|  |  |
| --- | --- |
| unipi-logo | Πανεπιστήμιο Πειραιώς, Τμήμα ΠληροφορικήςΘέματα Πτυχιακών Εργασιών  |

**Προ-απαιτούμενα ανάληψης πτυχιακής:**

1. Να έχετε συμπληρώσει με επιτυχία τα 2/3 των μαθημάτων
2. Να έχετε πάνω από 8 στα μαθήματα ασφάλειας, διοίκηση ασφάλειας, πληροφορική στην ναυτιλία
3. Να έχετε proficiency

**ΘΕΜΑ A:**

1. Αναλύστε τα πρότυπα (πχ ISO2800, NIST), μεθοδολογίες (νομικά πλαίσια (π.χ. NIST directive, BMCO/IMO cybersecurity guidelines) και ευρωπαϊκά έργα για την Διαχείρισης Ασφάλειας και Αξιολόγησης Επικινδυνότητας για εφοδιαστικές αλυσίδες (supply chains).
2. Μοντελοποιείστε μια υπηρεσία προμηθευτικής αλυσίδας (π.χ. διαχείριση φορτίων, μεταφορά εμπορευμάτων) χρησιμοποιώντας κάποιο εργαλείο μοντελοποίησης της επιλογής σας (π.χ. Draw.io και online και σαν app desktop).
3. Δημιουργείστε ένα διαδραστικό ερωτηματολόγιο (π.χ. <https://security.uci.edu/security-plan/plan-resources.html>) που να υπολογίζει το επίπεδο κινδύνων σε μια εφοδιαστική αλυσίδα.

**ΘΕΜΑ Β:**

1. Ποιες είναι οι απειλές (φυσικές, cyber, υβριδικές, γεωπολιτικές, βιολογικές) που αντιμετωπίζει το περιβάλλον (αέρας, θάλασσα, ωκεανοί, λίμνες, βιοποικιλότητα). Παραθέστε όλες τις απειλές) ? Τι τεχνολογικά αντίμετρα μπορούμε να πάρουμε για την προστασία το περιβάλλοντος για κάθε απειλή ? (πηγές π.χ. Global Industry Alliance (GIA) for Marine Biosafety).
2. Αναδρομή των κυρίων ευρωπαϊκών ερευνητικών έργων και αποτελεσμάτων τους που αφορούν την προστασία του περιβάλλοντος με τεχνολογικά μέσα.
3. Μελετήστε και αναλύστε όλες τις διεθνείς, Ευρωπαϊκές και εθνικές Οδηγίες και νομοθετικά πλαίσια στο θέμα αυτό (π.χ. Green Deal).
4. Δημιουργείστε ένα περιβαλλοντικό υπολογιστή (π.χ. ένα διαδραστικό ερωτηματολόγιο όπως. <https://security.uci.edu/security-plan/plan-resources.html>) που να υπολογίζει το επίπεδο περιβαλλοντικών κινδύνων σε μια υποδομή (ένα Δήμο ή Πόλη ή Χωριό η Κοινότητα ή λιμάνι) (επιλέξτε μια υποδομή).
5. **ΘΕΜΑ Γ:**

**Α**. Η πιστοποίηση ψηφιακών προϊόντων (software,hardware, σύστημα, η-υπηρεσία) προϋποθέτει την ανάλυση (τεχνικών) απειλών, ευπαθειών και κινδύνων και χρησιμοποιούνται στην διαδικασία αυτή διάφορα διεθνή πρότυπα, όπως:

* [ISO/IEC 15408-1/2/3:2005](http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm) (COMMON CRITERIA) - Information technology — Security techniques — Evaluation criteria for IT security —
* ISO/IEC 18045:2005 - Information technology -- Security techniques -- Methodology for IT security evaluation
* ISO/IEC 17065:2012 -Conformity assessment — Requirements for bodies certifying products, processes and services

Αναλύστε τα παραπάνω πρότυπα (ως προς την χρήση, σκοπό, στόχο, βήματα που προτείνουν ).

**Β.** Φτιάξτε ένα δια-δραστικό ή -πίνακα με όλους τους τεχνικούς όρους που εμφανίζονται στα παραπάνω πρότυπα μαζί με τους ορισμούς.

**Γ.** Η Ευρωπαϊκή Επιτροπή δημοσίευσε το ευρωπαϊκό σχήμα EUCC (<https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>). Αναλύστε το σχήμα και εξηγείστε την σχέση του με τα παραπάνω πρότυπα.

**Δ.** Επιλέξτε ένα ψηφιακό προϊόν (π.χ. software, hardware, υπηρεσία, διαδικασία) και εκτιμήστε τους κινδύνους σύμφωνα με το ISO15048 η με χρήση μεθοδολογίας που υλοποιεί το πρότυπο (πχ ISO18045).

**ΘΕΜΑ Δ:**

Για την ασφαλή λειτουργία ενός οργανισμού είναι πολύ σημαντική η διαχείριση ασφάλειας των πληροφοριακών του συστημάτων. Επισημαίνεται ότι η διαχείριση ασφάλειας αποτελεί ένα σημαντικό έργο πληροφορικής για κάθε οργανισμό.

Επιλέξτε ένα οργανισμό/εταιρεία/φορέα που φιλοξενεί πληροφοριακό σύστημα και αναπτύξτε

1. Μελέτη Ανάλυσης και Διαχείρισης Επικινδυνότητας η οποία θα πρέπει να περιλαμβάνει:

* Περιγραφή της Μεθοδολογίας
* Περιγραφή του Οργανισμού/ Εταιρίας/ Φορέα /Υπηρεσίας
* Απαιτήσεις Ασφάλειας - Νομικές Απαιτήσεις
* Χαρτογράφηση ΠΣ / αγαθών  (Cartography) και χρηστών
* Αποτίμηση Επιπτώσεων (Impact Assessment)
* Αποτίμηση Απειλών (φυσικών, ψηφιακών, ανθρώπινων) (Threat Assessment)
* Αποτίμηση Αδυναμιών (Vulnerability Assessment)
* Αποτίμηση Κινδύνων (Risk Analysis)
* Προτεινόμενα Μέτρα Προστασίας (Proposed Security Countermeasures) (τεχνικών και μη-τεχνικών)
* Σχέδιο Υλοποίησης Μέτρων Προστασίας (Risk Treatment Plan)

2. Κατανομή οργανωτικών δομών και αρμοδιοτήτων ασφάλειας (Security Roles and Responsibilities)

3. Βασικές Πολιτικές Ασφάλειας (Access Control Policy, Password Policy, Logging Policy, Backup Policy)

4. Βασικές Διαδικασίες (Διαδικασία αντιμετώπισης περιστατικών ασφάλειας, Διαδικασία Backup, Διαδικασία Δημιουργίας / Διαγραφής Χρήστη)

5. Σχέδιο Επιχειρησιακής Συνέχειας

Για την υλοποίηση της εργασίας μπορείτε να χρησιμοποιήσετε εργαλεία της επιλογής σας.

**ΘΕΜΑ Ε.**

Για την ασφαλή λειτουργία ενός οργανισμού είναι πολύ σημαντική η δημιουργία ενός ηλεκτρονικού συστήματος ασφάλειας (Information Security Management System- ISMS)

Επιλέξτε ένα οργανισμό/εταιρεία/φορέα που φιλοξενεί πληροφοριακό σύστημα και αναπτύξτε ένα σύστημα ISMS χρησιμοποιώντας όποια ανοιχτή πλατφόρμα (π.χ. Liferay, WordPress), εργαλείο ή γλώσσα προγραμματισμού επιθυμείτε. Το ISMS πρέπει να είναι συμβατό με τα πρότυπα ISO2700x και να παρέχει υπηρεσίες διαχείρισης ασφάλειας όπως :

* Χαρτογράφηση ΠΣ / αγαθών  (Cartography)
* Αποτίμηση Επιπτώσεων (Impact Assessment)
* Αποτίμηση Απειλών (Threat Assessment)
* Αποτίμηση Αδυναμιών (Vulnerability Assessment)
* Αποτίμηση Κινδύνων (Risk Analysis)
* Βιβλιοθήκη αντιμέτρων (Control list)

**ΘΕΜΑ Z.**

Ο covid-19 επέβαλε μια απότομη αλλαγή στο τρόπο που οι άνθρωποι δουλεύουνε. Ο περιορισμός των μετακινήσεων και η υποχρεωτική κοινωνική απόσταση μας αναγκάζει να αυξήσουμε:

* τις ηλεκτρονικές συναλλαγές μας (η-υγεία/η-τραπεζιτική/η-εμπόριο/τηλε-εκπαίδευση)
* χρήση εργαλείων τηλε-διασκέψεις / τηλε-εκπαίδευση
* χρήση συνεργατικών εργαλείων (π.χ. GSuite vs Word, remote productivity tracking tools )
* την η-ψυχαγωγία μας (Video/Music Streaming, Online Gaming)
1. Αναλύστε την αρχιτεκτονική 2 δημοφιλών η υπηρεσιών στην περίοδο του lockdown (π.χ. τηλ-εκπαίδευση, η-τραπεζιτική, …) ως προς τις διαδικασίες, ψηφιακά αγαθά που χρησιμοποιούνται.
2. Ποιες είναι οι απειλές ασφάλειας και κυβερνο-επιθέσεις των παραπάνω υπηρεσιών και εργαλείων που έχουν ανακοινωθεί?
3. Ποια αντίμετρα ασφάλειας πρέπει να έχουν εγκαταστήσει οι πάροχοι των υπηρεσιών η οι κατασκευαστές των εργαλείων ώστε να υπάρχει η αδιάλειπτη, συνεχής, ποιοτική χρήση τους ?
4. To JITSI <https://github.com/jitsi> είναι ένα video conferencing tool ανοιχτού κώδικα, χρησιμοποιείστε το εργαλείο CodeWeTrust <https://www.codewetrust.com> ή SNYK https://github.com/snyk ώστε να αξιολογήσετε το JITSI ως προς τους επιχειρηματικούς κινδύνους (π.χ. νομική συμβατότητα, επιχειρηματική φήμη, συμβατότητα με πρότυπα) και ευπάθειες (vulnerabilities).
5. Υπάρχουν διάφορα πρότυπα και βέλτιστες πρακτικές για την αξιολόγηση λογισμικού. Βάση κάποιου προτύπου/βέλτιστη πρακτική αξιολογείστε το εργαλείο SNYK

**Ημερομηνία παράδοσης**

Το κείμενο που θα παραδώσετε θα πρέπει να έχει έκταση μέχρι 50 σελίδες μεγέθους Α4 (γραμματοσειρά TimesNewRoman 12pt, κενό μεταξύ γραμμών 1.5 lines). Σε περίπτωση που χρειαστεί να προσθέσετε επιπλέον κείμενο, θα πρέπει να το κάνετε χρησιμοποιώντας παραρτήματα. Ο κώδικας θα είναι μέρος του παραδοτέου (url, USB, cloud,…). Η παρουσίαση θα πρέπει να έχει έκταση μέχρι 20 διαφάνειες.

 **Απορίες σχετικά με την εργασία**

Για οποιαδήποτε απορία σχετικά με τα θέματα μπορείτε να απευθύνεστε στην διδάσκουσα dpolemi@unipi.gr ή μέσω της σελίδας του μαθήματος στην πλατφόρμα e-class.

**Ζητήματα δεοντολογίας και Πολιτικής**

Η χρήση περιεχομένου που παράγεται από την τεχνητή νοημοσύνη (ΤΝ) (συμπεριλαμβανομένου αλλά όχι περιοριστικά κειμένου, σχημάτων, εικόνων και κώδικα) θα πρέπει να συνοδεύεται με βιβλιογραφική αναφορά ή με υποσημείωση. Το ΤΝ σύστημα που χρησιμοποιήθηκε θα πρέπει να επισημαίνεται, και συγκεκριμένες ενότητες του άρθρου που χρησιμοποιούν περιεχόμενο που παράγεται από την ΤΝ θα πρέπει να επισημαίνονται και να συνοδεύονται από μια σύντομη εξήγηση σχετικά με το επίπεδο στο οποίο το σύστημα ΤΝ χρησιμοποιήθηκε για τη δημιουργία του περιεχομένου.

Είναι προφανές ότι η βαθμολογία πρέπει να αντικατοπτρίζει το επίπεδο της γνώσης που αποκόμισε ο φοιτητής μέσα από τη μελέτη των ερευνητικών εργασιών και κατάφερε να μεταφέρει αυτή τη γνώση στην εργασία. Για να εξασφαλιστεί όσο είναι δυνατό η παραπάνω αρχή, σε περίπτωση βεβαιωμένης αντιγραφής οι εμπλεκόμενες εργασίες μηδενίζονται.