Τίτλος μαθήματος	Ασφάλεια πληροφοριών				
Κωδικός μαθήματος	DIS504				
Τύπος μαθήματος	Επιλεγόμενο				
Επίπεδο	Μεταπτυχιακές σπουδές				
Έτος / Εξάμηνο	1ο / 2ο				
ECTS	7.5	**Διαλέξεις / εβδομάδα**	1	**Εργαστήρια / εβδομάδα**	-
Σκοπός και στόχοι του μαθήματος	Στη σύγχρονη εποχή της τεχνολογίας των πληροφοριών, η ασφάλεια των πληροφοριών είναι υψίστης σημασίας. Οι οργανισμοί σε όλο τον κόσμο δίνουν μεγαλύτερη σημασία στη διασφάλιση των πληροφοριακών τους συστημάτων και αυτό έχει αυξήσει δραστικά την ανάγκη για επαγγελματίες στον τομέα της ασφάλειας πληροφοριών. Η προστασία ευαίσθητων δεδομένων δεν σημαίνει πλέον μόνο την προστασία των δεδομένων, αλλά περιλαμβάνει επίσης την προστασία διαφόρων συστημάτων, τον έλεγχο των κινδύνων, τις νομικές ενέργειες και την αντιμετώπιση ενεργών προσπαθειών παραβίασης. Το μάθημα Ασφάλειας Πληροφοριών (DIS504) καλύπτει τα πάντα, από την πολιτική έως τη νομοθεσία, ενσωματώνοντας προηγμένες τεχνικές δεξιότητες με διοικητικές έννοιες. Το μάθημα θα εξοικειώσει τους φοιτητές με τη διακυβέρνηση της ασφάλειας πληροφοριών όχι μόνο στις τεχνικές πτυχές της, όπως η κρυπτογραφία, ο έλεγχος πρόσβασης, η ανίχνευση εισβολών, οι επιθέσεις άρνησης παροχής υπηρεσιών, ο μετριασμός και η εγκληματολογία, αλλά και στις διαχειριστικές και νομικές πτυχές. Το μάθημα αυτό αποσκοπεί στην εξασφάλιση επάρκειας στην προστασία των πληροφοριακών συστημάτων, ενώ παράλληλα παρέχει στους σπουδαστές τις κατάλληλες δεξιότητες στην αξιολόγηση κινδύνων, τη νομική συμμόρφωση, τα ηθικά ζητήματα και την εγκληματολογική έρευνα στην επιστήμη των υπολογιστών. Οι φοιτητές, επομένως, θα κατανοήσουν πώς να σχεδιάζουν, να αναπτύσσουν, να υλοποιούν και να διαχειρίζονται πολύπλευρα συστήματα ασφαλείας σε διάφορα πρακτικά πλαίσια μετά την παρακολούθηση αυτού του μαθήματος. Οι φοιτητές θα τείνουν να σκέφτονται κριτικά για τα σύγχρονα ζητήματα ασφάλειας με τη βοήθεια διαδραστικών διαλέξεων, μελετών περιπτώσεων, εργασιών και συζητήσεων. Στόχος του μαθήματος είναι η ανάπτυξη αποφοίτων με καλές τεχνικές δεξιότητες και την ικανότητα να ηγούνται και να διαχειρίζονται λειτουργίες ασφάλειας σε οποιονδήποτε οργανισμό. Το				

	DIS504 συνδυάζει τη θεωρία και την πρακτική, έτσι ώστε οι φοιτητές να είναι πλήρως εξοπλισμένοι για να προωθήσουν την πρακτική της ασφάλειας πληροφοριών. Οι στόχοι του μαθήματος είναι: • Παροχή των βασικών αρχών της ασφάλειας πληροφοριών. • Παρουσιάστε τις απειλές και τις επιθέσεις στις πληροφορίες και τους τρόπους προστασίας των πληροφοριών από τις επιθέσεις αυτές. • Εξετάστε συγκεκριμένους τεχνικούς τομείς της ασφάλειας πληροφοριών, όπως η πιστοποίηση ταυτότητας, ο έλεγχος πρόσβασης, η άρνηση παροχής υπηρεσιών, τα συστήματα ανίχνευσης και πρόληψης εισβολών και, τέλος, οι κρυπτογραφικοί αλγόριθμοι. • Αφορά τις διαχειριστικές πτυχές της ασφάλειας των πληροφοριών και ειδικότερα τις διαχειριστικές πρακτικές που σχετίζονται με τη διαχείριση των κινδύνων. • Συζητήστε τα νομικά και ηθικά ζητήματα που απαντώνται συνήθως στους σημερινούς οργανισμούς. • Παρουσιάστε την εγκληματολογία υπολογιστών και πώς μπορούμε να βρούμε αποδεικτικά στοιχεία.
Μαθησιακά αποτελέσματα	Μετά την ολοκλήρωση του μαθήματος οι μαθητές αναμένεται να: O[1] Εξηγήστε τις προκλήσεις και το πεδίο εφαρμογής της ασφάλειας πληροφοριών, O[2] Προσδιορίστε τις κοινές απειλές που αντιμετωπίζουν σήμερα, O[3] Περιγράψτε τον μηχανισμό ελέγχου πρόσβασης που χρησιμοποιείται για την αυθεντικοποίηση και την εξουσιοδότηση των χρηστών, O[4] Να κατανοήσουν τη σημασία των κρυπτογραφικών αλγορίθμων που χρησιμοποιούνται στην ασφάλεια των πληροφοριών, O[5] Εξηγήστε τη χρήση εργαλείων ασφαλείας όπως τα τείχη προστασίας και τα συστήματα πρόληψης εισβολών, O[6] Αναγνωρίστε τη σημασία της φυσικής ασφάλειας και συζητήστε τρόπους βελτίωσης της φυσικής ασφάλειας μιας επιχείρησης, O[7] Διασφάλιση της ασφάλειας των υποδομών και του δικτύου, O[8] Εξετάστε και επιλύστε νομικά και ηθικά ζητήματα,

	O[9] Ενισχύστε τις δεξιότητες κριτικής σκέψης και ανάλυσης μέσω της χρήσης μελετών περιπτώσεων, ερευνητικών εργασιών και ασκήσεων σε μικρές ομάδες. O[10] Ενίσχυση των δεξιοτήτων έρευνας, συγγραφής και παρουσίασης.

1. Γνώση	C.L.O.[1] **Περιγράψτε** τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[2] **Αναλύστε** τα νομικά και ηθικά ζητήματα που απαντώνται συνήθως στους σημερινούς οργανισμούς. C.L.O.[3] **Συζητήστε** την εγκληματολογία υπολογιστών.
2. Δεξιότητες	C.L.O.[4] **Χρησιμοποιούν** συγκεκριμένες τεχνικές πτυχές της ασφάλειας των πληροφοριών, όπως η αυθεντικοποίηση, ο έλεγχος πρόσβασης , η άρνηση παροχής υπηρεσιών, τα συστήματα ανίχνευσης και πρόληψης επιθέσεων και, τέλος, οι κρυπτογραφικοί αλγόριθμοι. C.L.O.[5] **Πρακτική εξάσκηση** στις πτυχές της διαχείρισης της ασφάλειας των πληροφοριών και, πιο συγκεκριμένα, στις πρακτικές που σχετίζονται με τη διαχείριση των κινδύνων.
3. Ικανότητες	C.L.O.[6] **Δημιουργία** τρόπων προστασίας από επιθέσεις πληροφοριών και οποιεσδήποτε άλλες απειλές.
(Ευθύνη και αυτονομία)	C.L.O.[7] **Προτείνετε** τρόπους εύρεσης αποδεικτικών στοιχείων που σχετίζονται με την εγκληματολογία υπολογιστών.

Προαπαιτούμενα	Κανένα	**Απαιτούμενο**	Κανένα
Περιεχόμενο μαθήματος	1η εβδομάδα: Εισαγωγή στην Ασφάλεια Πληροφοριών. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. 2η εβδομάδα: Επιθέσεις και απειλές. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[6] - Δημιουργία τρόπων προστασίας από επιθέσεις σε πληροφορίες και οποιεσδήποτε άλλες απειλές.		

	3η εβδομάδα: Επιθέσεις άρνησης παροχής υπηρεσιών. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, όπως η άρνηση εξυπηρέτησης. C.L.O.[6] - Δημιουργία τρόπων προστασίας από επιθέσεις πληροφοριών και οποιεσδήποτε άλλες απειλές. 4η εβδομάδα: Συστήματα ανίχνευσης και πρόληψης εισβολών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, συμπεριλαμβανομένων των συστημάτων ανίχνευσης και πρόληψης επιθέσεων. C.L.O.[6] - Δημιουργία τρόπων προστασίας από επιθέσεις πληροφοριών και οποιεσδήποτε άλλες απειλές. 5η εβδομάδα: Εβδομάδα: Βασική κρυπτογραφία. C.L.O.[1] - Περιγραφή των θεμελιωδών στοιχείων της ασφάλειας των πληροφοριών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, συμπεριλαμβανομένων των κρυπτογραφικών αλγορίθμων. 6η εβδομάδα: Θεμελιώδεις αρχές ελέγχου πρόσβασης. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, όπως ο έλεγχος πρόσβασης. 7η εβδομάδα: Έλεγχος ταυτότητας χρήστη. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, όπως ο έλεγχος ταυτότητας. 8η εβδομάδα: Φυσική ασφάλεια. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[6] - Δημιουργία τρόπων προστασίας από επιθέσεις σε πληροφορίες και οποιεσδήποτε άλλες απειλές. 9η εβδομάδα: Διαχείριση κινδύνων. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[5] - Εξάσκηση στις πτυχές της διαχείρισης της ασφάλειας πληροφοριών, συμπεριλαμβανομένης της διαχείρισης κινδύνων. 10η εβδομάδα: Ασφάλεια δικτύων. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[4] - Χρήση συγκεκριμένων τεχνικών πτυχών της ασφάλειας πληροφοριών, όπως τα πρωτόκολλα ασφάλειας δικτύων. C.L.O.[6] - Δημιουργία τρόπων προστασίας από επιθέσεις σε πληροφορίες και οποιεσδήποτε άλλες απειλές.

	11η εβδομάδα: Εβδομάδα: Νομικά και ηθικά ζητήματα στην ασφάλεια πληροφοριών. C.L.O.[2] - Αναλύστε τα νομικά και ηθικά ζητήματα που συναντώνται συνήθως στους σημερινούς οργανισμούς. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών 12η εβδομάδα: Εβδομάδα: Εισαγωγή στην εγκληματολογία. C.L.O.[3] - Συζήτηση για την εγκληματολογία υπολογιστών. C.L.O.[7] - Πρόταση τρόπων εύρεσης αποδεικτικών στοιχείων που σχετίζονται με την εγκληματολογία υπολογιστών. 13η εβδομάδα: Επανάληψη. C.L.O.[1] - Περιγράψτε τα θεμελιώδη στοιχεία της ασφάλειας των πληροφοριών. C.L.O.[3] - Συζητήστε την εγκληματολογία υπολογιστών. C.L.O.[5] - Πρακτικές πτυχές της διαχείρισης της ασφάλειας των πληροφοριών. C.L.O.[7] - Να προτείνει τρόπους εύρεσης αποδεικτικών στοιχείων που σχετίζονται με την εγκληματολογία υπολογιστών.
Μεθοδολογία διδασκαλίας	Μείγμα διαδραστικών διαλέξεων, τεχνικών ενεργητικής μάθησης και δραστηριοτήτων. Πιο συγκεκριμένα: • Διαδραστικές διαλέξεις • Σημειώσεις και παρουσιάσεις PowerPoint σε ψηφιακή μορφή μέσω της ηλεκτρονικής πλατφόρμας • Βασικά εγχειρίδια και πρόσθετη βιβλιογραφία • Αναθέσεις • Διαδραστικές δραστηριότητες • Συζητήσεις σε φόρουμ μέσω της ηλεκτρονικής πλατφόρμας πραγματικών περιπτωσιολογικών μελετών • Σύνδεσμοι στο διαδίκτυο • Κριτικός προβληματισμός σχετικά με ερευνητικό άρθρο • Αξιολόγηση από ομότιμους για την ομαδική εργασία και συζήτηση στο φόρουμ • Εκπαιδευτικά βίντεο για μελέτες περιπτώσεων του πραγματικού κόσμου και κριτική συζήτηση στο φόρουμ
Βιβλιογραφία	Υποχρεωτική βιβλιογραφία • W. Stallings, L. Brown, Computer Security Principles and Practice, 4η έκδοση, 2018, Pearson • Wenliang Du, Ασφάλεια Υπολογιστών και Διαδικτύου: Χειροπιαστή Προσέγγιση

<table>
<tr><td></td><td>

- Michael E. Whitman, Principles of Information Security, 6η έκδοση, 2018

Πρόσθετη βιβλιογραφία

- Yang, J., Chen, Y.-L., Por, L.Y., Ku, C.S. Συστηματική βιβλιογραφική ανασκόπηση της ασφάλειας πληροφοριών στα chatbots. Appl. Sci. 2023, 13, 6355. https://doi.org/10.3390/app13116355.
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Απειλές και τρωτά σημεία της ασφάλειας στον κυβερνοχώρο: Μια συστηματική μελέτη χαρτογράφησης. Arabian Journal for Science and Engineering, 45(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2.
-

</td></tr>
<tr><td>Αξιολόγηση</td><td>

5% Κουίζ
20% Έργα/Αναθέσεις
10% Αξιολόγηση από ομότιμους
5% Προφορική παρουσίαση
60% Τελικές εξετάσεις

Μέθοδοι αξιολόγησης και αντιστοίχιση με τα μαθησιακά αποτελέσματα

	Ποσοστό	Ο1	Ο2	Ο3	Ο4	Ο5	Ο6	Ο7	Ο8	Ο9	Ο10
Κουίζ	5%	√	√			√			√		
Έργα / Εργασίες	20%			√	√		√	√			√
Αξιολόγηση από ομότιμους	10%			√	√		√	√		√	√
*Προφορική παρουσίαση	5%									√	√
Τελική εξέταση	60%	√	√	√	√	√			√		

*Προφορική παρουσίαση μιας σύγχρονης ερευνητικής εργασίας ή μιας μελέτης περίπτωσης στον τομέα της "Ασφάλειας Πληροφοριών". Ο κατάλογος των εργασιών ή των μελετών περίπτωσης θα ανακοινωθεί κατά τη διάρκεια της εβδομάδας 4.

</td></tr>
<tr><td>Γλώσσα</td><td>Αγγλικά</td></tr>
</table>