



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΝΑΥΤΙΛΙΑΣ ΚΑΙ  
ΝΗΣΙΩΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ  
ΑΡΧΗΓΕΙΟ ΛΙΜΕΝΙΚΟΥ ΣΩΜΑΤΟΣ –  
ΕΛΛΗΝΙΚΗΣ ΑΚΤΟΦΥΛΑΚΗΣ  
ΚΛΑΔΟΣ ΕΛΕΓΧΟΥ ΠΛΟΙΩΝ  
ΔΕΔΑΠΛΕ Γ΄**

Ταχ. Διεύθυνση : Γρ. Λαμπράκη 150  
Ταχ. Κώδικας : 185 18 Πειραιάς  
Πληροφορίες : Αντιπλοίαρχος Λ.Σ. (Τ) ΤΣΑΓΚΑΛΙΔΗΣ Ιωάννης  
: Αντιπλοίαρχος Λ.Σ. ΚΩΣΤΕΛΙΔΗΣ Χρήστος  
Τηλέφωνο : 213 137 1939-1911  
E-mail : [dedaple@hcg.gr](mailto:dedaple@hcg.gr)

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ  
Πειραιάς, 30 Ιουλίου 2021  
Αριθμ. Πρωτ.: 2343.3-10 / 55896 / 2021

**ΠΡΟΣ: ΩΣ Π.Δ.**

**ΘΕΜΑ: «Διαχείριση των απειλών ασφαλείας του κυβερνοχώρου (Cyber Security) από τις υποχρεώσεις του κώδικα ISPS λιμενικές εγκαταστάσεις και λιμένες και διευκρινίσεις για την εκπόνηση/ανασκόπηση και αναθεώρηση των μελετών ασφαλείας αυτών».**

**ΣΧΕΤ.:** α) Κανονισμός (ΕΚ) 725/2004 «Για τη βελτίωση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις».  
β) Οδηγία (ΕΕ) 2016/1148 «Σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση».  
γ) Οδηγία 2005/65/ΕΚ «Σχετικά με την ενίσχυση της ασφαλείας των λιμένων».  
δ) Ν. 3622/2007 (ΦΕΚ 281 Α΄) «Ενίσχυση της ασφαλείας πλοίων, λιμενικών εγκαταστάσεων και λιμένων και άλλες διατάξεις», ως ισχύει.  
ε) Η με Αριθμ. 4113.319/02/2014 Υ.Α. (ΦΕΚ 3191 Β΄) «Καθορισμός των προϋποθέσεων και της διαδικασίας για την αναθεώρηση των εγκεκριμένων μελετών αξιολόγησης ασφαλείας και σχεδίων ασφαλείας πλοίων, λιμενικών εγκαταστάσεων και λιμένων».

**1.** Η αυξανόμενη χρήση της προηγμένης τεχνολογίας πληροφοριών - επικοινωνιών και αυτοματισμών στις λιμενικές εγκαταστάσεις και στους λιμένες, έχει λάβει μια εκθετικά αυξανόμενη πορεία. Οι εν λόγω τεχνολογίες χρησιμοποιούν ως επί το πλείστον τον κυβερνοχώρο και ως εκ τούτου εκτίθενται στις εγγενείς τρωτότητες/κινδύνους και απειλές ασφαλείας που υφίστανται σε αυτόν.

**2.** Λαμβάνοντας υπόψη την αυξανόμενη συχνότητα των συμβάντων ασφαλείας στον κυβερνοχώρο το Ευρωπαϊκό κοινοβούλιο εξέδωσε την (β) σχετική οδηγία ([https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC)) σχετικά με κοινά μέτρα για υψηλό επίπεδο ασφαλείας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

**3.** Ο κώδικας ISPS, ο οποίος έχει καταστεί υποχρεωτικός βάσει του Κανονισμού (ΕΚ) αριθ. 725/2004 για τη βελτίωση της ασφαλείας πλοίων και λιμενικών εγκαταστάσεων, σχετίζεται σαφώς και με την ασφάλεια στον κυβερνοχώρο λόγω της απαίτησής του να λαμβάνονται υπόψη τα συστήματα και τα δίκτυα υπολογιστών. Με γνώμονα τα παραπάνω, η Ευρωπαϊκή Επιτροπή δημοσίευσε ένα εγχειρίδιο «transport cyber security toolkit» για την ασφάλεια στον κυβερνοχώρο, το οποίο περιλαμβάνει προτεινόμενες πρακτικές και για τον τομέα των θαλασσιών μεταφορών και δύναται να ανακτηθεί από τον σύνδεσμο ([https://ec.europa.eu/transport/sites/default/files/cybersecurity-toolkit\\_en.pdf](https://ec.europa.eu/transport/sites/default/files/cybersecurity-toolkit_en.pdf)). Επίσης, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών «ENISA» έχει αναπτύξει κατευθυντήριες πρακτικές «Good practices for cybersecurity in the maritime sector», οι οποίες δύναται να ανακτηθούν από τον σύνδεσμο (<https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>), σχετικά με τη διαχείριση κινδύνων στον κυβερνοχώρο για τη ναυτιλιακή βιομηχανία καθώς επίσης και μια αναφορά βέλτιστων πρακτικών «Cyber Risk Management for Ports», η οποία δύναται να ανακτηθεί από τον σύνδεσμο (<https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports>) σχετικά με τη μεθοδολογία αξιολόγησης κινδύνου των λιμενικών εγκαταστάσεων και των λιμένων στον κυβερνοχώρο.

4. Τα παραπάνω έχουν ως στόχο να παρέχουν στους φορείς διαχείρισης και τους αναγνωρισμένους οργανισμούς ασφαλείας οδηγίες για την εκτίμηση κινδύνου στον κυβερνοχώρο, ώστε να μπορούν να προσαρμόζονται σε οποιαδήποτε μεθοδολογία αξιολόγησης κινδύνου που ακολουθούν. Προκειμένου να επιτευχθεί αυτό, οι κατευθυντήριες οδηγίες εισάγουν μια προσέγγιση στη διαχείριση κινδύνων στον κυβερνοχώρο για τους φορείς διαχείρισης λιμένων και λιμενικών εγκαταστάσεων, η οποία βασίζεται στις υπάρχουσες μεθοδολογίες εκτίμησης κινδύνου που έχουν υιοθετηθεί με τον κώδικα ISPS.
5. Παρακαλούμε όπως οι ανωτέρω οδηγίες/κατευθύνσεις/πρακτικές, καθώς και τα ειδικότερα δεδομένα/λειτουργικά χαρακτηριστικά της κάθε λιμενικής εγκατάστασης/λιμένα που σχετίζονται με απειλές ασφάλειας στον κυβερνοχώρο, να λαμβάνονται υπόψη κατά την εκπόνηση, ανασκόπηση και αναθεώρηση των μελετών ασφαλείας λιμενικών εγκαταστάσεων/λιμένων (κατά περίπτωση) σύμφωνα με (ε) σχετική.
6. Επιπρόσθετα και προς υποβοήθηση του έργου σας επισημαίνεται ότι σε κάθε περίπτωση επικαιροποιημένο υλικό (νομοθεσία, μελέτες, αναφορές, έρευνες, οδηγίες, πρακτικές κ.α.) για την κυβερνοασφάλεια στον τομέα της ναυτιλιακής βιομηχανίας δύναται να αναζητηθεί στην ιστοσελίδα της Ευρωπαϊκής Ένωσης [https://ec.europa.eu/transport/themes/security/cybersecurity\\_en](https://ec.europa.eu/transport/themes/security/cybersecurity_en) και στην ιστοσελίδα του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών <https://www.enisa.europa.eu>.
7. Η παρούσα εγκύκλιος να τεθεί στον πίνακα εγκυκλίων ISPS, ο οποίος είναι αναρτημένος στις ιστοσελίδες ΗCG και ΥΝΑΝΠ.
8. Παρακαλούμε για την ενημέρωση και τις δικές σας ενέργειες.-

Ο Διευθυντής

Πλοίαρχος Λ.Σ. (Τ) ΤΣΑΡΤΙΝΟΓΛΟΥ Κύρος-Νικόλαος

#### **ΠΙΝΑΚΑΣ ΔΙΑΝΟΜΗΣ**

##### **I. ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΕΝΕΡΓΕΙΑ**

1. ΟΡΓΑΝΙΣΜΟΙ ΛΙΜΕΝΑ Α.Ε. - ΔΗΜΟΤΙΚΑ ΛΙΜΕΝΙΚΑ ΤΑΜΕΙΑ - ΛΙΜΕΝΙΚΑ ΤΑΜΕΙΑ - ΙΔΙΩΤΙΚΕΣ ΛΙΜΕΝΙΚΕΣ ΕΓΚΑΤΑΣΤΑΣΕΙΣ (μέσω Λιμ. Αρχών)
2. ΑΝΑΓΝΩΡΙΣΜΕΝΟΙ ΟΡΓΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

##### **II. ΑΠΟΔΕΚΤΕΣ ΓΙΑ ΚΟΙΝΟΠΟΙΗΣΗ**

Λιμενικές Αρχές Εσωτερικού

##### **III. ΕΣΩΤΕΡΙΚΗ ΔΙΑΝΟΜΗ**

1. ΥΝΑΝΠ/Γρ. κ. Υπουργού (υ.τ.α.)
2. ΥΝΑΝΠ/Γρ. κ. Υφυπουργού (υ.τ.α.)
3. ΥΝΑΝΠ/Γρ. κ. ΓΓΛΠΝΕ (υ.τ.α.)
4. ΥΝΑΝΠ/Γρ. κ. Αρχηγού ΛΣ-ΕΛΑΚΤ (υ.τ.α.)
5. ΥΝΑΝΠ/Γρ. κ. Α΄ Υπαρχηγού ΛΣ-ΕΛΑΚΤ (υ.τ.α.)
6. ΥΝΑΝΠ/Γρ. κ. Β΄ Υπαρχηγού ΛΣ-ΕΛΑΚΤ (υ.τ.α.)
7. ΥΝΑΝΠ/Γρ. κ. ΔΚ Γ΄ (υ.τ.α.)
8. ΥΝΑΝΠ/Γρ. κ. ΔΚ Β΄ (υ.τ.α.)
9. ΥΝΑΝΠ/Γρ. κ. ΔΚ Δ΄ (υ.τ.α.)
10. ΥΝΑΝΠ/ΓΓΛΠΝΕ/ΓΔΛΠΝΕ/ΔΛΠ-ΔΙΛΙΚΥΠ