 2017
6. X. He and H. Dai, “Dynamic Games for Network Security”, Springer, 2018
7. E. Maiwald, “Network Security”, Mc Graw Hill, 2013

7. Εφαρμοσμένη Κρυπτογραφία

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**CSCYB103**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	1ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΕΦΑΡΜΟΣΜΕΝΗ ΚΡΥΠΤΟΓΡΑΦΙΑ**		

ΚΑΤΑΝΟΜΗ ΜΑΘΗΜΑΤΩΝ	**Εβδομαδιαίες Ώρες Διδασκαλίας**	**ECTS Μονάδες**
Διαλέξεις	3	
Άσκηση Πράξης	2	
	5	**8**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Επιστημονικής Περιοχής,*
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uniwa.gr/courses/CSCYB105/YES

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ
• - Εισαγωγή στους ορισμούς και τις έννοιες της κρυπτογραφίας • - Εξοικείωση με θέματα ασφάλειας • - Κατανόηση των δυνατοτήτων των κρυπτογραφικών πρωτοκόλλων • - Οι δεξιότητες επιλογής των καταλληλότερων κρυπτογραφικών λύσεων για δεδομένο πρόβλημα ασφάλειας.
ΔΕΞΙΟΤΗΤΕΣ
• *- Αναζήτηση βέλτιστων κρυπτογραφικών λύσεων* • *- Ανεξάρτητη εργασία*

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Η περιγραφή περιέχει την ύλη που θα καλυφθεί κατά τη διάρκεια 13 διαλέξεων.
1) Εισαγωγή στην κρυπτογραφία. Ιστορία της κρυπτογραφίας και ορισμοί
2) Μαθηματικό υπόβαθρο. Modular computations, συναρτήσεις Boole, παράδοξο γενεθλίων
3) Ψευδοτυχαίες γεννήτριες και κρυπτογράφηση ροής
4) Ψευδοτυχαίες συναρτήσεις. Κωδικοποιητές μπλοκ (AES) και τρόποι λειτουργίας (CBC,CTR).
5) Μονόδρομες συναρτήσεις και συναρτήσεις κατακερματισμού (SHA-2, SHA-3).
6) Κώδικες ελέγχου ταυτότητας μηνυμάτων. HMAC και ECBC.
7) Αυθεντική κρυπτογράφηση με τα σχετικά δεδομένα (GCM).
8) Κρυπτογραφία δημόσιου κλειδιού. RSA και ασφαλείς υλοποιήσεις. Το πρόβλημα της παραγοντοποίησης
9) El Gamal και ελλειπτικές καμπύλες. Το πρόβλημα του διακριτού λογαρίθμου.
10) Ψηφιακές υπογραφές. Αλγόριθμος ψηφιακής υπογραφής, EdDSA.
11)Επιθέσεις κατά πρωτοκόλλων κρυπτογράφησης συμμετρικού και δημόσιου κλειδιού
12) Μηχανισμός ενθυλάκωσης κλειδιών, κρυπτογράφηση κλειδιών, συμφωνία κλειδιών Diffie-Hellman και πρωτόκολλα αυθεντικοποίησης
13)Προηγμένη κρυπτογραφία: MPC, ORAM, ομομορφική κρυπτογράφηση

4. ΜΕΘΟΔΟΙ ΔΙΔΑΣΚΑΛΙΑΣ -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*	• - Χρήση των ΤΠΕ στη διδασκαλία μαθημάτων • - Χρήση του συστήματος Open e-Class, με αναρτημένες σημειώσεις, διαλέξεις, ασκήσεις για εξάσκηση και επικοινωνία με τους φοιτητές.
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*	

Περιγραφή Μεθόδου	***Φόρτος Εξαμήνου***
Διαλέξεις	39
Άσκηση Πράξης	26
Ερευνητική εργασία	60
Μελέτη	75
Σύνολο	***200***

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	I. Γραπτή τελική εξέταση (60%) και II. Ερευνητική εργασία (40%)
Περιγραφή της διαδικασίας αξιολόγησης	

5. ΠΗΓΕΣ

Essential

- *Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell (2nd Edition!)*
- *Cryptography Made Simple. Nigel Smart. Springer*

Recommended

- *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*
- *ENISA, Algorithms, key size and parameters, report – 2014*
- *ECRYPT – CSA, Algorithms, Key Size and Protocols Report (2018)*

8. ΑΣΦΑΛΕΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ και ΛΟΓΙΣΜΙΚΟΥ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	**ΜΗΧΑΝΙΚΩΝ**		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΜΕΤΑΠΤΥΧΙΑΚΟ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	**CSCYB205**	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	2ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ και ΛΟΓΙΣΜΙΚΟΥ**		

ΚΑΤΑΝΟΜΗ ΜΑΘΗΜΑΤΩΝ	**Εβδομαδιαίες Ώρες Διδασκαλίας**	**ECTS Μονάδες**
Διαλέξεις	3	
Άσκηση Πράξης	1	
	4	**7**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *Υποβάθρου , Γενικών Γνώσεων, Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων*	*Επιστημονικής Περιοχής,*
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	

6. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ
• - Να κατανοήσετε τους κινδύνους που υπάρχουν στη δημοσίευση δεδομένων • - Να γνωρίζει τις υπάρχουσες επιλογές για ασφαλείς βάσεις δεδομένων • - Να σχεδιάσει ασφαλέστερες βάσεις δεδομένων • - Να είναι σε θέση να προστατεύει τα δεδομένα του πελάτη από επιθέσεις
ΔΕΞΙΟΤΗΤΕΣ
• - Να κατανοήσουν την κύρια έννοια των μεγάλων δεδομένων και τις τάσεις και τους κινδύνους ασφαλείας των σύγχρονων εφαρμογών • - Να γνωρίζει ποια δεδομένα πρέπει να προστατεύονται- Κατανόηση των δυνατοτήτων των κρυπτογραφικών πρωτοκόλλων • - Οι δεξιότητες επιλογής των καταλληλότερων κρυπτογραφικών λύσεων για δεδομένο πρόβλημα ασφάλειας

7. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Η περιγραφή περιέχει την ύλη που θα καλυφθεί κατά τη διάρκεια 13 διαλέξεων. Με την παρακάτω θεματογραφία
- Διακριτικός και υποχρεωτικός έλεγχος πρόσβασης
- Δυνατότητες προστασίας της ασφάλειας της γλώσσας SQL
- Προστασία απορρήτου για σχεσιακά, χωρικά και γραφικά δεδομένα
- Προστασία της ιδιωτικότητας των δεδομένων που μεταβάλλονται με την πάροδο του χρόνου
- Ψηφιακό υδατογράφημα και δακτυλικό αποτύπωμα σε σχεσιακές βάσεις δεδομένων.
- Κρυπτογραφημένες βάσεις δεδομένων και ανάκτηση κρυπτογραφημένων δεδομένων
- Ασφάλεια σε στατιστικές και κατανεμημένες βάσεις δεδομένων
- Ασφάλεια μεγάλων δεδομένων
- Ασφάλεια δεδομένων και προστασία της ιδιωτικής ζωής σε επιγραμμικά κοινωνικά δίκτυα.
- Ολοκλήρωση και ασφάλεια μεγάλων δεδομένων

8. ΜΕΘΟΔΟΙ ΔΙΔΑΣΚΑΛΙΑΣ -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*	• - Χρήση των ΤΠΕ στη διδασκαλία μαθημάτων • - Χρήση του συστήματος Open e-Class, με αναρτημένες σημειώσεις, διαλέξεις, ασκήσεις για εξάσκηση και επικοινωνία με τους φοιτητές.
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*	

Περιγραφή Μεθόδου	***Φόρτος Εξαμήνου***
Διαλέξεις	39
Άσκηση Πράξης	26
Ερευνητική εργασία	50
Μελέτη	60
Σύνολο	***175***

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ *Περιγραφή της διαδικασίας αξιολόγησης*	I. Γραπτή τελική εξέταση (20%) και II. Ερευνητική εργασία (80%)

9. ΠΗΓΕΣ

Essential

- *Privacy Preserving Data Publishing: An Overview, Synthesis Lectures on Data Management, 2010, Raymond Chi Wing Wong, Ada Wai Chee Fu*
- *Συστήματα Διαχείρισης Βάσεων Δεδομένων, 3η Έκδοση, Ramakrishnan Raghu, Gehrke Joahannes . (Κεφάλαιο 24)*
- *Θεμελιώδεις αρχές συστημάτων βάσεων δεδομένων, Elmasri Ramez, Navathe Shamkant B.B (Κεφάλαιο 17)*
- *Rakesh Agrawal and Jerry Kiernan. 2002. Watermarking relational databases. In Proceedings of the 28th international conference on Very Large Data Bases*

Recommended

- *Chen, Bee Chung & Kifer , Daniel & LeFevre, Kristen & Machanavajjhala , Ashwin. (2009). Privacy Preserving Data Publishing. Foundations and Trends in Databases.*
- *Fung, Benjamin & Wang, ke & Chen, Rui & Yu, Philip. (2010). Privacy Preserving Data Publishing: A Survey of Recent Developments. ACM Comput . Surv .. 42.*

Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, Raju Halder, Shantanu Pal and Agostino Cortesi

9. ΔΟΚΙΜΗ ΔΙΕΙΣΔΥΣΗΣ ΚΑΙ ΨΗΦΙΑΚΗ ΣΗΜΑΝΣΗ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΜΗΧΑΝΙΚΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ		
ΠΜΣ	ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	7		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	CSCYB204	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**Β’**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΔΟΚΙΜΉ ΔΙΕΊΣΔΥΣΗΣ ΚΑΙ ΨΗΦΙΑΚΗ ΣΗΜΑΝΣΗ**		

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	
Άσκηση 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, Ειδίκευσης*
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	ΚΑΝΕΝΑ
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά και Αγγλικά
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	UNIWA Open eClass | Digital Forensics and Penetratio...

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ
Πρώτο μέρος Στο πρώτο μέρος του μαθήματος διδάσκονται στους φοιτητές οι βασικές αρχές και πολλές από τις τακτικές, τις τεχνικές, τις διαδικασίες και τα εργαλεία που χρησιμοποιούνται από επαγγελματίες κατά την δοκιμή διείσδυσης σε windows συστήματα. Σκοπός του μαθήματος μεταξύ άλλων είναι να κατανοήσουν

την απειλή και τον τρόπο δράσης των επιτιθέμενων.

Οι φοιτητές θα μάθουν να εφαρμόζουν ολόκληρη τη διαδικασία δοκιμής διείσδυσης, συμπεριλαμβανομένου του σχεδιασμού, της συλλογής πληροφοριών από ανοικτές πηγές (OSINT – Open Source Intelligence), της αναγνώρισης συστημάτων, της σάρωσης, της αξιολόγησης ευπαθειών, της εκμετάλλευσης και της απόκτησης αρχικής πρόσβασης, τις ενέργειες και διαδικασίες μετά την αρχική πρόσβαση και της αναφοράς αποτελεσμάτων. Το μάθημα θα παρέχει τις βασικές τεχνικές πληροφορίες που σχετίζονται με καθεμία από τις μεθόδους που χρησιμοποιούνται από τους περισσότερους επαγγελματίες δοκιμής διείσδυσης.

Δεύτερο μέρος

Στο δεύτερο μέρος του μαθήματος οι φοιτητές θα διδαχθούν την διαδικασία διαχείρισης / αντιμετώπισης κυβερνοεπιθέσεων σε ένα windows δίκτυο και την διαδικασία ψηφιακής εγκληματολογικής έρευνας ή διαφορετικά ψηφιακή σήμανση.

Το μάθημα διαχείρισης κυβερνοεπιθέσεων και ψηφιακής σήμανσης σε Windows OS καλύπτει συνολικά τις έξι φάσεις που ακολουθούνται στην διαδικασία διαχείρισης κυβερνοεπιθέσεων, καθώς και την διαδικασία ψηφιακής εγκληματολογικής έρευνας ή διαφορετικά ψηφιακής σήμανσης που περιλαμβάνει την συλλογή και ανάλυση μνήμης των Windows, την συλλογή και ανάλυση της registry, την συλλογή και ανάλυση του συστήματος αρχείων και την ψηφιακή ανάλυση εφαρμογών. Στο τέλος του μαθήματος οι φοιτητές θα έχουν την δυνατότητα να πραγματοποιούν διαχείριση κυβερνοεπίθεσης και ψηφιακή σήμανση χρησιμοποιώντας μια ποικιλία από δωρεάν, ανοιχτού κώδικα και εμπορικά εργαλεία. Θα μάθουν να προσδιορίζουν και να χειρίζονται σωστά

Τα ψηφιακά αποδεικτικά στοιχεία και να απαντούν σε κρίσιμα ερωτήματα σχετικά με την υπόθεση της ψηφιακής εγκληματολογίας. Ερωτήματα όπως τυχόν εκτέλεση υπόπτων εφαρμογών, παράνομη πρόσβαση σε αρχεία, κλοπής δεδομένων, χρήση ύποπτης εξωτερικής συσκευής, μεταφόρτωση υπόπτων αρχείων κλπ. Στο τέλος θα μάθουν πως να συντάσσουν ολοκληρωμένη αναφορά όπου θα παρουσιάζουν με τεκμηριωμένο τρόπο τα ευρήματά τους.

Ο στόχος του μαθήματος είναι να διδάξει τους φοιτητές πώς να εκτελούν την διαδικασία διαχείρισης μιας κυβερνοεπίθεσης, ακολουθώντας ένα σχέδιο διαχείρισης καθώς και πως να εφαρμόζουν μια ολοκληρωμένη ψηφιακή εγκληματολογική έρευνα σε ένα Windows σύστημα.

Γενικές Δεξιότητες / Γνώσεις.

- Κατανόηση της κυβερνοαπειλής και του τρόπου δράσης των επιτιθέμενων στον κυβερνοχώρο.
- Κατανόηση των τακτικών, τεχνικών, διαδικασιών και των εργαλείων που εφαρμόζουν και χρησιμοποιούν οι ελεγκτές ασφαλείας (penetration testers) και οι κόκκινες ομάδες (Read Teams).
- Διεξαγωγή ολοκληρωμένης διαδικασίας δοκιμής διείσδυσης
- Πρακτική εφαρμογή της διαδικασίας διαχείρισης μιας κυβερνοεπίθεσης ακολουθώντας τις έξι φάσεις αντιμετώπισης.
- Πρακτική διεξαγωγή μιας ολοκληρωμένης ψηφιακής εγκληματολογικής έρευνας.

3. ΠΕΡΙΕΧΟΜΕΝΑ ΜΑΘΗΜΑΤΟΣ

Τα περιεχόμενα της κάθε μιας εκ των 13 διαλέξεων περιλαμβάνουν:

1. Εισαγωγή στη αξιολόγηση Δοκιμής Διείσδυσης και κόκκινης ομάδας (Penetration Testing and Red Teaming assessment)
   α. Τι είναι αξιολόγηση Δοκιμής Διείσδυσης και κόκκινης ομάδας (penetration test and red team assessment)

β. Μεθοδολογία Δοκιμής διείσδυσης (Penetration Test Methodology)
γ. Προετοιμασία διεξαγωγής Δοκιμής διείσδυσης (Penetration test Essentials Pre-engagement)
δ. Πεδίο εφαρμογής, Δεοντολογικές απαιτήσεις και νομικά ζητήματα
ε. Δομή και εξαρτήματα της έκθεσης δοκιμής διείσδυσης
στ. Δημιουργία εργαστηρίου δοκιμών διείσδυσης
ζ. Προετοιμασία, ανάπτυξη υποδομής OSINT και ανωνυμίας.

2. Συλλογή πληροφοριών
α. Αναγνώριση (αναγνώριση DNS TCP, UDP, συνδέσεις)
β. OSINT (Νοημοσύνη ανοιχτού κώδικα)
γ. Μεθοδολογία σάρωσης
δ. Σάρωση συστήματος και δικτύου, Σάρωση με χρήση nmap

3. Αξιολόγηση ευπαθειών (vulnerability assessment)
α. Netcat
β. Nessus
γ. OpenVas

4. Πλατφόρμες διεξαγωγής ελέγχου διείσδυσης (Penetration test frameworks)
α. Metasploit
β. Poshc2
γ. Covenant
δ. Mythic

5. Βασική γνώση στην ασφάλεια ενός windows λειτουργικού συστήματος
α. Εσωτερικοί μηχανισμοί ασφαλείας ενός Windows
β. Πολιτικές ασφαλείας (Security policies)
γ. Συσκευές και λογισμικά ασφαλείας (Security software and devices)

6. Τεχνικές απόκτησης αρχικής πρόσβασης (Gaining initial access)
α. Εισαγωγή στις επιθέσεις των windows
β. Brute forcing
γ. Απομακρυσμένη εκμετάλλευση ευπαθειών
δ. Επιθέσεις τελικού χρήστη
ε. Πλατφόρμες και επιθέσεις phishing (Spear-phishing / phishing / κλοπή έγκυρων διαπιστευτηρίων)

7. Τεχνικές και διαδικασίες επιθέσεων μετά την αρχική πρόσβαση σε ένα Windows δίκτυο (post exploitation techniques)
α. Επαύξηση δικαιωμάτων privilege escalation)
β. Εσωτερική δικτυακή μετακίνηση (Password Spraying, AV, EDR evasion)
γ. Powershel για penetration testers
δ. Επιθέσεις Active Directory (Kerberos Authentication, Domain enumeration, Domain attacks, Kerberoasting attack, Golden ticket, Pass the hash attack, pass the ticket, over pass the hash)

8. Διαχείριση κυβερνοεπιθέσεων (Incident handling process)
α. Εισαγωγή στην Διαχείριση κυβερνοεπιθέσεων
β. Σχέδιο Διαχείρισης κυβερνοεπιθέσεων (Incident handling plan)

9. Διαδικασία ψηφιακής σήμανσης (Digital Forensics process)

α. Μεθοδολογία ψηφιακής σήμανσης (Digital Forensics methodology) β. Δημιουργία ενός υπολογιστή ανάλυσης ψηφιακής ευρημάτων (Building a forensics analysis station). γ. Δημιουργία ενός εργαστηρίου ψηφιακής σήμανσης (Building a forensics lab). 10. Ανάλυση μνήμης ενός Windows συστήματος (memory forensics) α. Εισαγωγή στην μνήμη ενός windows λειτουργικού (Memory Essentials) β. Συλλογή μνήμης (Dumping the memory) γ. Ανάλυση της μνήμης (Memory analysis 11. Ψηφιακή ανάλυση μητρώου (Windows registry forensics) α. Εισαγωγή στην Registry Essentials β. Συλλογή της registry γ. Ανάλυση της Registry 12. Ψηφιακή σήμανση αρχείου συστήματος (Windows file system forensics) α. Εισαγωγή στο windows file system β. Συλλογή των αρχείων συστήματος (Gathering file system relative to case information) γ. Ανάλυση του File system δ. Ανάλυση των Windows event log 13. Ψηφιακή σήμανση Windows εφαρμογών (application forensics) α. Browser Forensics β. Email forensics γ. Usb forensics δ. Σύνταξη αναφοράς ψηφιακής σήμανσης

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ – ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	*Πρόσωπο με πρόσωπο, Εξ αποστάσεως*
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, στην Εργαστηριακή Εκπαίδευση και στην Επικοινωνία με τους Φοιτητές***
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*	***Δραστηριότητα*** — ***Φόρτος Εργασίας Εξαμήνου*** *Διαλέξεις* — 39 *Εργαστηριακή Άσκηση* — 26 *Συγγραφή εργασίας* — 40

(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*	*Μελέτη* 60 Ανάλυση βιβλιογραφίας 35 Σύνολο Μαθήματος ***200***
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.*	*Η αξιολόγηση των φοιτητών πραγματοποιείται με γραπτή εργασία, καθώς και με την πρακτική διεξαγωγή ελέγχου διείσδυσης ή ολοκληρωμένης ψηφιακής εγκληματολογικής ανάλυσης ενός παραβιασμένου windows λειτουργικού συστήματος.*

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία*:*

- *The Hacker Playbook 3: Practical Guide To Penetration Testing,* ***Peter Kim****, 2018, Red Team Book.*
- ***Incident Response with Threat Intelligence: Practical insights into developing an incident response capability through intelligence-based threat hunting****, by Roberto Martínez,* ***2022, Packet Publishing****.*
- *Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8, by Harlan Carvey, 2009*

Recommended

- *Harlan Carvey, Investigating Windows Systems 1st Edition , Elsevier*
- *File System Forensic Analysis 1st Edition by Brian Carrier, 2005. Addison-Wesley Professional*
- *Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition by Daniel Teixeira (Author), Abhinav Singh (Author), Monika Agarwal (Author), 2018, Packt Publishing*
- *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey. 2011*
- *Penetration Tester's Open Source Toolkit 4th Edition, Kindle Edition by Jeremy Faircloth, 2016, Singress.*

Αναλυτική περιγραφή των μαθημάτων (ΑΓΓΛΙΚΑ)

1. Blockchain & Distributed Ledger technologies

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF EDUCATION	GRADUATE		
COURSE CODE	CSCYB-105	**SEMESTER OF STUDIES**	**A’**
COURSE TITLE	**Blockchain & Distributed Ledger Technologies**		

INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in separate parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the whole course, indicate the weekly teaching hours and the total number of credits.*	**WEEKLY HOURS OF TEACHING**	**ECTS CREDITS**
Lectures	3	
Practice -Exercises	2	
Add rows if needed. The teaching organization and teaching - methods used are described in detail in 4.	**5**	**7.5**

COURSE TYPE *Background, General Knowledge, Scientific Area, Skills Development*	*Skills Development, Background*
PREREQUISITE COURSES:	-NONE
LANGUAGE OF TEACHING AND EXAMS :	ENGLISH
ERASMUS STUDENTS	Yes (English)
ONLINE COURSE (URL)	Cscyb.uniwa.gr and eclass (https://eclass.uniwa.gr/courses/CSCYB103/)

2.LEARNING OUTCOMES

Learning outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Refer to Appendix A.

- *Description of the Level of Learning Outcomes for each course according to the Qualifications Framework of the European Higher Education Area*
- *Descriptive Indicators Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

In the Blockchain & Distributed Ledger Technologies course, students will get to know the characteristics of the Blockchain technology and its features without any pre-requisite.

Upon completion of the course, students will be able to:

- argue about the use (or not) of a solution based on blockchain technology in a given use case.
- design a solution based on blockchain technology
- understand how the use of cryptography and digital signatures can improve data integrity and security
- create a wallet and use it for transactions
- connect and trade in the most popular Blockchain networks (Ethereum, Bitcoin).
- create and install a Smart Contract
- create an NFT

General Abilities

Taking into account the general skills that the graduate must have acquired (as they are listed in the Diploma Supplement and are listed below), which of them is intended for the course ?.

Search, analysis and synthesis of data and information, using the necessary technologies	*Project design and management*
Adaptation to new situations	*Respect for diversity and multiculturalism*
Decision making	*Respect for the natural environment*
Autonomous work	*Demonstration of social, professional and moral responsibility and sensitivity in gender issues*
Teamwork	*Exercise criticism and self-criticism*
Working in an international environment	*Promoting free, creative and inductive thinking*
Work in an interdisciplinary environment	
Production of new research ideas	

Search, analysis and synthesis of data and information, using the necessary technologies
Adaptation to new situations
Decision making
Autonomous work
Teamwork

3. COURSE CONTENT

Theoretical Part of the Course:

The course is divided into 8 sections:

Section 1: Introduction to Blockchain Technology

In this Section, the main features of blockchain technology are presented and its advantages and disadvantages are analyzed. In addition, the types of blockchains that exist are analyzed and it is studied how one can find if a blockchain solution is suitable for a use case and if so which type fits best.

Section 2: Popular Blockchain Platforms

This Section analyzes the two most popular blockchain networks, that of Bitcoin and Ethereum. Their main operating characteristics are examined and their similarities and differences are noted.

Section 3: Keys and Addresses

In this Section, there is a detailed presentation on the role of asymmetric cryptography for the creation of the private and public key pair. Also, it is analyzed how the user's address in the Bitcoin network and Ethereum is obtained from this pair of keys.

Section 4: Digital Signatures and Wallets

This Section presents how digital signatures are created using encryption and explains the role they play in a Blockchain network. In addition, the role that wallets play in a blockchain network is analyzed and the different types of wallets that exist are studied.

Section 5: Transactions

This Section explains how transactions are done on the Bitcoin and Ethereum networks. Their main difference is explained and examples are presented for understanding.

Unit 6: Smart Contracts and Non-Fungible Tokens (NFTs)

In this Section there will be a presentation of Smart Contracts on the Ethereum network. The way they are compiled and the role of gas in their execution will be explained. Also, a Smart Contract will be drawn up and installed on a real test network. In addition, the ERC standards on which NFTs and tokens are based will be presented and examples of how NFTs based on the ERC721 standard can be created.

Unit 7: Decentralized Applications and Introduction to Web 3.0

In this Section, a presentation of Web3.0 will be made and its differences with Web 2.0 will be explained. Then, it will be explained how a Decentralized Application can be created (DApp) and how it is connected to a blockchain network and the necessary Smart Contracts.

Section 8: Use Cases

This Section presents many use cases where the use of blockchain technology can have very good results and improve the performance of modern solutions. In addition, it analyzes both why blockchain technology can help and what kind of solution is proposed to be used in each case.

Laboratory Part of the Course

The laboratory part of the course follows the theoretical part. It uses tools like *ETH.Build* which is recommended by the Ethereum Foundation to educate the world on Blockchain technology. This tool gives exercises related to:

- Cryptography
- Digital Signatures
- Transactions

In addition, *Remix* tool is used to write the Smart Contracts and install them on a real Ethereum Test Network. For this reason, an account will be made in a wallet (e.g., *Metamask*). The wallet will also be used to transfer NFTs between the students.

4. TEACHING AND LEARNING METHODS - EVALUATION

METHOD OF DELIVERY *Face to face, Distance education etc.*	In class face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Education, in Communication with students*	Use of ICT in Teaching, Laboratory Education and Communication with Students

TEACHING ORGANIZATION *The way and methods of teaching are described in detail.* *Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography study & analysis, Tutoring, Internship (Placement), Clinical Exercise, Art Workshop, Interactive teaching , Study visits, Study work, artwork, creation. λπ.* *The student study hours for each learning activity are indicated as well as the non-guided study hours so that the total workload at the semester level corresponds to the ECTS standards .*	Projection system and presentation capability with the application of the Power Point program, - Internet connection, - Use of bibliography search engines HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR - Use of e-mail and the Department's website to communicate with students and keep them informed - Use of the course eclass
STUDENT EVALUATION *Description of the evaluation process* *Assessment Language, Assessment Methods, Formative or Concluding, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment, Report / Report, Oral Examination, Public Presentation, Public Presentation, Others* *Explicitly defined assessment criteria are stated and if and where they are accessible to students.*	A final project will be assigned and the grade will depend on: - On the submitted written report (40%) - In the oral presentation of the work (60%) Each exercise/problem of the project has a different score which is indicated in the project.

5. RECOMMENDED-BIBLIOGRAPHY

- Suggested Bibliography:

English

3. *A. Antonopoulos, “Mastering Bitcoin”, O’Reilly, 2nd edition, 2017.*
4. *A. Antonopoulods, G. Wood, “Mastering Ethereum: Building Smart Contracts and DApps”, O’Relly, 1st Edition, 2018.*

Greek

Patrikakis, C., Leligkou, H., & Kogias, D. (2023). *Blockchain* [Postgraduate textbook]. Kallipos, Open Academic Editions. https://dx.doi.org/10.57713/kallipos-171

Links

https://bitcoin.org/bitcoin.pdf

2. Applied Cryptography

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE		
COURSE UNIT CODE	**CSCYB103**	**SEMESTER OF STUDY**	1st
COURSE TITLE	**Applied Cryptography**		

COURSEWORK BREAKDOWN	TEACHING WEEKLY HOURS	ECTS Credits
Lectures	3	
Tutorials	1	
	4	**8**

COURSE UNIT TYPE	Compulsory, Specialized general knowledge
COURSE DELIVERED TO ERASMUS STUDENTS	YES
MODULE WEB PAGE (URL)	https://eclass.uniwa.gr/courses/CSCYB105/

2.LEARNING OUTCOMES

Learning Outcomes
• An introduction on cryptographic definitions and notions • Familiarization with security issues • Understanding of the cryptographic protocols capabilities • The skills to select the most adequate cryptographic solutions for given security problem.
General Skills
• *Search for optimal cryptographic solutions* • *Independent work*

3.COURSE CONTENTS

The description contains the material to be covered during 13 sessions.

1) Introduction to cryptography. History of cryptography and definitions
2) Mathematical background. Modular computations, Boolean functions, birthday paradox
3) Pseudorandom generators and stream ciphers
4) Pseudorandom functions. Block ciphers (AES) and modes of operation (CBC,CTR).
5) One way functions and hash functions (SHA-2, SHA-3).
6) Message Authentication codes. HMAC and ECBC.
7) Authenticated encryption with associated data (GCM).
8) Public key cryptography. RSA and secure implementations. The problem of factorization
9) El Gamal and elliptic curves. The discrete logarithm problem.
10) Digital signatures. Digital signature algorithm, EdDSA.
11) Attacks against symmetric and public key encryption protocols
12) Key Encapsulation Mechanism, Key encryption, Diffie-Hellman Key agreement, and authentication protocols
13) Advanced cryptography: MPC, ORAM, Homomorphic encryption

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open e-Class system, with uploaded notes, lectures, exercises for practice and communication with students.

TEACHING METHODS

Method description	*Semester Workload*
Lectures	39

	Tutorials	39
	Research work	50
	Self study	60
	Total course hours (25 h workload per ECTS)	***188***
ASSESSMENT METHODS	I. A written final examination (60%) and II. Research work (40%)	

5.RESOURCES

Essential

- *Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell (2nd Edition!)*
- *Cryptography Made Simple. Nigel Smart. Springer*

Recommended

- *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*
- *ENISA, Algorithms, key size and parameters, report – 2014*
- *ECRYPT – CSA, Algorithms, Key Size and Protocols Report (2018)*

3. Software and DATABASE SYSTEMS SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE		
COURSE UNIT CODE	**CSCYB205**	**SEMESTER OF STUDY**	2nd
COURSE TITLE	**Software and Database Systems Security**		
COURSEWORK BREAKDOWN		**TEACHING WEEKLY HOURS**	**ECTS Credits**
	Lectures	3	
	Tutorials	2	
		5	**7**
COURSE UNIT TYPE	Compulsory, Specialized general knowledge		
PREREQUISITES :	NONE		
LANGUAGE OF INSTRUCTION/EXAMS:	GREEK, ENGLISH		
COURSE DELIVERED TO ERASMUS STUDENTS	YES		
MODULE WEB PAGE (URL)			

2. LEARNING OUTCOMES

Learning Outcomes
• To understand the risks that exists in data publishing • To know the existing options for secure databases • To design more secure databases

General Skills
• To be able to protect client’s data from attacks • To understand the main concept of big data and the trends and security risks of the modern applications • To know which data should be protected

3.COURSE CONTENTS

The description contains the material to be covered during 13 sessions.

- Discretionary and mandatory access control
- Security protection capabilities of the SQL language
- Privacy protection for relational, spatial and graph data
- Privacy protection of data changing over time
- Digital watermarking and fingerprinting in relational databases.
- Encrypted databases and retrieval of encrypted data
- Security in statistical and distributed databases
- Big data security
- Data security and privacy protection in online social networks.
- Big data integration and security

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.
TEACHING METHODS	***Method description*** / ***Semester Workload*** Lectures: 39 Tutorials: 26 *Research work*: 50 Self study: 60 ***Total course hours (25 h workload per ECTS)***: ***175***
ASSESSMENT METHODS	I. A written final examination (20%) and II. Research work (80%)

5.RESOURCES

Essential

- *Privacy Preserving Data Publishing: An Overview, Synthesis Lectures on Data Management, 2010, Raymond Chi Wing Wong, Ada Wai Chee Fu*
- *Rakesh Agrawal and Jerry Kiernan. 2002. Watermarking relational databases. In Proceedings of the 28th international conference on Very Large Data Bases*
- *Database management systems, 3rd. Ed., Ramakrishnan Raghu, Gehrke Joahannes . (Chapter 24)*
- *Fundamentals of Database Systems, 7th Edition, Elmasri Ramez, Navathe Shamkant B.B (Chapter 17)*

Recommended

- *Chen, Bee Chung & Kifer , Daniel & LeFevre, Kristen & Machanavajjhala , Ashwin. (2009). Privacy Preserving Data Publishing. Foundations and Trends in Databases.*

- *Fung, Benjamin & Wang, ke & Chen, Rui & Yu, Philip. (2010). Privacy Preserving Data Publishing: A Survey of Recent Developments. ACM Comput . Surv .. 42.*
- *Watermarking Techniques for Relational Databases: Survey, Classification and Comparison, Raju Halder, Shantanu Pal and Agostino Cortesi*

4. HARDWARE SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF EDUCATION	GRADUATE		
COURSE CODE	CSCYB-201	**SEMESTER OF STUDIES**	**B’**
COURSE TITLE	**HARDWARE SECURITY**		
INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in separate parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the whole course, indicate the weekly teaching hours and the total number of credits.*		**WEEKLY HOURS OF TEACHING**	**ECTS CREDITS**
	Lectures	3	
	Practice -Exercises		
Add rows if needed. The teaching organization and teaching - methods used are described in detail in 4.		**3**	**8**
COURSE TYPE *Background, General Knowledge, Scientific Area, Skills Development*	*Compulsory, Specialized general knowledge*		
ERASMUS STUDENTS	Yes (English)		
ONLINE COURSE (URL)	Cscyb.uniwa.gr and eclass (UNIWA Open eClass | Επιλογή μαθημάτων)		

2.LEARNING OUTCOMES

Learning outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Refer to Appendix A.

- *Description of the Level of Learning Outcomes for each course according to the Qualifications Framework of the European Higher Education Area*
- *Descriptive Indicators Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

The aim of this course is to provide post-graduate students with the appropriate knowledge and skills about major topics in hardware security, including hardware security vulnerabilities, attacks, and appropriate protection mechanisms. Upon successful completion of the course the student will be able to:

- Formulate hardware security requirements for a system.
- Describe the types of errors, faults and hazards in a system and how to deal with them, and select appropriate methods to deal with them.

- Describe and apply hardware security analysis methods.
- Describe and apply hardware security assessment methods.
- Design digital circuits for cryptographic applications.
- Design circuits that will contain built-in test structures for easy controllability.
- Check circuits for defects or harmful additional hardware components.

General Abilities

Taking into account the general skills that the graduate must have acquired (as they are listed in the Diploma Supplement and are listed below), which of them is intended for the course ?.

Search, analysis and synthesis of data and information, using the necessary technologies	*Project design and management*
Adaptation to new situations	*Respect for diversity and multiculturalism*
Decision making	*Respect for the natural environment*
Autonomous work	*Demonstration of social, professional and moral responsibility and sensitivity in gender issues*
Teamwork	*Exercise criticism and self-criticism*
Working in an international environment	*Promoting free, creative and inductive thinking*
Work in an interdisciplinary environment	
Production of new research ideas	

The course aims to the following general competences:

- Search for, analysis and synthesis of data and information, with the use of the necessary technology
- Working independently
- Team work
- Working in an international environment
- Decision making

3.COURSE CONTENT

The description contains the material to be covered during 13 lectures.

Lectures 1-2: Introduction and basic concepts, evolution of hardware security, overview and layers of a computing system, types of electronic hardware, hardware security vs. hardware trust, security and test/debug, electronic supply chain.

Lectures 3-4: Introduction to data encryption and security, data encryption standards (DES, AES) and block ciphers, public key cryptography and RSA asymmetric key algorithm.

Lecture 5: Basics of VLSI Design and Test

Lecture 6: Physical attacks

Lectures 7: Hardware Intellectual Property (IP) piracy and reverse engineering

Lecture 8: Side-Channel Attacks

Lecture 9: Hardware Trojans

Lecture 10: Attacks on PCB, RFID and JTAG

Lecture 11-12: Hardware security primitives, physically unclonable functions (PUFs) and true random number generators (TRNGs)

Lecture 13: Hardware metering and digital watermarking

4.TEACHING AND LEARNING METHODS - EVALUATION

METHOD OF DELIVERY *Face to face, Distance education etc.*	This module is taught through a combination of lectures, exercises, computer laboratory sessions, and coursework exercises.

USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Education, in Communication with students*	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.
TEACHING ORGANIZATION *The way and methods of teaching are described in detail.* *Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography study & analysis, Tutoring, Internship (Placement), Clinical Exercise, Art Workshop, Interactive teaching , Study visits, Study work, artwork, creation. λπ.* *The student study hours for each learning activity are indicated as well as the non-guided study hours so that the total workload at the semester level corresponds to the ECTS standards .*	Projection system and presentation capability with the application of the Power Point program, - Internet connection, - Use of bibliography search engines HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR - Use of e-mail and the Department's website to communicate with students and keep them informed - Use of the course eclass
STUDENT EVALUATION *Description of the evaluation process* *Assessment Language, Assessment Methods, Formative or Concluding, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment, Report / Report, Oral Examination, Public Presentation, Public Presentation, Others* *Explicitly defined assessment criteria are stated and if and where they are accessible to students.*	I. Project 1 (50%) and II. Project 2 (50%)

5. RECOMMENDED-BIBLIOGRAPHY

Essential

- S. Bhuniaand, M. Tehranipoor, Hardware Security: A Hands-on Learning Approach, Morgan Kaufmann–Elsevier, 1st edition, 2018.

Recommended

- 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.

5. INFORMATION SYSTEMS SECURITY

1.GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF EDUCATION	GRADUATE		
COURSE CODE	CSCYB-101	**SEMESTER OF STUDIES**	**A’**
COURSE TITLE	**INFORMATION SYSTEMS SECURITY**		
INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in separate parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the whole course, indicate the weekly teaching hours and the total number of credits.*		**WEEKLY HOURS OF TEACHING**	**ECTS CREDITS**
Lectures		3	
Practice -Exercises		2	
Add rows if needed. The teaching organization and teaching - methods used are described in detail in 4.		**5**	**8**
COURSE TYPE *Background, General Knowledge, Scientific Area, Skills Development*	*Skills Development*		
PREREQUISITE COURSES:	-NONE		
LANGUAGE OF TEACHING AND EXAMS :	ENGLISH		
ERASMUS STUDENTS	Yes (English)		
ONLINE COURSE (URL)	Cscyb.uniwa.gr and eclass https://eclass.uniwa.gr/main/login_form.php?next=%2Fmodules%2Fauth%2Fcourses.php%3Ffc%3D247		

2. LEARNING OUTCOMES

Learning outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Refer to Appendix A.

- *Description of the Level of Learning Outcomes for each course according to the Qualifications Framework of the European Higher Education Area*

- *Descriptive Indicators Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

Knowledge

The MSc students can:

- Understand modern information systems security issues and their challenges
- Desing the framework for the development of information security management system
- Demonstrate critical understanding of the design, application, and performance evaluation of the appropriate controls/safeguards/countemeasures: organizational, technological, physical, people
- Have specific knowledge for the special characteristics of the cloud controls
- Understand the information security risk management methodology
- Know the problems that generated when personal data have been processed and know personal data protection by design methodologies
- Have critical perception of the evolutionary dynamics of the area of cybersecurity and personal data protection.

During the lecturers, modern international standards are described for the selection of the suitable controls: detection, prevention, correction.

Skills

This course is structured in a way that lectures and practical exercises give students the necessary skills for the job market, in order to improve their possibility of professional rehabilitation
After their studies MSc students can:

- Apply theories and methodologies from the area of information systems security, with emphasis on information security risk management
- Evaluate methods and tools thar are used to implement information systems security
- Develop solutions, with scientific documented way, for the complex security and privacy problems

Competences

The MSc students will be able to:

- Develop autonomously their knowledge and capabilities
- Solve problems and kame strategic decisions with inductive thinking
- Contribute to develop knowledge and practices and have operational capabilities in crisis management

General Abilities

Taking into account the general skills that the graduate must have acquired (as they are listed in the Diploma Supplement and are listed below), which of them is intended for the course ?.

Search, analysis and synthesis of data and information, using the necessary technologies	*Project design and management*
Adaptation to new situations	*Respect for diversity and multiculturalism*
Decision making	*Respect for the natural environment*
Autonomous work	*Demonstration of social, professional and moral responsibility and sensitivity in gender issues*
Teamwork	*Exercise criticism and self-criticism*
Working in an international environment	*Promoting free, creative and inductive thinking*
Work in an interdisciplinary environment	
Production of new research ideas	

The general competences that the MSc students must acquire are:

- Search, analysis, synthesis of data and information, with the use of the appropriate technologies
- Decision making
- Working independently
- Effective team work
- Adapting to new situations
- Project planning and management guaranteeing quality (iron triangle: time, cost, scope)
- Activation in multidisciplinary environment
- Production of new research ideas

3.COURSE CONTENT

Theory:

1. Introduction to information and communication systems security. Terminology and ISO 27000:2018.
2. Authorization and Access Control: Mandatory Access Control, Discretionary Access Control (Access Control Matrix, Access Control List, Capabilities List), Role-based Access Control (Core, Hierarchical, Constrained).
3. Information Security Management System ISMS and ISO 27001:2022,
4. controls and ISO 27002:2022,
5. guidance on implementing ISMS and ISO 27003:2017,
6. best practices for Cloud environment and ISO 27017: 2015.
7. Guidance for Information Security Risk Management and ISO 27005:2022.
8. Information Security Management Guidelines for Cyber insurance and ISO 27102:2019.
9. Legal and regulatory framework for personal data protection and electronic communication security:
10. General Data Protection Regulation and ISO 29100:2017,
11. EU Directive e-Privacy 2002/58, EU Directive for data retention 2006/24.
12. The Constitution of Greece, article 19 for communication security and related national laws: law 5002/2022, law 3115/2003. Spyware and risk treatment.

Laboratory:

Case studies: Enterprise Risk Management, Personal Data Protection, Electronic Communication Security

4.TEACHING AND LEARNING METHODS - EVALUATION

METHOD OF DELIVERY *Face to face, Distance education etc.*	In class face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Education, in Communication with students*	Use of ICT in Teaching, Laboratory Education and Communication with Students
TEACHING ORGANIZATION *The way and methods of teaching are described in detail.* *Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography study & analysis, Tutoring, Internship (Placement), Clinical Exercise, Art Workshop, Interactive teaching , Study visits, Study work, artwork, creation. λπ.* *The student study hours for each learning activity are indicated as well as the non-guided study hours so that the total workload at the semester level corresponds to the ECTS standards .*	Projection system and presentation capability with the application of the Power Point program, - Internet connection, - Use of bibliography search engines HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR - Use of e-mail and the Department's website to communicate with students and keep them informed - Use of the course eclass

STUDENT EVALUATION *Description of the evaluation process* *Assessment Language, Assessment Methods, Formative or Concluding, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment, Report / Report, Oral Examination, Public Presentation, Public Presentation, Others* *Explicitly defined assessment criteria are stated and if and where they are accessible to students.*	Written final exam and Assignments (Individual and Group). The performance in the exams is calculated as follows: 50% of the final grade for the written exams, 50% for the Assignment

5.RECOMMENDED-BIBLIOGRAPHY

- Suggested Bibliography:

Books
Security Engineering A Guide to Building Dependable Distributed Systems, R. Anderson, J. Wiley & Sons, 3rd edition, 2020
The Cyber Security Handbook, A. Calder, ITGP, 2020
Cybersecurity, E. Lewis, 2020
The Age of Surveillance Capitalism, S. Zuboff, Profile Books, 2019
Computer Security, D. Gollmann, J. Wiley & Sons, 3rd edition, 2018

Journals
IEEE Communications Surveys and Tutorials
International Journal of Information Security, Springer
Computers and Security, Elsevier
Information and Computer Security, Emerald

6. INFORMATION SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE		
COURSE UNIT CODE	**csCYB104**	**SEMESTER OF STUDY**	1st
COURSE TITLE	**INFORMATION SECURITY**		
COURSEWORK BREAKDOWN		**TEACHING WEEKLY HOURS**	**ECTS Credits**
	Lectures	2	
	Tutorials	1	
		3	**3**
COURSE UNIT TYPE	Compulsory, Specialized general knowledge		
PREREQUISITES :	NONE		
LANGUAGE OF INSTRUCTION/EXAMS:	ENGLISH		
COURSE DELIVERED TO ERASMUS STUDENTS	YES		
MODULE WEB PAGE (URL)	http://		

2.LEARNING OUTCOMES

Learning Outcomes
The course aims at training students in the area of information and communication systems security, as well as in privacy protection technologies. Overall, the course has been planned taking the following points into consideration: Upon successful completion of this course, the student will be able to: • the deepening and consolidation of a high level of knowledge in the breadth of the field of Information Security. • Acquire specialized skills in solving Information Security Systems problems with the aim of gaining a base for research and innovation design in the field of Security. In particular the student must: • Understand the structure and operation of Information Security (at Internet) Systems. • Have a thorough knowledge of Network layers, IPv4, ICMP, ARP, Sniffing, MAC Spoofing, . • Know and explain the security of internet applications, network architectures, signaling, and communication protocols. • Evaluate the Cryptology’s criteria • Choose the appropriate digital signatures and digital certificates. • Analyze and compare the modern cryptographic algorithms • Create and design the Security Management Systems • Learn the Legal framework of the Internet Privacy and Cybercrime
General Skills
• Retrieve, analyze and synthesize data and information, with the use of necessary technologies • Team work • Be critical and self-critical • Advance free, creative and causative thinking

3.COURSE CONTENTS

The description contains the material to be covered during 13 sessions.

1) Basic security concepts and issues
2) Networks and Internet
3) Secured Interface Connection
4) Internet programming
5) Security of Internet Applications
6) Introduction to Cryptology
7) Modern Cryptographic Algorithms
8) Message Integrity and Authenticity
9) Digital Signatures and Digital Certificates
10) Virtual Private Networks
11) Security Management
12) Response to Security Events & Digital Forensics
13) Internet Privacy and Cybercrime

4.TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.

TEACHING METHODS	*Method description*	*Semester Workload*
	Lectures	26
	Tutorials	13
	Research work	25
	Self study	48
	Total course hours (25 h workload per ECTS)	***125***
ASSESSMENT METHODS	I. A written final examination (60%) and II. Research work (40%)	

5.RESOURCES

Essential

- *Κρυπτογραφία & Ασφάλεια Δικτύων Αρχές& Εφαρμογές, William Stallings, Εκδόσεις ΙΩΝ.*
- *Κάτσικα Σ, Γκρίτζαλη Δ., Γκρίτζαλη Σ. Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέες Τεχνολογίες.*
- *Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Δικτύων Υπολογιστών, Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ ΟΕ, 2003.*
- *Business Information Systems: Technology, Development and Management for the Modern Business, Paul Bocij, Andrew Greasley, Simon Hickie, Sixth edition, Pearson 2018*

Recommended

- *Cybersecurity, Mowbray Thomas J.,* Third edition, *John Wiley & Sons In*
- *Anderson R., Security Engineering, Wiley (2nd ed.), USA, 2008.*
- *Gollmann D., Computer Security, 3rd edition, Wiley, March 2011.*
- *Pfleeger C., Security in Computing, Prentice Hall (4th ed.), USA, 2006.*
- *Rhodes-Ousley M. Information security: The complete reference. McGraw-Hill Education. Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., Ασφάλεια της Πληροφορίας, Εκδόσεις Νέες Τεχνολογίες, 2004*

7. NETWORK SECURITY

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	DEPARTMENT OF INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF EDUCATION	GRADUATE		
COURSE CODE	CSCYB206	**SEMESTER OF STUDIES**	**B’**
COURSE TITLE	**Network Security**		

INDEPENDENT TEACHING ACTIVITIES *in case the credits are awarded in separate parts of the course e.g. Lectures, Laboratory Exercises, etc. If the credits are awarded uniformly for the whole course, indicate the weekly teaching hours and the total number of credits.*	**WEEKLY HOURS OF TEACHING**	**ECTS CREDITS**
Lectures	3	
Practice -Exercises	2	

Add rows if needed. The teaching organization and teaching methods used are described in detail in 4.	5	**7**
COURSE TYPE *Background, General Knowledge, Scientific Area, Skills Development*	*Skills Development*	
PREREQUISITE COURSES:	-NONE	
LANGUAGE OF TEACHING AND EXAMS :	ENGLISH	
ERASMUS STUDENTS	Yes (English)	
ONLINE COURSE (URL)	Cscyb.uniwa.gr and eclass (UNIWA Open eClass | Επιλογή μαθημάτων)	

2. LEARNING OUTCOMES

Learning outcomes

The learning outcomes of the course are described, the specific knowledge, skills and abilities of an appropriate level that students will acquire after the successful completion of the course.

Refer to Appendix A.

- *Description of the Level of Learning Outcomes for each course according to the Qualifications Framework of the European Higher Education Area*
- *Descriptive Indicators Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Annex B*
- *Summary Guide for writing Learning Outcomes*

Network Security is a key topic in a Cybersecurity Master of Science program that enhances students' knowledge on security in many different types of computer networks.
The aim of the course is to deepen the theoretical and practical skills that students already have in computer networks and in the field of computer security, and cover the required complementary topics in a cybersecurity framework. This will provide them with additional expertise and high-level skills for the job market and research dimensions to continue their studies at the next level.
By the end of this course a student will reach the professional level in network security in terms of up-to-date terminologies, main concepts, new technologies, and popular tools.

Upon successful completion of the course the student will be able to:

- to recognize the factors that lead to the need for network and communications security.
- identify and categorize specific examples of network attacks.
- identify vulnerabilities in communications and networks.
- to design and implement secure network systems and applications.
- to distinguish the advantages and disadvantages of alternative secure network and communications architectures.
- to distinguish and compare symmetric and asymmetric cryptosystems and to know the characteristics of hybrid systems.
- to know the tools and techniques to identify the security gaps of network devices and applications and to distinguish problems and errors due to insufficient implementation of security mechanisms of devices and insufficient protection of information transmitted through online applications.
- to apply his knowledge to protect devices and networked information from malicious interception, modification, destruction and falsification of information.
- to evaluate the secure operation of networks, to identify any security gaps when accessing and transmitting information, especially to remote users.
- to face developments in the field of network and communications security, topics in which he will have deepened his knowledge.
- will have the ability to guide the changes brought about by technological

developments in this field.
- will have the ability to evaluate and distinguish between secure and non-secure network systems and communications between their parts.
- will have the ability to systematically apply the acquired knowledge to understand and solve practical problems.
- will have the ability to use modern methods to protect network and communication systems.

will have the ability to work with others to solve real-world problems.

General Abilities

Taking into account the general skills that the graduate must have acquired (as they are listed in the Diploma Supplement and are listed below), which of them is intended for the course ?.

Search, analysis and synthesis of data and information, using the necessary technologies *Adaptation to new situations* *Decision making* *Autonomous work* *Teamwork* *Working in an international environment* *Work in an interdisciplinary environment* *Production of new research ideas*	*Project design and management* *Respect for diversity and multiculturalism* *Respect for the natural environment* *Demonstration of social, professional and moral responsibility and sensitivity in gender issues* *Exercise criticism and self-criticism* *Promoting free, creative and inductive thinking*

Working in an interdisciplinary environment
Generating new research ideas
Searching, analysing and synthesising data
Adapting to new situations
Decision-making

3. COURSE CONTENT

This course is organized as follows:
Lecture 1: Introduction to Network Security
Lecture 2: Encryption
Lecture 3: Intrusion Detection Systems
Lecture 4: Vehicular Ad-hoc Networks
Lecture 5: WEKA
Lecture 6: TCP Attacks
Lecture 7: Privacy
Lecture 8: Firewall Avoidance using VPN
Lecture 9: SNORT
Lecture 10: Advanced Intrusion Detection Topics
Lecture 11: Security and Privacy on the Blockchain
Lecture 12: Trusted Supply Chains
Lecture 13: Presentation of final papers and public discussion on them

4. TEACHING AND LEARNING METHODS - EVALUATION

METHOD OF DELIVERY *Face to face, Distance education etc.*	In class face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES *Use of ICT in Teaching, in Laboratory Education, in Communication with students*	Use of ICT in Teaching, Laboratory Education and Communication with Students

TEACHING ORGANIZATION
The way and methods of teaching are described in detail.
Lectures, Seminars, Laboratory Exercise, Field Exercise, Bibliography study & analysis, Tutoring, Internship (Placement), Clinical Exercise, Art Workshop, Interactive teaching , Study visits, Study work, artwork, creation. λπ.

The student study hours for each learning activity are indicated as well as the non-guided study hours so that the total workload at the semester level corresponds to the ECTS standards .

Projection system and presentation capability with the application of the Power Point program,
- Internet connection,
- Use of bibliography search engines HEAL-LINK, PUBMED, SCOPUS, GOOGLE SCHOLAR
- Use of e-mail and the Department's website to communicate with students and keep them informed
- Use of the course eclass
-

Semester Workload Activity

Method description	*Semester Workload*
Lectures	39
Practice exercises that focus on the application of methodologies and analysis of studies	26
Research work	50
Self study	60
Total course hours (25 h workload per ECTS)	***175***

STUDENT EVALUATION
Description of the evaluation process

Assessment Language, Assessment Methods, Formative or Concluding, Multiple Choice Test, Short Answer Questions, Essay Development Questions, Problem Solving, Written Assignment, Report / Report, Oral Examination, Public Presentation, Public Presentation, Others
Explicitly defined assessment criteria are stated and if and where they are accessible to students.

Presentation and examination of Final Project (100%).

5. RECOMMENDED-BIBLIOGRAPHY

- Προτεινόμενη Βιβλιογραφία :

1. W.Stallings, Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, Εκδότης Παρίκου ΕΠΕ, 2011 (Κωδ. Εύδοξος: 12777632)
2. J.F. Kurose, K.W. Ross, “Δικτύωση Υπολογιστών, Προσέγγιση από πάνω προς τα κάτω, 6η Έκδοση 2013”, Εκδόσεις: Γκιούρδα & ΣΙΑ, (Κωδ. Εύδοξος: 33094885)
3. B. Forouzan, Cryptography and Network Security, McGraw Hill, Εκδόσεις Επίκεντρο Α.Ε, 2008 (Κωδ. Εύδοξος: 12562157)
4. J.F. Kizza, “Guide to Computer Network Security”, Springer, 2017
5. L. Ertaul, L.H. Encinas and E. El-Sheikh “Computer and Network Security Essentials”, Springer, 2017
6. X. He and H. Dai, “Dynamic Games for Network Security”, Springer, 2018
7. E. Maiwald, “Network Security”, Mc Graw Hill, 2013

8. FORENSICS and PENETRATION TESTING

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POST-GRADUATE (7)		
COURSE UNIT CODE	**CSCYB204**	**SEMESTER OF STUDY**	2nd
COURSE TITLE	**Computer Forensics and Penetration Testing**		
COURSEWORK BREAKDOWN		**TEACHING WEEKLY HOURS**	**ECTS Credits**
	Lectures	3	
	Tutorials	2	
		5	**8**
COURSE UNIT TYPE			
PREREQUISITES :	NONE		
LANGUAGE OF INSTRUCTION/EXAMS:	GREEK, ENGLISH		
MODULE WEB PAGE (URL)			

2.LEARNING OUTCOMES

Learning Outcomes

PART A
Windows penetration testing
This course teaches students the underlying principles and many of the tactics, techniques, procedures and tools associated with the penetration testing or ethical hacking.
Students will learn about the entire penetration testing process including planning, OSINT, reconnaissance, scanning, Vulnerability assessment, exploitation, post exploitation, and result reporting. The course will provide the fundamental information associated with each of the methods employed by most professionals.
PART B

Windows incident handling and forensics syllabus
The Windows OS Incident handling and Forensics course covers windows memory, registry, file system and application analysis. You will build an in-house forensic capability using a variety of free, open-source, and commercial tools.
Identify and handle digital artefact/evidence to answer critical questions, including application execution, file access, data theft, external device usage, file download, anti-forensics, and detailed system usage and Implement triage, live system analysis, and alternative acquisition techniques.
Compile reports and presents the findings during the digital forensics examination to the entity which was impacted by the cyberattack, or to the court for public investigation.
The objective of the course is to show students how to perform a fully digital forensic investigation of a Windows system.

General Skills

- Understanding the cyber threat and how cyber attackers operate.
- Understanding the tactics, techniques, procedures and tools used by penetration testers and red teams.
- Conducting a comprehensive penetration test assessment.
- Applying the cyber incident handling and response (IH&R) process.
- Conducting a comprehensive digital forensics investigation.

3. COURSE CONTENTS

The description contains the material to be covered during 13 lectures.

1. Introduction to Penetration Testing and Red Teaming
    a. What is a penetration test or red team assessment
    b. Penetration Test Methodology
    c. Penetration test Essentials Pre-engagement
    d. Scoping Ethical requirements and legal issues
    e. Penetration test report structure and components
    f. Building a Penetration Test lab
    g. Preparation, OSINT and anonymity infrastructure development.
2. Information Gathering
    a. Reconnaissance (DNS reconnaissance TCP, UDP, connections)
    b. OSINT (Open Source Intelligence)
    c. Scanning methodology
    d. System and network scanning, Scanning using nmap
3.vulnerability assessment
    a. Netcat
    b. Nessus
    c. OpenVas
4. Penetration test frameworks
    a. Metasploit
    b. Poshc2
    c. Covenant
    d. Mythic
5.Basics of windows security
    a. Windows internal security mechanisms
    b. Security policies
    c. Security software and devices
6. Gaining initial access
    a. Introduction to windows attacks
    b. Brute forcing
    c. Remote exploitation
    d. Client side attacks
    e. Phishing frameworks and attacks (Spear-phishing / phishing / stealing valid credentials)
7. Windows post exploitation techniques
    a. privilege escalation
    b. Lateral movement (Password Spraying, AV, EDR evasion)
    c. Powershel for penetration testers
    d. Active Directory Attacks (Kerberos Authentication, Domain enumeration, Domain attacks, Kerberoasting attack, Golden ticket, Pass the hash attack, pass the ticket, over pass the hash)
8. Incident handling process
    a. Introduction to the incident handling process
    b. Incident handling plan
9. Digital Forensics process
    a. Digital Forensics methodology
    b. Building a forensics analysis station.

c. Building a forensics lab.
10. Windows memory forensics
a. Memory Essentials
b. Dumping the memory
c. Memory analysis
11. Windows registry forensics
a. Registry Essentials
b. Getting the registry
c. Registry analysis
12. Windows file system forensics
a. Introduction to file system
b. Gathering file system relative to case information
c. File system analysis
d. Windows event log analysis
13. Windows application forensics
a. Browser Forensics
b. Email forensics
c. Usb forensics
d. How to compile a comprehensive report

4.TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	• Use of ICT in Course Teaching • Use of the Open eClass system, with uploaded notes, lectures, exercises for practice and communication with students.
	Method description / ***Semester Workload***
	Lectures: 39
	Tutorials: 26
	Research work: 50
	Self study: 70
	Total course hours (25 h workload per ECTS): ***200***
ASSESSMENT METHODS	I. A short case to analyse in class for 30 min (20%) and II. Research work (80%)

5.RESOURCES

Essential

- *The Hacker Playbook 3: Practical Guide To Penetration Testing by Peter Kim*
- *Incident Response with Threat Intelligence by Roberto Martínez*
- *Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 8 by Harlan Carvey*

Recommended

- *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry by Harlan Carvey*
- *Investigating Windows Systems 1st Edition, by Harlan Carvey*
- *File System Forensic Analysis 1st Edition by Brian Carrier*
- *Metasploit Penetration Testing Cookbook - Third Edition: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework 3rd Revised edition by Daniel Teixeira (Author), Abhinav Singh (Author), Monika Agarwal (Author)*
- *Penetration Tester's Open Source Toolkit 4th Edition, Kindle Edition by Jeremy Faircloth*

9. Cybersecurity Protocols and Standards

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POSTGRADUATE (7)		
MSc Program	CYBERSECURITY		
COURSE UNIT CODE	**CSCYB102**	**SEMESTER OF STUDY**	1st
COURSE TITLE	**Cybersecurity Protocols and Standards**		
COURSEWORK BREAKDOWN		**TEACHING WEEKLY HOURS**	**ECTS Credits**
	Lectures	3	
	Problem Solving- Research	2	
	Tutorials		
		5	**7**
COURSE UNIT TYPE	COMPULSORY		
PREREQUISITES :	NONE		
LANGUAGE OF INSTRUCTION/EXAMS:	GREEK, ENGLISH		
MODULE WEB PAGE (URL)	UNIWA Open eClass | ΚΑΝΟΝΕΣ και ΠΡΩΤΟΚΟΛΛΑ ΚΥΒΕΡΝΟΑΣ...		

2. LEARNING OUTCOMES

Learning Outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B Guidelines for writing Learning Outcomes*

Students can

- understand the purpose, scope, and importance of various standards
- memorize key terms, definitions, and foundational principles of cybersecurity standards. This level helps build a fundamental understanding of security concepts cybersecurity standards.
- analyze the structure, components, and requirements of cybersecurity standards
- Evaluate cybersecurity standards, considering their strengths, weaknesses, and relevance to specific organizational needs.
- Apply cybersecurity standards to real-world situations
- Describe, the methods used for a protocol launch
- Demonstrate, the ability to select the appropriate protocol

- Modify a protocol in order to update its contents
- Compare, similar protocols
- Develop from scratch a protocol with all the responsible committees
- Decide, on the protocol selection for a given task to undertake

General Skills

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology	*Project planning and management*
Adapting to new situations	*Respect for difference and multiculturalism*
Decision-making	*Respect for the natural environment*
Working independently	*Showing social, professional and ethical responsibility and sensitivity to gender issues*
Team work	*Criticism and self-criticism*
Working in an international environment	*Production of free, creative and inductive thinking*
Working in an interdisciplinary environment	*Others*
Production of new research ideas	

Recall basic facts and concepts related to cybersecurity standards
Use cybersecurity standards in specific contexts or scenarios
Examine and break down cybersecurity standards to understand their components.
Assess the effectiveness and appropriateness of cybersecurity standards Develop innovative solutions or strategies based on cybersecurity standards.
Comprehend the meaning and significance of cybersecurity standards.

3. COURSE CONTENTS

The description contains the material to be covered during the 13 sessions.

1) Description of Protocols and Standards
2) Leading Organisations in Cybersecurity protocols, The hierarchy in protocol production
3) BOT Basics, Automotive Protocols (e.g. FlexRay, SAE J2735)
4) Telecommunication Protocols
5) Cybersecurity Maritime Protocols and Standards, AI ethics code
6) FIPS
7) Governance Risk and Compliance (ERNEST YOUNG) and Trusted Computer Security
8) GDPR, Protection of Personal Data GRC ()
9) CERT, NIST, NIS, NERC
10) Common Criteria (ISO 15408) and Orange Book
11) Network protocols
12) Mobile Cybersecurity Protocols and standards
13) Hospital Cybersecurity protocols and standards

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	**Using interactive notes and slides to demonstrate the basic functionality of digital systems**
TEACHING METHODS	

Method description	*Semester Workload*
Lectures	39
Tutorials	26
Research work	50
Self study	60
Total course hours (25 h workload per ECTS)	***175***

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

5. RESOURCES

***Recommended Books**:*

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*

Webliography

https://www.itgovernanceusa.com/cybersecurity-standards

https://www.enisa.europa.eu

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αιγάλεω, 26 Ιανουαρίου 2024

Ο Πρύτανης

ΠΑΝΑΓΙΩΤΗΣ ΚΑΛΔΗΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

Το Εθνικό Τυπογραφείο αποτελεί δημόσια υπηρεσία υπαγόμενη στην Προεδρία της Κυβέρνησης και έχει την ευθύνη τόσο για τη σύνταξη, διαχείριση, εκτύπωση και κυκλοφορία των Φύλλων της Εφημερίδας της Κυβερνήσεως (ΦΕΚ), όσο και για την κάλυψη των εκτυπωτικών - εκδοτικών αναγκών του δημοσίου και του ευρύτερου δημόσιου τομέα (ν. 3469/2006/Α΄ 131 και π.δ. 29/2018/Α΄58).

1. ΦΥΛΛΟ ΤΗΣ ΕΦΗΜΕΡΙΔΑΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ (ΦΕΚ)

• Τα **ΦΕΚ σε ηλεκτρονική μορφή** διατίθενται δωρεάν στο **www.et.gr**, την επίσημη ιστοσελίδα του Εθνικού Τυπογραφείου. Όσα ΦΕΚ δεν έχουν ψηφιοποιηθεί και καταχωριστεί στην ανωτέρω ιστοσελίδα, ψηφιοποιούνται και αποστέλλονται επίσης δωρεάν με την υποβολή αίτησης, για την οποία αρκεί η συμπλήρωση των αναγκαίων στοιχείων σε ειδική φόρμα στον ιστότοπο www.et.gr.

• Τα **ΦΕΚ σε έντυπη μορφή** διατίθενται σε μεμονωμένα φύλλα είτε απευθείας από το Τμήμα Πωλήσεων και Συνδρομητών, είτε ταχυδρομικά με την αποστολή αιτήματος παραγγελίας μέσω των ΚΕΠ, είτε με ετήσια συνδρομή μέσω του Τμήματος Πωλήσεων και Συνδρομητών. Το κόστος ενός ασπρόμαυρου ΦΕΚ από 1 έως 16 σελίδες είναι 1,00 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,20 €. Το κόστος ενός έγχρωμου ΦΕΚ από 1 έως 16 σελίδες είναι 1,50 €, αλλά για κάθε επιπλέον οκτασέλιδο (ή μέρος αυτού) προσαυξάνεται κατά 0,30 €. Το τεύχος Α.Σ.Ε.Π. διατίθεται δωρεάν.

• **Τρόποι αποστολής κειμένων προς δημοσίευση:**

Α. Τα κείμενα προς δημοσίευση στο ΦΕΚ, από τις υπηρεσίες και τους φορείς του δημοσίου, αποστέλλονται ηλεκτρονικά στη διεύθυνση **webmaster.et@et.gr** με χρήση προηγμένης ψηφιακής υπογραφής και χρονοσήμανσης.

Β. Κατ’ εξαίρεση, όσοι πολίτες δεν διαθέτουν προηγμένη ψηφιακή υπογραφή μπορούν είτε να αποστέλλουν ταχυδρομικά, είτε να καταθέτουν με εκπρόσωπό τους κείμενα προς δημοσίευση εκτυπωμένα σε χαρτί στο Τμήμα Παραλαβής και Καταχώρισης Δημοσιευμάτων.

• Πληροφορίες, σχετικά με την αποστολή/κατάθεση εγγράφων προς δημοσίευση, την ημερήσια κυκλοφορία των Φ.Ε.Κ., με την πώληση των τευχών και με τους ισχύοντες τιμοκαταλόγους για όλες τις υπηρεσίες μας, περιλαμβάνονται στον ιστότοπο (www.et.gr). Επίσης μέσω του ιστότοπου δίδονται πληροφορίες σχετικά με την πορεία δημοσίευσης των εγγράφων, με βάση τον Κωδικό Αριθμό Δημοσιεύματος (ΚΑΔ). Πρόκειται για τον αριθμό που εκδίδει το Εθνικό Τυπογραφείο για όλα τα κείμενα που πληρούν τις προϋποθέσεις δημοσίευσης.

2. ΕΚΤΥΠΩΤΙΚΕΣ - ΕΚΔΟΤΙΚΕΣ ΑΝΑΓΚΕΣ ΤΟΥ ΔΗΜΟΣΙΟΥ

Το Εθνικό Τυπογραφείο ανταποκρινόμενο σε αιτήματα υπηρεσιών και φορέων του δημοσίου αναλαμβάνει να σχεδιάσει και να εκτυπώσει έντυπα, φυλλάδια, βιβλία, αφίσες, μπλοκ, μηχανογραφικά έντυπα, φακέλους για κάθε χρήση, κ.ά.

Επίσης σχεδιάζει ψηφιακές εκδόσεις, λογότυπα και παράγει οπτικοακουστικό υλικό.

Ταχυδρομική Διεύθυνση: Καποδιστρίου 34, τ.κ. 10432, Αθήνα	Ιστότοπος: **www.et.gr**
ΤΗΛΕΦΩΝΙΚΟ ΚΕΝΤΡΟ: 210 5279000 - fax: 210 5279054	Πληροφορίες σχετικά με την λειτουργία του ιστότοπου: **helpdesk.et@et.gr**
ΕΞΥΠΗΡΕΤΗΣΗ ΚΟΙΝΟΥ **Πωλήσεις - Συνδρομές:** (Ισόγειο, τηλ. 210 5279178 - 180) **Πληροφορίες:** (Ισόγειο, Γρ. 3 και τηλεφ. κέντρο 210 5279000) **Παραλαβή Δημ. Ύλης:** (Ισόγειο, τηλ. 210 5279167, 210 5279139)	Αποστολή ψηφιακά υπογεγραμμένων εγγράφων προς δημοσίευση στο ΦΕΚ: **webmaster.et@et.gr**
Ωράριο για το κοινό: Δευτέρα ως Παρασκευή: 8:00 - 13:30	Πληροφορίες για γενικό πρωτόκολλο και αλληλογραφία: **grammateia@et.gr**

Πείτε μας τη γνώμη σας,

για να βελτιώσουμε τις υπηρεσίες μας, συμπληρώνοντας την ειδική φόρμα στον ιστότοπό μας.

0200878070224007 2