Πρώτο Μέρος Εκπαίδευσης: ΤΟ ΣΥΓΧΡΟΝΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Ενότητα 1: Εισαγωγή στο Διαδίκτυο και στο Κυβερνοέγκλημα

·      Διαδίκτυο/Internet. Τεχνική περιγραφή και τρόπος λειτουργίας - Θεωρητικά θέματα

·      Βασικές υπηρεσίες Διαδικτύου. Το περιβάλλον λειτουργίας του Διαδικτύου

·      Χρησιμότητα Κυβερνοχώρου

·      Σκοπός εισηγήσεων

·         Έννοια χρησιμοποιούμενων όρων

·         Γενικά αποδεκτό περιεχόμενο των χρησιμοποιούμενων τεχνικών όρων/ εννοιών

·         Διαχείριση Ιστότοπων

·         Ονόματα Χώρου (Domain Names)

·         Τι είναι η ιστοσελίδα – Τι είναι το ιστολόγιο

·         Τι είναι το Κυβερνοέγκλημα

·         Mορφές ΚυβερνοεγκλημάτωνHackers και crackers (Διαφορές αυτών)

·         Μετάλλαξη Εγκλήματος

·         Νομικοί Τρόποι Προσέγγισης Ηλεκτρονικών Εγκλημάτων

·         Φαινόμενα Εποχής (CyberBullying – CyberAddiction)

2 ώρες

Ενότητα 3: Κατάχρηση δυνατοτήτων του Κυβερνοχώρου - Σε τι κινδύνους μας εκθέτει η «δικτύωση»

•             Αρνητική πλευρά Κυβερνοχώρου - Κατάχρηση δυνατοτήτων του

•             Κατάχρηση δυνατοτήτων του Κυβερνοχώρου στην πράξη - Τεχνικά θέματα

•             Περιγραφή των αθέμιτων, ζημιογόνων και ποινικά κολάσιμων συμπεριφορών που εκτελούνται/εμφανίζονται στον Kυβερνοχώρο -Τυπολογία/Μορφές Κυβερνοεγκλημάτων

•             Τεχνικά χαρακτηριστικά και ιδιότητες που παρουσιάζει η ψηφιακή εγκληματικότητα

•             Δυσχέρειες στην διερεύνηση και την διαλεύκανση Κυβερνοεγκλήματος

•             Υπηρεσίες & Φορείς με αρμοδιότητα το Έγκλημα στον Κυβερνοχώρο και την Ψηφιακή Εγκληματικότητα

•             Νέες τάσεις και προκλήσεις στο Κυβερνοέγκλημα

•             Ψηφιακά νομίσματα (cryptocurrencies) (Bitcoin, Ethereum κ.α.) και Τεχνολογία Blockchain -Νομική και Τεχνολογική προσέγγιση

•             Deepweb – Darkweb (σύντομη παρουσίαση)

2 ώρες,

Δεύτερο Μέρος Εκπαίδευσης– ΟΥΣΙΑΣΤΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ενότητα 1: Γνήσια Κυβερνοεγκλήματα

Παράνομη πρόσβαση σε πληροφοριακό σύστημα – άρθρο  370Γ ΠΚ

Παραβίαση απορρήτων υπολογιστών – άρθρο  370Β ΠΚ

2 ώρες

Απάτη με υπολογιστή -  - άρθρο 386Α ΠΚ

2 ώρες

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων – άρθρο 292Β ΠΚ

2 ώρες

Ενότητα 2: Εγκλήματα κατά της σεξουαλικής ελευθερίας και ανηλικότητας, τελούμενα μέσω Διαδικτύου

Πορνογραφία ανηλίκων

3 ώρες

Άλλα σεξουαλικά εγκλήματα κατά ανηλίκων: προσβολή της αιδούς των ανηλίκων στο διαδίκτυο, προσέλκυση παιδιών για γενετήσιους λόγους, προσβολή της γενετήσιας αξιοπρέπειας στο ψηφιακό περιβάλλον, πορνογραφικές παραστάσεις ανηλίκων

3 ώρες

Ειδικές μορφές κυβερνοεγκλημάτων: διαδικτυακή παρενόχληση, ρητορική μίσους, πρόκληση βλάβης με συνεχή σκληρή συμπεριφορά, έμφυλη βία στο διαδίκτυο

4 ώρες

Ενότητα 3: Μη γνήσια κυβερνοεγκλήματα

Ποινική προστασία προσωπικών δεδομένων

2 ώρες

Ποινική προστασία πνευματικής ιδιοκτησίας στον Κυβερνοχώρο – Διαδικτυακές προσβολές πνευματικής Ιδιοκτησίας

2 ώρες

Τρίτο Μέρος Εκπαίδευσης – ΔΙΕΡΕΥΝΗΣΗ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΗ ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

Ενότητα 1:Διερεύνηση Κυβερνοεγκλημάτων – Τεχνικές και Διαδικασίες έρευνας

•             Έρευνες στον Κυβερνοχώρο꞉ Μέθοδοι συλλογής ψηφιακών αποδείξεων και τεκμήριων  στον Κυβερνοχώρο για την βεβαίωση των εγκλημάτων και την αποκάλυψη της ταυτότητας των δραστών.

•             Συλλογή, έρευνα και ανάλυση ηλεκτρονικών ιχνών στο Διαδίκτυο

2ώρες

Ενότητα 2: Ειδικές ανακριτικές πράξεις επί Κυβερνοεγκλημάτων

·                   Ανακριτική Διείσδυση, Συγκεκαλυμμένη έρευνα κτλ

·                   Άρση Απορρήτου Επικοινωνίας στο διαδίκτυο.

·                   Άρση Απορρήτου Επικοινωνίας (Legal interception) στην τηλεφωνία και στο διαδίκτυο

·                   Διατήρηση δεδομένων επικοινωνίας από παρόχους υπηρεσιών τηλεφωνίας και Διαδικτύου

·                   Οικονομικό έγκλημα στον Κυβερνοχώρο - Άρση τραπεζικού απορρήτου

2ώρες

Ενότητα 3:Διαδικασίες εξέτασης και πραγματογνωμοσύνης ψηφιακών πειστήριων

•             Ψηφιακή Εγκληματολογία (Digital Forensics) - Διαδικασίες εξέτασης και πραγματογνωμοσύνης ψηφιακών πειστήριων

•             Μοναδική ψηφιακή ταυτότητα (Hash Value), ψηφιακών αρχείων (εικόνας, εγγράφων κτλ)

•             Τεχνική Διερεύνηση μηνυμάτων ηλεκτρονικού ταχυδρομείου  (Email Forensics) ως αντικείμενο ή μέσο του εγκλήματος

·                  Συλλογή, έρευνα και ανάλυση ηλεκτρονικών ιχνών στο Διαδίκτυο

·                  Πως λειτουργεί μια ιστοσελίδα/ιστολόγιο-Τρόποι Κατασκευής-Συλλογή στοιχείων από ανοιχτές πήγες (OSINT)

·                  Σύστημα Ονοματοδοσίας στο Διαδίκτυο [Domain Naming System] – Ονόματα Χώρου (Domain Names) – Διαδικασίες έρευνας

2ώρες

Τέταρτο  Μέρος Εκπαίδευσης – ΔΙΚΟΝΟΜΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ. ΔΙΕΘΝΗΣ ΣΥΝΕΡΓΑΣΙΑ

Ενότητα 1: Δικονομικό Ποινικό Δίκαιο και Έγκλημα στον Κυβερνοχώρο. Εκτίμηση ψηφιακών αποδείξεων στο Δικαστήριο

·               Έννοια όρων. Ροή και κατάχρηση ψηφιακών δεδομένων.

·               Ανάκριση «ηλεκτρονικού» εγκλήματος.

·               «Κατάσχεση» ψηφιακών δεδομένων.

·               Ψηφιακή «επικοινωνία» -Ψηφιακά πειστήρια και ίχνη.

·               Που «βρίσκονται» τα ψηφιακά ίχνη-Ποιος αναζητά τα ψηφιακά πειστήρια και ίχνη.

·               Απόρρητο ψηφιακών δεδομένων

·               Διαδικασία αυτοφώρου (τόπος και χρόνος τέλεσης) σε περιπτώσεις Κυβερνοεγκλημάτων

·               Δικονομικές εγγυήσεις των ανακριτικών πράξεων και ερευνών στον Κυβερνοχώρο - Ακυρότητες

·               Χρήση και παρουσίαση ψηφιακών αποδείξεων στην ποινική διαδικασία και στο Δικαστήριο

·               Εκτίμηση ψηφιακών αποδείξεων και αποδεικτικών μέσων από τον Δικαστή

·               Πρακτική εφαρμογή/Μελέτες περιπτώσεις (case studies).

4 ώρες

Ενότητα 2: Διεθνής Συνεργασία επί υποθέσεων Κυβερνοεγκλημάτων

•             Δικαστική και Αστυνομική Συνεργασία με σκοπό την πρόληψη και καταστολή των εγκλημάτων στον Κυβερνοχώρο

•             Φορείς συνεργασίας Europol, EC3, Interpol, Eurojust κλπ

•             Διεθνές Ποινικό Δίκαιο και Έγκλημα στον Κυβερνοχώρο

•             Δικαστική συνδρομή και Ευρωπαϊκή Εντολή Έρευνας (ΕΕΕ) σε υποθέσεις Κυβερνοεγκλημάτων

Πρακτική εφαρμογή/Μελέτες περιπτώσεις (case studies).

4 ώρες

Πέμπτο  Μέρος Εκπαίδευσης

Τεχνικά και Οργανωτικά Μέτρα συμμόρφωσης με την Οδηγία NIS, υπόχρεων οργανισμών και φορέων:

·        Πολιτική Ασφαλείας σχετική με την ασφάλεια συστημάτων δικτύου και πληροφοριών

·        Βασικές Απαιτήσεις Ασφάλειας και επιλογή κατάλληλων μέτρων ασφάλειας

·        Ορισμός Υπεύθυνου Ασφάλειας Πληροφοριών και Δικτύων (ΥΑΠΔ/CISO)

Διαδικασία κοινοποίησης συμβάντων ασφάλειας

Κυβερνοασφάλεια – η οδηγία NIS kαι η ενσωμάτωσή της στο εθνικό δίκαιο

4 ώρες