

ΑΝΑΛΥΤΙΚΟ ΠΕΡΙΕΧΟΜΕΝΟ ΠΡΟΓΡΑΜΜΑΤΟΣ ΚΑΤΑΡΤΙΣΗΣ

1. Τίτλος προγράμματος κατάρτισης:

Κυβερνοασφάλεια στη Ναυτιλία

2. Σύνδεση με Πρότυπα Επαγγελματικών Προσόντων:

3. Διάρκεια κατάρτισης (ώρες): 21

4. Ανάγκη κατάρτισης:

Η ναυτιλιακή βιομηχανία εξαρτάται ολοένα και περισσότερο από τις ψηφιακές τεχνολογίες για τη διαχείριση των πλοίων, τη λειτουργία των λιμένων και την ανταλλαγή δεδομένων μεταξύ των εμπλεκόμενων φορέων. Ωστόσο, η αυξανόμενη χρήση ψηφιακών συστημάτων συνεπάγεται και μεγαλύτερους κινδύνους κυβερνοεπιθέσεων, που μπορούν να επηρεάσουν την επιχειρησιακή συνέχεια, την ασφάλεια των πληρωμάτων και τη συμμόρφωση με διεθνείς κανονισμούς.

Το πρόγραμμα κατάρτισης "Κυβερνοασφάλεια στη Ναυτιλία" έχει σχεδιαστεί για να εξοπλίσει τα στελέχη της ναυτιλιακής βιομηχανίας με τις απαραίτητες γνώσεις και δεξιότητες, ώστε να αναγνωρίζουν, να προλαμβάνουν και να αντιμετωπίζουν κυβερνοαπειλές, συμβάλλοντας στην ασφαλή λειτουργία των ναυτιλιακών επιχειρήσεων και πλοίων.

5. Στόχοι:

- **Κατανόηση του κυβερνοκινδύνου στη ναυτιλία:** Ανάλυση των απειλών και των επιπτώσεών τους στη λειτουργία των πλοίων και των λιμενικών εγκαταστάσεων.
- **Ανάπτυξη στρατηγικών πρόληψης και ανίχνευσης κυβερνοεπιθέσεων:** Παρουσίαση τεχνικών για την αποτροπή και την ανίχνευση κυβερνοαπειλών.
- **Εφαρμογή μέτρων προστασίας και αντιμετώπισης περιστατικών:** Ανάπτυξη διαδικασιών άμεσης απόκρισης και αποκατάστασης λειτουργιών έπειτα από κυβερνοεπιθέσεις.
- **Συμμόρφωση με διεθνή πρότυπα και κανονισμούς:** Κατανόηση και εφαρμογή κανονιστικών πλαισίων όπως το IMO MSC-FAL.1/Circ.3 και το ISO 27001.
- **Εκπαίδευση και ευαισθητοποίηση προσωπικού:** Ενίσχυση της κυβερνοασφάλειας μέσω της εκπαίδευσης και της ενδυνάμωσης των ναυτικών και των στελεχών της ναυτιλίας.
- **Πρακτικές εφαρμογές και προσομοιώσεις:** Συμμετοχή σε βιωματικές ασκήσεις και σενάρια προσομοίωσης κυβερνοεπιθέσεων.

6. Περιγραφή υποψηφίων για συμμετοχή:

Άνεργοι με προηγούμενη εμπειρία σε ναυτιλιακούς κλάδους, συμπεριλαμβανομένων εμπορικών σκαφών, πληρωμάτων κρουαζιερόπλοιων, πληρωμάτων Superyacht, διευθυντές ποιότητας, διευθυντές πληρωμάτων, αξιωματικοί ναυτιλίας, μηχανικοί. Εργαζόμενοι στο δημόσιο και ευρύτερο δημόσιο τομέα (όπως υπάλληλοι του Υφυπουργείου Ναυτιλίας, ΑΨΑ κλπ.). Εργαζόμενοι στον ιδιωτικό τομέα (εργαζόμενοι στη Ναυτιλιακή Βιομηχανία). Αυτοαπασχολούμενους σε ναυτιλιακούς κλάδους.

7. Περιεχόμενο κατάρτισης:

A/A Ενότητας	ΑΝΑΛΥΣΗ ΠΕΡΙΕΧΟΜΕΝΟΥ ΕΝΟΤΗΤΩΝ	ΔΙΑΡΚΕΙΑ (ΩΡΕΣ)
Ενότητα 1	Εισαγωγή στα κυβερνο-φυσικά συστήματα (CPS) • Ορισμός και εφαρμογές στον τομέα της ναυτιλίας • Βασικά χαρακτηριστικά των CPS • Εμβάθυνση στις βασικές λειτουργίες των CPS • Ανάλυση του τρόπου που τα CPS συνδυάζουν τον φυσικό κόσμο και τον υπολογιστικό κόσμο για την αυτοματοποίηση και τον έλεγχο διαδικασιών • Ιστορική εξέλιξη των CPS • Αρχιτεκτονικές CPS • Παραδείγματα CPS • Επισκόπηση του ναυτιλιακού τομέα σχετικά με τα CPS	3,5
Ενότητα 2	Προκλήσεις στις ναυτιλιακές επιχειρήσεις σχετικά με τα των CPS • Προβλήματα ασφάλειας και κυβερνοεπιθέσεων • Διαχείριση Δεδομένων και Ανάλυση • Ανθεκτικότητα Συστήματος • Προβλήματα Επικοινωνίας • Προσαρμογή σε Κανονιστικά Πλαίσια • Εκπαίδευση και Ευαισθητοποίηση • Διαχείριση Περιορισμένων Πόρων	3,5
Ενότητα 3	Κύριες τεχνολογίες και πρακτικές εφαρμογές • Τεχνολογίες CPS στην Ναυτιλία • Έξυπνα Λιμάνια • Αυτόνομα Πλοία • Αναγνώριση και Πρόληψη Κινδύνων • Συστήματα Παρακολούθησης και Διοίκησης Στόλου • Διαχείριση Περιβαλλοντικών Κινδύνων • Αυτόνομα Συστήματα Υποστήριξης Πλοίων • Ασφάλεια Δεδομένων και Ιδιωτικότητα • Διαχείριση Κρίσεων	3,5
Ενότητα 4	Κύριες τεχνολογίες – edge computing, IoT • Ορισμός του Edge Computing • Σύνδεση με τα CPS • Παρακολούθηση και Διαχείριση Στόλου • Αξιοποίηση του Edge Computing στη Ναυτιλία • Ο Ρόλος του IoT στην Ενεργειακή Διαχείριση • Ενεργειακή Αποδοτικότητα στον Ναυτιλιακό Τομέα	3,5
Ενότητα 5	Ασφάλεια, Κανονισμοί, Πρότυπα και Το Μέλλον των CPS στην Ναυτιλία • Αναγκαιότητα Κυβερνοασφάλειας • Απειλές και Κίνδυνοι στον Ναυτιλιακό Τομέα • Διαχείριση Κυβερνοαπειλών • Συμμόρφωση με Διεθνή Πρότυπα • Επιθέσεις σε Συστήματα Ελέγχου • Ασφάλεια Συσκευών IoT • Συμβατότητα με Παλαιά Συστήματα • Ασφάλεια Συναλλαγών και Επαληθεύσιμα Δεδομένα • Ανθρώπινος Παράγοντας και Σφάλματα Χρήστη	4

Ενότητα 6	Πρακτικές Εφαρμογές • Βιωματικές Ασκήσεις: Οργάνωση ασκήσεων που θα επιτρέψουν στους συμμετέχοντες να αποκτήσουν πρακτική εμπειρία στην αντιμετώπιση κυβερνοεπιθέσεων, να εργαστούν σε πραγματικά σενάρια και να εφαρμόσουν τις στρατηγικές που διδάχθηκαν.	3
-----------	--	---