Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Επιτεύγματα και προκλήσεις στη διαχείριση ασφάλειας εμπορικών λιμένων: Μελέτη περίπτωσης(CRAMM)** **Assets and challenges in security management at trading ports: Example analysis (CRAMM)**
Ονοματεπώνυμο Φοιτητή	**Σωπίκης Παύλος**
Πατρώνυμο	**Σωπίκης Βασίλειος**
Αριθμός Μητρώου	**ΜΠΠΛ13077**
Επιβλέπων	**Καθηγητής Δουληγέρης Χρήστος**

Ημερομηνία Παράδοσης **19/10/2017**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης Καθηγητής	Μιχαήλ Ψαράκης Επίκουρος Καθηγητής	ΠαναγιώτηςΚοτζανικολάου Επίκουρος Καθηγητής

Περίληψη

Στην παρούσα διπλωματική διατριβή διερευνάται το θέμα της ασφάλειας των εμπορικών λιμένων. Η εργασία αυτή αποσκοπεί στη διευκρίνιση του περιεχομένου της έννοιας «ασφάλεια» Ο παράγων ασφάλεια παίζει σημαντικό ρόλο στη λειτουργία των λιμένων. Με τον όρο ασφάλεια εννοείται τόσο η ασφάλεια της εργασίας όσο και η ασφάλεια από έκνομες ενέργειες. Επίσης στην έννοια της ασφάλειας περιλαμβάνεται και η προστασία από τα φυσικά φαινόμενα. Η εργασία καταλήγει στη διαπίστωση ότι προκύπτει έλλειμμα, στη διεθνή νομοθεσία, ως προς την ασφάλεια των λιμένων από τις φυσικές καταστροφές. Οι φορείς διοίκησης των λιμένων οφείλουν να διαμορφώσουν ασφαλές περιβάλλον για τους εργαζόμενους, λαμβάνοντας υπόψη και αυτή την πτυχή της ασφάλειας. Επίσης, παρουσιάζεται και αναλύεται η μέθοδος CRAMM, μια μέθοδος ανάλυσης και αντιμετώπισης ρίσκου που χρησιμοποιείται σε μεγάλο βαθμό στους λιμένες σήμερα.

Abstract

This present postgraduate dissertation examines the issue of the security in commercial ports. This work aims to clarify the content of the 'security' concept. Pivotal security plays an important role in the functioning of the ports. Safeguarding the safety of both work and safety is a matter of security. Security also includes the protection of natural phenomena. The work concludes that there is a deficit, in international law, as regards the security of ports from natural disasters. The port authorities have to design a safe environment for workers, also taking into account this aspect of security. Also presented and analyzed is the CRAMM method, a method of risk analysis and risk management that is used extensively in ports today.

Περιεχόμενα

Εισαγωγή

Το τραγικό δυστύχημα του Τιτανικού (1912) επέβαλε τη νέα τότε έννοια της "ασφάλειας" στον τομέα της ναυτιλίας. Πολλές νομοθεσίες και οδηγίες που δημοσιεύθηκαν έκτοτε επικεντρώνονται στην φυσική προστασία των πλοίων, του πληρώματος, των επιβατών, του φορτίου και της θάλασσας.

Οι τρομοκρατικές επιθέσεις στη Νέα Υόρκη και την Ουάσιγκτον (2001), την Μαδρίτη (2004) και το Λονδίνο (2005), επέβαλαν την έννοια της «ασφάλειας» με πρόσθετες οδηγίες και νομοθεσία (π.χ. ο Διεθνής Κώδικας Προστασίας των Πλοίων και Παρόχων Λιμένων ISPS – International Ship & Portfacility Security). Παρά το γεγονός ότι αυτές οι νέες προσπάθειες επικεντρώθηκαν στις οργανωτικές και τις πτυχές ελέγχου της φυσικής ασφάλειας των πλοίων, οι ναυτιλιακές εταιρείες και οι εμπορικοί λιμένες δεν έχουν λάβει υπόψη την ICT (Information and Communication Technologies) και τις απειλές και τους κινδύνους για την ασφάλεια στον κυβερνοχώρο. Το ναυάγιο στην Ιταλία του Costa Concordia το 2012 ήταν μια φυσική συνέπεια αυτής της άγνοιας, δεδομένου ότι διαπιστώθηκε πως η επικοινωνία μεταξύ των λιμένων και των πλοίων δεν ήταν αξιόπιστη, τα συστήματα πλοήγησης και γραμμής ακτών δεν λειτουργούν σωστά και ένα σχέδιο αποκατάστασης των καταστροφών δεν εφαρμόστηκε. Με άλλα λόγια, δεν καλύφθηκαν πολλές πτυχές της ασφάλειας ICT.

Τον Δεκέμβριο του 2011, ο ENISA δημοσίευσε την έκθεση Industrial Control Systems/SCADA στην οποία αναλύονται οι προκλήσεις για την ασφάλεια στον κυβερνοχώρο στην Ναυτιλία. Η έκθεση αυτή, που παρουσιάζει τα αποτελέσματα από το εργαστήριο του ENISA για το θέμα αυτό, επικεντρώνεται στην ασφάλεια των λιμένων και, ειδικότερα, στη διαχείριση της ασφάλειας των τεχνολογιών της πληροφορίας και των λιμενικών συστημάτων (PICT – Port Installation Configuration Table). Η εκπληκτική παρατήρηση, όπως αναφέρεται στην έκθεση, ήταν ότι «η ευαισθητοποίηση στον κυβερνοχώρο σχετικά με τις ανάγκες και τις προκλήσεις στον τομέα της ναυτιλίας της ασφάλειας είναι σήμερα χαμηλή έως ανύπαρκτη» - Dr. Cédric Levy-Bencheton. Παρά το γεγονός ότι οι πτυχές που αφορούν την ασφάλεια (π.χ. φυσική ασφάλεια) θεωρούνται μέσω του κώδικα ISPS, αγνοείται η ασφάλεια PICT. Διάφορες προτάσεις και λύσεις που παρέχονταν στην έκθεση ήταν οι εξής:

“Σας συνιστούμε ότι μια ολιστική προσέγγιση, με βάση τον κίνδυνο, θα απαιτούσε την αξιολόγηση των υφιστάμενων κινδύνων στον κυβερνοχώρο, που σχετίζονται με τις τρέχουσες εφαρμογές συστημάτων σχετικά με τον ευρωπαϊκό ναυτιλιακό τομέα, καθώς και την αναγνώριση όλων των κρίσιμων στοιχείων του ενεργητικού στον τομέα αυτό. Για τους οικονομικούς φορείς της ναυτιλίας και τα ενδιαφερόμενα μέρη, είναι σημαντικό να εφαρμόζονται προληπτικά μέτρα στον κυβερνοχώρο, καθώς και οι αρχές διαχείρισης κινδύνων ασφάλειας πληροφοριών μέσα στους οργανισμούς και το περιβάλλον τους». Στην παρούσα εργασία, θα ακολουθήσει η περαιτέρω ανάλυση αυτής της σύστασης με ιδιαίτερη έμφαση στο σύστημα CRAMM.

ΚΕΦΑΛΑΙΟ 1 Λειτουργίες και ασφάλεια Λιμένων

1.1 Λιμένες στην κοινωνία της πληροφορίας

Όπως ορίστηκε από το Ευρωπαϊκό Συμβούλιο το 2008 στις Βρυξέλλες (14368/08) μια κρίσιμη υποδομή είναι ένα «επενδυτικό αγαθό, σύστημα ή μέρος, το οποίο είναι απαραίτητο για την διατήρηση των ζωτικών λειτουργιών της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των ανθρώπων, και η βλάβη ή η καταστροφή των οποίων θα έχει σημαντικές επιτττώσεις, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών ».

Στη σημερινή κοινωνία, η ανάπτυξη προηγμένων πληροφοριακών συστημάτων και η διάδοση και ταχεία εξέλιξη των υποδομών ευρυζωνικών επικοινωνιών προκάλεσαν την ευρεία υιοθέτηση της τεχνολογίας των επικοινωνιών από όλες τις υποδομές ζωτικής σημασίας. Η υποβάθμιση, βλάβη ή καταστροφή των υποδομών αυτών θα έχουν σοβαρό αντίκτυπο στην καθημερινή ζωή των πολιτών. Οι διαδικασίες ανταλλαγής πληροφοριών που υποστηρίζονται από τις IOT – Internet of Things(ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων ή ανθρώπων που διαθέτουν μοναδικά αναγνωριστικά στοιχεία και τη δυνατότητα μεταφοράς δεδομένων μέσω δικτύου χωρίς να απαιτείται αλληλεπίδραση ανθρώπου με άνθρωπο ή άνθρωπο με υπολογιστή) αποτελώντας υποδομές ζωτικής σημασίας, για τον εαυτό τους ή όντας κρίσιμης σημασίας, για τη λειτουργία των άλλων κρίσιμων υποδομών, ορίζονται ως υποδομές πληροφοριών ζωτικής σημασίας (Operational Intelligence – OI).

Οι εμπορικοί λιμένες είναι οι φορείς OI στην ψηφιακή εποχή, δεδομένου ότι φιλοξενούν κρίσιμα συστήματα IOT, των οποίων η βλάβη ή η καταστροφή έχει σημαντική επίπτωση στην οικονομία, το εμπόριο και την εθνική ασφάλεια. Η κανονική λειτουργία των εμπορικών λιμένων εξαρτάται σε μεγάλο βαθμό, από την ορθή λειτουργία των συστημάτων IOT. Η μεγάλη ποσότητα των κρίσιμων και ευαίσθητων δεδομένων, των πληροφοριών και των υπηρεσιών που διαχειρίζονται σε καθημερινή βάση, ο μεγάλος αριθμός των φορέων που καλούνται να εξυπηρετηθούν, και οι αλληλεξαρτήσεις με άλλες υποδομές απαιτούν αποτελεσματική διαχείριση της ασφάλειας.

Οι εμπορικοί λιμένες εφαρμόζουν κρίσιμες ηλεκτρονικές υπηρεσίες και επιχειρηματικές διαδικασίες. Έτσι, απαιτούνται οι προσεγγίσεις κατάλληλης διαχείρισης της ασφάλειας και της προστασίας διατηρώντας την ασφαλή εκτέλεση των λιμένων σε περίπτωση βλάβης, επιθέσεων, ατυχημάτων ή κακόβουλων ενεργειών και, επίσης, για ελαχιστοποίηση του χρόνου αποκατάστασης των ζημιών. Μεγάλη προσοχή πρέπει να δοθεί στην ασφάλεια και την προστασία των υφισταμένων υπηρεσιών και και για την νέα γενιά κρίσιμων υπηρεσιών ηλεκτρονικού λιμένος.

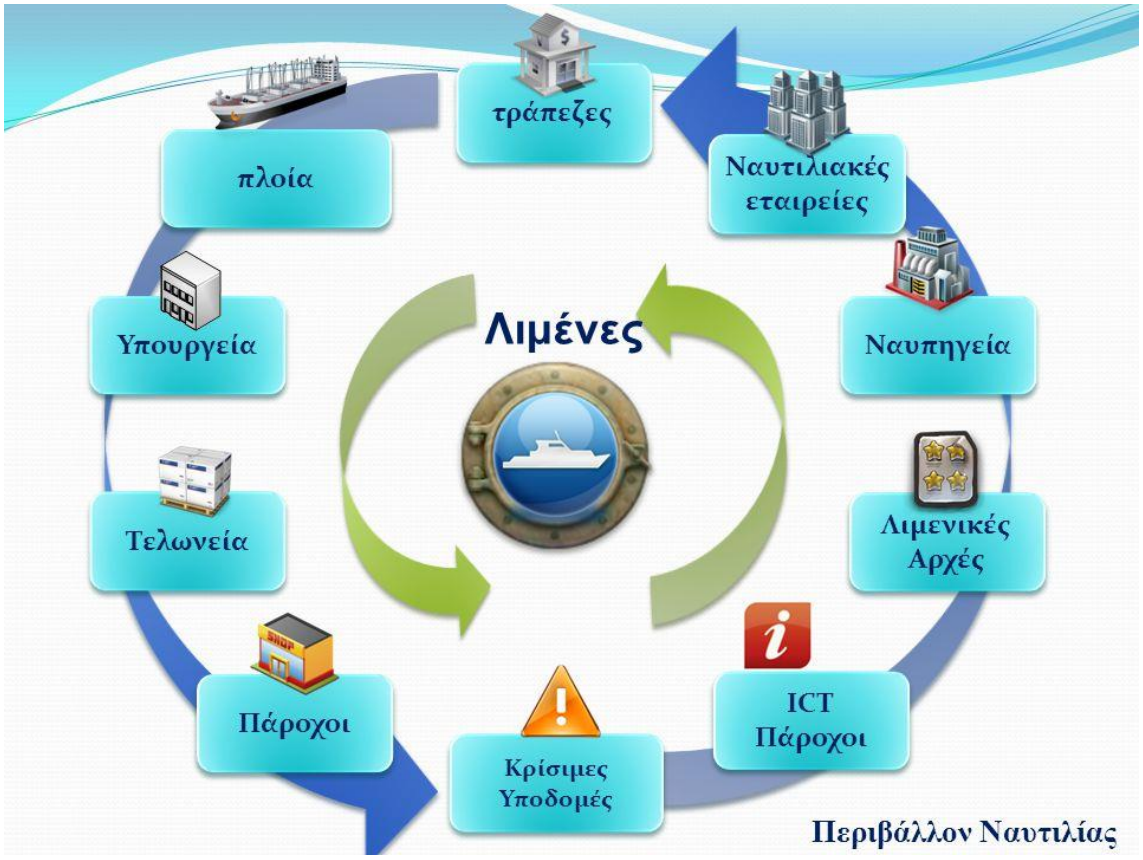
Στις ακόλουθες παραγράφους, παρουσιάζεται μια πολύ σύντομη εισαγωγή στο ναυτιλιακό οικοσύστημα, τα στοιχεία των συστημάτων Port - IOT, καθώς και και τις υπηρεσίες ηλεκτρονικού λιμένος. Το υλικό αυτό είναι πολύ χρήσιμο για την κατανόηση της εκτίμηση της κρισιμότητας των υπηρεσιών

ηλεκτρονικού λιμένος, η οποία αποτελεί αναπόσπαστο μέρος της διαχείρισης ασφάλειας των συστημάτων.

1.2 Ναυτιλιακό Περιβάλλον- Ο ρόλος των εμπορικών λιμένων

Το ναυτιλιακό περιβάλλον είναι πολύπλοκο, όπως φαίνεται στο επόμενο σχήμα στην Εικόνα 1 λόγω της συμμετοχής πολλών φορέων - λιμένες, πλοία (μαζί με τους επιβάτες, το πλήρωμα και το φορτίο), λιμενικές αρχές, ναυτιλιακές και ασφαλιστικές εταιρείες, τελωνεία, βιομηχανία των πλοίων, τράπεζες, υπουργεία, άλλοι εμπορικοί πάροχοι, άλλες κρίσιμες υποδομές (π.χ. σιδηρόδρομοι, αεροδρόμια)- οι οποίοι αλληλεπιδρούν μεταξύ τους και υποστηρίζονται από πολύπλοκα και ετερογενή συστήματα IOT.

Κεντρικός ρόλος, στο ναυτιλιακό περιβάλλον, έχει αναληφθεί από τους εμπορικούς λιμένες, δεδομένου ότι είναι η μόνη οντότητα που αλληλεπιδρά άμεσα με όλους τους ναυτιλιακούς εταίρους, προσφέροντας υπηρεσίες (λιμενικές υπηρεσίες) με διαφορετικό βαθμό κρισιμότητας.



Εικόνα 1: Περιβάλλον Ναυτιλίας Πηγή: unipi.gr

1.3 Στοιχεία του Port Installation Configuration Table (PICT)

Πολλές από τις υπηρεσίες που προσφέρονται και από τις διαδικασίες που υποστηρίζουν τη λειτουργία του εμπορικού λιμένα έχουν αυτοματοποιηθεί. Τα Συστήματα Πληροφορικής και Τηλεπικοινωνιών Λιμένων είναι σύνθετα και αποτελούνται (όπως όλα τα συστήματα ICT) από τα ακόλουθα έξι (6) συνεχή σημεία αναφοράς:

1. Φυσικές υποδομές (π.χ. κτίρια, αποβάθρες, πύλες, μαρίνες, κέντρα δεδομένων, πλατφόρμες)

2. Υποδομές ICT (π.χ. δίκτυα, εξοπλισμός, τους δορυφόρους, εξυπηρετητές, σταθμοί αναμετάδοσης, παράπλευροι σταθμοί)

3. Συστήματα και λογισμικό (π.χ. δίκτυα επικοινωνιών, συστήματα μετάδοσης, δεδομένα ταυτοποίησης, θαλάσσια ναυσιπλοΐα, Προγραμματισμός Επιχειρηματικών Πόρων -ERPs-, έκδοση εισιτηρίων, GIS, συστήματα προσαρμοστικότητας λιμένων)

4. Πληροφορίες και ηλεκτρονικά δεδομένα (π.χ. θαλάσσια και παράκτια δεδομένα, εμπορικά δεδομένα)

5. Υπηρεσίες (π.χ. τιμολόγιο, πλοήγηση, διαχείριση αποσκευών / φορτίου / πλοίου, λογιστική, ηλεκτρονικές υπηρεσίες υγείας)

6. Χρήστες: α. εσωτερικοί χρήστες (π.χ. διαχειριστές, προσωπικό) β. εξωτερικοί χρήστες (π.χ. λιμενικές αρχές, ναυτιλιακές εταιρείες, τελωνεία, ασφαλιστικές εταιρείες, παροχείς IT και εμπορίου γ). αντικείμενα (π.χ. πλοία, φορτίο του πληρώματος, αποσκευές, οχήματα).

1.4 Υπηρεσίες ηλεκτρονικών λιμένων (E-Port)

Υπάρχουν διάφορες υπηρεσίες ηλεκτρονικών λιμένων (e-port), οι οποίες μπορούν να κατηγοριοποιηθούν, ανάλογα με τον κύριο στόχο τους και τις λειτουργείες τους, στις ακόλουθες πέντε (5) κατηγορίες:

- Υπηρεσίες διαχείρισης πλοίων: παροχή ηλεκτρονικών πληροφορίων, για την κατάσταση σκαφών σε όλους τους πράκτορες· ηλεκτρονικές διοικητικές διαδικασίες· ηλεκτρονική επικοινωνία με το λιμάνι / ναυτιλιακές αρχές, αστυνομία, επιτροπή ελέγχου μετανάστευσης, κλπ· υπηρεσίες ελέγχου ταυτότητας σκάφους και παρακολούθησης (μέσω RFID, συστήματων GIS)· υπηρεσίες πλοήγησης

- Υπηρεσίες διαχείρισης φορτίων: παροχή ηλεκτρονικής τεκμηρίωσης, σε όλους τους εμπλεκόμενους φορείς· ηλεκτρονικές πληροφορίες για την κατάσταση των φορτίων,

ηλεκτρονική διαχείριση φορτίου, έλεγχος ταυτότητας φορτίου και υπηρεσίες παρακολούθησης (μέσω RFID, συστήματα GIS)· υπηρεσίες πλοήγησης

- Λογιστικές υπηρεσίες της ενδοχώρας: ηλεκτρονική διαχείριση των λειτουργιών των χερσαίων μεταφορών (π.χ. μεταφορές / αποδοχή / ηλεκτρονικές παραγγελίες παράδοσης)· ηλεκτρονικός εφοδιασμός, ηλεκτρονική τιμολόγηση, ηλεκτρονική πληρωμή· υπηρεσίες ηλεκτρονικής ανίχνευσης (π.χ. ηλεκτρονικές πληροφορίες σχετικά με τις μεταφορές σε ολόκληρη την λογιστική αλυσίδα)· ηλεκτρονική κράτηση

- Υπηρεσίες επικοινωνίας στο επίπεδο λιμένα: Διακαναλική ανακοίνωση (τηλεόραση, Διαδίκτυο, ασύρματο δίκτυο, VPN, δίκτυα επικοινωνίας), υπηρεσίες λιμένων για την επικοινωνία με όλες τις ναυτιλιακές εταιρείες (άλλοι λιμένες, πλοία, πλήρωμα κλπ.)

- Υπηρεσίες ενσωμάτωσης με άλλα συστήματα: Υπηρεσίες ολοκλήρωσης με τα τελωνειακά συστήματα, για τα διάφορα ηλεκτρονικά διοικητικά τελωνειακό έγγραφα (π.χ. τελωνειακές διασαφήσεις, εισαγωγές / εξαγωγές) και τους ελέγχους (π.χ. φόροι, κυρώσεις)· ολοκλήρωση, με την αστυνομία λιμένος και τα συστήματα μετανάστευσης, της ηλεκτρονικής παρακολούθησης και του ελέγχου των πλοίων, των φορτίων, των αγαθών και των ανθρώπων· ενοποίηση των συστημάτων οργανισμών υγείας, για την παροχή υπηρεσιών ηλεκτρονικής υγείας (ειδικά στο πλήρωμα)· ενοποίηση με άλλες μεταφορές (π.χ. με σιδηρόδρομους και αεροδρόμια), προσφέροντας συνεργατικές ηλεκτρονικές υπηρεσίες τουρισμού (κρατήσεις, προγραμματισμός, έκδοση εισιτηρίων).

Ωστόσο, δεν έχουν όλες οι παραπάνω υπηρεσίες τους ίδιους βαθμούς "ηλεκτρονικής εκλέπτυνσης", δηλαδή οι επιχειρηματικές τους διαδικασίες δεν έχουν τον ίδιο βαθμό εξάρτησης, από τα ηλεκτρονικά μέσα. Για την μέτρηση του επιπέδου της υπάρχουσας ωριμότητας εκλέπτυνσης κάθε ηλεκτρονικής υπηρεσίας, κάποιος μπορεί να υιοθετήσει το πλαίσιο τεσσάρων επιπέδων που χρησιμοποιούνται στον τομέα της ηλεκτρονικής διακυβέρνησης, δηλαδή τις πληροφορίες, την αλληλεπίδραση, την αμφίδρομη αλληλεπίδραση και τον πλήρη χειρισμό. Ειδικότερα, το πρώτο επίπεδο εξειδίκευσης περιλαμβάνει τις υπηρεσίες που παρέχουν μόνο πληροφορίες σε απευθείας σύνδεση (καμία περαιτέρω αλληλεπίδραση επιτρέπεται). Στο δεύτερο επίπεδο, υπάρχει η δυνατότητα απόκτησης ενός ηλεκτρονικού εγγράφου (καμία περαιτέρω αλληλεπίδραση επιτρέπεται). Υπηρεσίες του τρίτου επιπέδου (αμφίδρομη επικοινωνία) είναι εκείνες που προσφέρουν την δυνατότητα ηλεκτρονικής πρόσληψης, με επίσημη ηλεκτρονική μορφή, για να ξεκινήσει η διαδικασία για την απόκτηση αυτής της υπηρεσίας. Τέλος, στο τέταρτο επίπεδο, οι υπηρεσίες προσφέρουν τη δυνατότητα πλήρους εφαρμογής της λιμενικής υπηρεσίας σε ηλεκτρονική μορφή, συμπεριλαμβανομένης της παράδοσης. Καμία άλλη επίσημη διαδικασία δεν είναι απαραίτητη για τον αιτούντα μέσω των "γραπτών αιτήσεων". Τα δύο τελευταία επίπεδα απαιτούν έλεγχο ταυτότητας του χρήστη και του διαχειριστή της υπηρεσίας ηλεκτρονικού λιμένος.

1.5 Οι λειτουργίες ενός λιμένα

Στο λιμένα λαμβάνουν χώρα πολλές και διάφορες υπηρεσίες ναυτιλιακού χαρακτήρα όπως υπηρεσίες προς τους πλοιοκτήτες, προς τους ναυτικούς, προς τους επιβάτες, προς τους εισαγωγείς και εξαγωγείς των εμπορευμάτων, στους φορτωτές και παραλήπτες των φορτίων, κ.λπ. και υπηρεσίες προς τα πλοία, όπως πλοήγηση, ρυμούλκηση, αγκυροβολία, κ.λπ.

Οι λειτουργίες ενός λιμένα είναι πολλαπλές και αποσκοπούν στο να καθιστούν τον λιμένα παράγοντα οικονομικής ανάπτυξης. Η πρώτη και κύρια λειτουργία του λιμένα είναι η παροχή υπηρεσιών για τη διακίνηση των φορτίων και των επιβατών. Ο λιμένας είναι απαραίτητο να διαθέτει τους κατάλληλους χώρους και τις κατάλληλες υποδομές σε κτίρια και μηχανήματα ώστε να εξυπηρετεί το πλοίο, το φορτίο και τους επιβάτες. Βέβαια τα έργα υποδομής που απαιτούνται για την εξυπηρέτηση όλων αυτών δεν είναι τα ίδια για όλους τους λιμένες, αλλά εξαρτώνται από την κατηγορία του κάθε λιμένα. Σε γενικές γραμμές όμως υπάρχουν κάποια βασικά έργα και μηχανικός εξοπλισμός που είναι αναγκαία σε κάθε λιμένα.

Τα λιμενικά έργα και ο μηχανικός εξοπλισμός ανάλογα με την ανάγκη που ικανοποιούν είναι (Μυλωνόπουλος, 2004:269-272):

α) ως προς την εξυπηρέτηση του πλοίου. Απαιτούνται λιμενικά έργα που αφορούν στην υποδοχή του πλοίου. Αυτά αποβλέπουν στην προσόρμιση του πλοίου από πλευράς βυθίσματος αυτού και ασφάλειας και στη λειτουργική εξυπηρέτησή του. Έτσι το βάθος του λιμένα πρέπει να είναι μεγαλύτερο από το έμφορτο βύθισμα του πλοίου που υποδέχεται. Η απαίτηση αυτή προϋποθέτει έργα εκβάθυνσης και διαμόρφωσης του βυθού για την αγκυροβολία του πλοίου. Η απαίτηση ασφαλούς προσόρμισης ενδεχομένως να προϋποθέτει έργα προφύλαξης του λιμένα από τις άσχημες καιρικές συνθήκες, όπως λιμενοβραχίονες, κυματοθραύστες κ.λπ. Η λειτουργική εξυπηρέτηση του πλοίου απαιτεί προβλήτες για την πρυμνοδέτηση και παραβολή του πλοίου, κρηπιδώματα με μεγάλο μήκος κ.λπ.

β) ως προς την εξυπηρέτηση του φορτίου. Για τη φορτοεκφόρτωση του φορτίου στο πλοίο όπως και για τη διακίνηση αυτού στους χώρους του λιμένα απαιτείται μηχανικός εξοπλισμός. Επίσης για την αποθήκευση του φορτίου απαιτούνται κτιριακές εγκαταστάσεις. Τόσο ο μηχανικός εξοπλισμός όσο και οι κτιριακές εγκαταστάσεις εξαρτώνται από τα ιδιαίτερα χαρακτηριστικά του φορτίου που διακινείται στο λιμένα

Συνήθως στους λιμένες με μεγάλη κίνηση φορτίων δημιουργούνται ειδικοί σταθμοί (terminal) που απαιτούν εξειδικευμένες εγκαταστάσεις και εξειδικευμένο μηχανολογικό εξοπλισμό. Τέτοιοι σταθμοί (Παρδάλη, 2001:101-429) είναι:

♦ Σταθμοί διακίνησης εμπορευματοκιβωτίων. Εξυπηρετεί πλοία που μεταφέρουν εμπορευματοκιβώτια και γι΄ αυτό διαθέτει προβλήτες με μεγάλο μήκος για την πρόσδεση των πλοίων αυτών. Επίσης διαθέτει

γερανογέφυρες ξηράς που κινούνται σε σιδηροτροχιές κατά μήκος του προβλήτα, γερανούς που κινούνται με τροχούς, ελκυστήρες – πλατφόρμες, περονοφόρα οχήματα κ.λπ. Διαθέτει χώρους εναπόθεσης και φύλαξης των εμπορευματοκιβωτίων, χώρους πλήρωσης και εκκένωσης των εμπορευματοκιβωτίων κ.λπ.

♦ Σταθμοί διακίνησης συμβατικού φορτίου. Εξυπηρετεί πλοία που μεταφέρουν συμβατικό φορτίο δηλαδή γενικό φορτίο και χύδην ξηρό φορτίο. Απαιτεί προβλήτες για την παραβολή των πλοίων. Ο μηχανολογικός εξοπλισμός που απαιτείται για τη φορτοεκφόρτωση του φορτίου είναι αυτοκινούμενοι γερανοί, περονοφόρα οχήματα, γερανοί αρπάγες για τα χύδην ξηρά φορτία όπως και συστήματα αέρος που λειτουργούν ως αντλίες αναρρόφησης και προώθησης του χύδην ξηρού φορτίου. Επίσης απαιτούνται στεγασμένοι χώροι αποθήκευσης, υπόστεγα διαμετακόμισης, ανοικτοί χώροι εναπόθεσης κ.λπ.

♦ Σταθμοί διακίνησης υγρών φορτίων. Για τη φορτοεκφόρτωση των υγρών φορτίων απαιτούνται ειδικές εγκαταστάσεις με σωληνώσεις και αγωγούς στον προβλήτα αλλά και μέσα στη θάλασσα ανάλογα με το είδος του υγρού φορτίου.

γ) ως προς την εξυπηρέτηση των επιβατών. Για την εξυπηρέτηση των επιβατών λειτουργεί ο σταθμός επιβατών που διαθέτει αίθουσες αναμονής, τουριστικά καταστήματα, εστιατόρια και καφετέριες, και επιπλέον τράπεζες, ανταλλακτήρια συναλλάγματος, καταστήματα αφορολογήτων ειδών, χώρους στάθμευσης τουριστικών λεωφορείων κ.λπ. όταν είναι σταθμός επιβατών πλοίων εξωτερικού.

δ) οδικό δίκτυο. Για την κίνηση των τροχοφόρων μέσα στον λιμένα είναι απαραίτητο να υπάρχει κατάλληλο οδικό δίκτυο. Επίσης, η προσπέλαση στον λιμένα πρέπει να είναι εύκολη. Σε πολλούς λιμένες λειτουργεί σιδηροδρομικό δίκτυο για τη γρήγορη διακίνηση του φορτίου εντός και εκτός αυτών.

ε) ανθρώπινο δυναμικό. Η λειτουργία των κτιριακών εγκαταστάσεων και του μηχανολογικού εξοπλισμού και η γενική λειτουργία του λιμένα βασίζεται στο ανθρώπινο δυναμικό που προσφέρει την εργασία του. Για την άριστη απόδοσή του απαιτούνται κατάλληλες κτιριακές εγκαταστάσεις, άριστες συνθήκες εργασίας, τεχνολογική υποστήριξη π.χ. ηλεκτρονικοί υπολογιστές και εξειδικευμένο λογισμικό, συνεχής επιμόρφωση και κατάρτιση κ.λπ.

Η λειτουργία του λιμένα κατά κανόνα γίνεται είτε με το συγκεντρωτικό σύστημα είτε με το αποκεντρωτικό. Σύμφωνα με το συγκεντρωτικό σύστημα, ο φορέας λειτουργίας του λιμένα αναλαμβάνει όλες τις λιμενικές δραστηριότητες. Όλες οι υπηρεσίες, που παρέχονται στο λιμένα, τίθενται υπό ενιαία διοίκηση και οργάνωση.

Με ενιαίο σύστημα διοίκησης λειτουργούν οι λιμένες της Κύπρου, της Μασσαλίας, του Πειραιά κ.λπ. Οι λιμένες έχουν σημαντική συμβολή στη διεξαγωγή του διεθνούς εμπορίου. Σύμφωνα με στοιχεία της Στατιστικής Υπηρεσίας της Ευρωπαϊκής Ένωσης, το 90% του εμπορίου της Ευρωπαϊκής Ένωσης με τις άλλες χώρες και το 30% του ενδοκοινοτικού εμπορίου διεξάγεται μέσω των λιμένων. Σήμερα επικρατεί η τάση της ναυτιλίας των μικρών αποστάσεων (Γουλιέλμος-Σαμπράκος, 2002:33-36) - shortsea shipping

- δηλαδή η διακίνηση των ενδοκοινοτικών φορτίων μέσω της θάλασσας για να απομακρυνθούν τα φορτία από τους δρόμους και τους σιδηροδρόμους. Σύμφωνα με το αποκεντρωτικό σύστημα, οι υπηρεσίες του λιμένα παρέχονται από αυτόνομες επιχειρηματικές μονάδες. Στο λιμάνι δραστηριοποιούνται ανεξάρτητες οικονομικές μονάδες σε ξεχωριστά πεδία επιχειρηματικής εξειδίκευσης. Με αυτό το σύστημα λειτουργούν οι λιμένες της Αμβέρσας, του Ρότερνταμ, της Νέας Υόρκης κ.λπ. Ο λιμένας είναι ένας συγκοινωνιακός κόμβος στη διακίνηση των εμπορευμάτων. Ως κόμβος εισόδου και εξόδου από χώρα απαιτεί τη λειτουργία τελωνειακών, υγειονομικών και αστυνομικών αρχών.

1.6 Η ασφάλεια ενός λιμένα

Για την οικονομική ανάπτυξη του λιμένα ο παράγοντας «ασφάλεια» έχει πρωταρχική σημασία. Η ασφάλεια όμως αποκτά διττή σημασία. Από τη μια πλευρά αναφέρεται στην ασφαλή διεξαγωγή της εργασίας (safety) στο χώρο του λιμένα που περιλαμβάνει το κατάλληλο εργασιακό και φυσικό περιβάλλον και από την άλλη πλευρά αναφέρεται στο κλίμα ασφάλειας (security) σχετικά με τις παράνομες ενέργειες που θέτουν σε κίνδυνο την ανθρώπινη ζωή και περιουσία.

1.6.1 Ασφάλεια εργασίας (safety)

1.6.1.1 Εργασιακό περιβάλλον

Σε κάθε λιμένα αναπτύσσονται εργασιακές πρακτικές που προστατεύουν την ασφάλεια και την υγεία των εργαζομένων λαμβάνοντας υπόψη τις ιδιαίτερες περιστάσεις κάτω από τις οποίες παρέχεται η κάθε είδους λιμενική εργασία. Προς αυτή την κατεύθυνση, δηλ. της προστασίας του εργαζόμενου στο λιμένα, ο International Labor Organization (ILO), μέσω Διεθνών Συνθηκών και άλλων κειμένων καθόρισε Κώδικες Συμπεριφοράς (ILO, 2005).

Με βάση τη Συνθήκη με αριθ. 152 και τη Σύσταση με αριθ. 160 ο ILO θέσπισε Κώδικα που καλύπτει όλες τις πτυχές της εργασίας στους λιμένες όπου τα αγαθά φορτο-εκφορτώνονται και οι επιβάτες απο-επιβιβάζονται στα πλοία. Ο Κώδικας εφαρμόζεται όχι μόνο στο διεθνές εμπόριο αλλά και στο εσωτερικό εμπόριο των κρατών δηλ. στις πλωτές υδάτινες οδούς, ποτάμιες και λιμναίες. Αν και στους λιμένες λαμβάνει χώρα ένα πολύ ευρύ φάσμα διαφορετικών χειρισμών του φορτίου, ώστε να μην είναι πρακτικό να καλυφθούν όλοι τους λεπτομερώς, εντούτοις, ο Κώδικας καλύπτει τις πιο κοινές δραστηριότητες.

Σύμφωνα με τον Κώδικα για την ασφάλεια εργασίας πρωταρχικό στοιχείο είναι η ενημέρωση στις εφαρμοζόμενες καινοτομίες. Πριν από την εφαρμογή οποιασδήποτε καινοτομίας κρίνεται απαραίτητη η πραγματοποίηση διαβουλεύσεων μεταξύ των εργοδοτών και των εργαζομένων σχετικά με τις πτυχές της ασφάλειας και της υγείας καθώς και η επίτευξη συμφωνίας μεταξύ τους για την εισαγωγή των καινοτομιών.

Επίσης, απαραίτητη είναι η πρόβλεψη και η καθιέρωση μηχανισμών για τον έλεγχο της ασφαλούς χρήσης οποιασδήποτε τεχνολογίας. Σε αυτόν τον έλεγχο είναι επιβεβλημένη η συμμετοχή των εργοδοτών και των εργαζομένων.

Η ασφάλεια στους λιμένες είναι ευθύνη του κάθε ατόμου που έχει άμεση ή έμμεση εργασιακή σχέση με τον χώρο του λιμένα. Πέραν όμως από την ατομική ευθύνη υπάρχει και συλλογική ευθύνη ως προς τη συνεργασία για την ανάπτυξη ασφαλών συστημάτων εργασίας και την εξασφάλιση εφαρμογής τους (ILO, 2005:12).

1.6.1.2 Υγεία

Η ασφάλεια στους λιμένες επιτυγχάνεται με τη λήψη μέτρων στους τομείς της εργασίας. Στον τομέα της εργασίας η πρόληψη αναφέρεται στο διαχωρισμό των ανθρώπων από τα οχήματα και μηχανήματα, στην ανθεκτικότητα των επιφανειών των χώρων του λιμένα, στην ανύψωση των φορτίων, στην πυροπροστασία και στην πυρόσβεση, στις οδικές αρτηρίες, στις περιοχές διαχείρισης του φορτίου, στην πρόσβαση στις εγκαταστάσεις στις αποθήκες και στα υπόστεγα, στον εξοπλισμό ατομικής προστασίας και στην παραβολή των πλοίων.

Στον τομέα της υγείας, η πρόληψη αναφέρεται στις επαγγελματικές ασθένειες, στην κόπωση, στο θόρυβο, στον καπνό, στις δονήσεις, στις επικίνδυνες ουσίες και σε ακραίο φυσικό περιβάλλον (θερμοκρασία, κλιματικές συνθήκες κ.α.).

Οι εργαζόμενοι στο λιμένα κυρίως αλλά και οι συναλλασσόμενοι με αυτόν, λόγω της φύσης της λιμενικής εργασίας, είναι ευάλωτοι αφενός σε τραυματισμούς και ασθένειες που προκαλούνται από ατυχήματα, από πτώση στη θάλασσα, πυρκαγιές και διαρροή υγρού φορτίου και αφετέρου σε φυσικές καταστροφές που προκαλούνται από θυελλώδεις ανέμους, τσουνάμι, τυφώνες, πλημμύρες, πάγους-χιόνια, σεισμούς, ηφαιστειακές εκρήξεις κ.λπ.

Η διαχείριση της ασφάλειας και της υγείας των εργαζομένων στους λιμένες και των προσώπων που επηρεάζονται από τις λιμενικές λειτουργίες πρέπει να γίνεται με τέτοιο τρόπο ώστε να επιτυγχάνεται ισορροπία μεταξύ των κινδύνων λειτουργίας και του κόστους εξάλειψης ή περιορισμού των ατυχημάτων. Για την επίτευξη του στόχου αυτού είναι απαραίτητη η αξιολόγηση του πραγματικού κόστους των τραυματισμών και της βλάβης της υγείας (ILO, 2005:20).

Στις πραγματικές οικονομικές δαπάνες των ατυχημάτων και της ασθένειας περιλαμβάνεται το κόστος των αξιώσεων άμεσης ζημίας, του χαμένου χρόνου και των αποζημιώσεων για τραυματισμούς, καθώς επίσης και των επακόλουθων δαπανών όπως είναι ο χρόνος που δαπανά η διοίκηση για τη αντίκρουση των υποβληθεισών αξιώσεων και την αναπλήρωση των εργαζομένων. Επίσης, δεν πρέπει να αγνοούνται οι δαπάνες των ατυχημάτων που δεν επιφέρουν τραυματισμό καθώς μπορεί να συνιστούν προειδοποίηση για ενδεχόμενα σοβαρότερα γεγονότα στο μέλλον.

Η έκβαση ενός γεγονότος μπορεί να κυμανθεί από τον μηδενικό τραυματισμό ως τον θανάσιμο τραυματισμό. Μια προσέγγιση "συνολικής απώλειας" στην πρόληψη ατυχήματος αναγνωρίζει αυτό το γεγονός και συμπεριλαμβάνει την έρευνα για τα γεγονότα μη-τραυματισμών (ILO, 2005:21).

Η αξιολόγηση του κινδύνου είναι ένα ουσιαστικό εργαλείο στην διαχείριση της ασφάλειας, διότι παρέχει μια υγιή βάση για τη βελτίωση της ασφάλειας. Ένα σύστημα διαχείρισης ασφάλειας βασισμένο στον κίνδυνο απαιτεί διοικητικό μηχανισμό για να προσδιορισθούν οι δραστηριότητες που πρέπει να αναληφθούν. Μια προσέγγιση βασισμένη στον κίνδυνο, επιτρέπει τη συνεχή βελτίωση των προτύπων, σε αντίθεση με ένα σύστημα βασισμένο στην ποιότητα που απαιτεί μόνο την εμμονή σε σταθερά πρότυπα.

Τα συστήματα αξιολόγησης του κινδύνου μπορεί να είναι ποιοτικά ή ποσοτικά. Στην ποιοτική αξιολόγηση του κινδύνου, ο κίνδυνος εκτιμάται με μεθόδους όπως η ανάλυση στόχου, ο προσδιορισμός των ανθρώπινων παραγόντων και η διαμόρφωση της απόδοσης. Στην ποσοτική αξιολόγηση του κινδύνου, ο κίνδυνος εκτιμάται με βάση την πιθανότητα και τη δριμύτητα της έκβασης ενός κινδύνου (ILO, 2005:22). Αυτή είναι η μέθοδος που χρησιμοποιείται συνηθέστερα για να αξιολογήσει την απειλή των κινδύνων στους λιμένες.

Σε απλούστερη μορφή, η ποσοτική εκτίμηση του κινδύνου είναι το προϊόν της πιθανότητας της εμφάνισης ενός κινδύνου και των πιθανών συνεπειών, συμπεριλαμβανομένης της δριμύτητάς τους. Αυτοί οι δύο παράγοντες πρέπει να καθοριστούν ανεξάρτητα. Αν και μια πιθανή συνέπεια μπορεί να είναι εξαιρετικά σοβαρή, η πιθανότητα της εμφάνισής της μπορεί να είναι πολύ μικρή. Τα πιο λεπτομερή συστήματα αξιολόγησης κινδύνου εξετάζουν επίσης τη συχνότητα της παρουσίας του κινδύνου. Η ποσοτική αξιολόγηση του κινδύνου είναι ένα εργαλείο που βοηθά στη λήψη των αποφάσεων.

Η αξιολόγηση του κινδύνου διενεργείται καλύτερα από μια ομάδα στην οποία συμμετέχουν (ILO, 2005:23) ο διευθυντής του λιμένα, ο εκπρόσωπος των εργαζομένων, ο επόπτης, ο σύμβουλος ασφάλειας και ο σύμβουλος υγείας.

Τα εθνικά και τοπικά συστήματα διαχείρισης ασφάλειας και υγείας για τους λιμένες πρέπει να βασιστούν στην αξιολόγηση του κινδύνου, σύμφωνα με τα κύρια στοιχεία των οδηγιών του ILO για τα συστήματα διαχείρισης επαγγελματικής ασφάλειας και υγείας (ILO-OSH, 2001). Αυτά είναι:

- Πολιτική. Σαφής δήλωση του Οργανισμού διαχείρισης του λιμένα ότι στην ασκούμενη πολιτική του πρωτεύουσα θέση έχει η ασφάλεια και η υγεία των εργαζομένων σε όλα τα επίπεδα.
- Οργάνωση. Εξειδίκευση των ευθυνών και των αρμοδιοτήτων σε όλα τα επίπεδα. Προσδιορισμός των απαιτούμενων ικανοτήτων και δεξιοτήτων.
- Προγραμματισμός. Προγραμματισμός της ανάπτυξης και της εφαρμογής του συστήματος διαχείρισης. Αυτό πρέπει να προσδιορίζει τα απαραίτητα μέτρα για την εξάλειψη ή τον έλεγχο των κινδύνων και της θέσης ρεαλιστικών στόχων για την τρέχουσα περίοδο.
- Αξιολόγηση. Έλεγχος και μέτρηση της τρέχουσας απόδοσης, έρευνα για τα ατυχήματα, τους περιοδικούς ελέγχους και την αναθεώρηση του συστήματος διαχείρισης.

- Δράση. Η εφαρμογή της απαραίτητης δράσης για να επιτευχθεί η συνεχής βελτίωση της επαγγελματικής ασφάλειας και της υγείας.

Για την αποτελεσματικότητα ενός ασφαλούς συστήματος της εργασίας είναι αναγκαίες οι διαβουλεύσεις με όλα τα συμβαλλόμενα μέρη που ασχολούνται με την εφαρμογή του. Μετά την οριστικοποίηση το σύστημα ασφάλειας πρέπει να γνωστοποιηθεί σε όλους τους εμπλεκόμενους και να ακολουθήσει η κατάλληλη εκπαίδευσή τους. Τα ασφαλή συστήματα της εργασίας πρέπει να αναθεωρούνται περιοδικά λαμβάνοντας υπόψη τις αλλαγές και τη λειτουργική εμπειρία αλλά και τις πραγματικές ανάγκες.

Το νομικό πλαίσιο ασφάλειας εργασίας λιμένα στην Ελλάδα.

Στη χώρα μας, ο Ν. 1568/85 «Υγιεινή και ασφάλεια των εργαζομένων» (ΦΕΚ 117/Α/18-10-85) και το Π.Δ. 17/96 «Μέτρα για τη βελτίωση της ασφάλειας και της υγείας των εργαζομένων κατά την εργασία σε συμμόρφωση με τις οδηγίες 89/391/ΕΟΚ και 91/383/ΕΟΚ». (ΦΕΚ 11/Α/18-1-96) αποτελούν το βασικό θεσμικό πλαίσιο, ενώ το Π.Δ. 294/1988 «Ελάχιστος χρόνος απασχόλησης τεχνικού ασφαλείας και γιατρού εργασίας, επίπεδο γνώσεως και ειδικότητα τεχνικού ασφάλειας για τις επιχειρήσεις, εκμεταλλεύσεις και εργασίες του άρθρου 1 παρ. 1 του Ν. 1568/1985 "Υγιεινή και ασφάλεια των εργαζομένων"» (ΦΕΚ 138/Α/21-6-1988), το Π.Δ. 159/1999 «Τροποποίηση του Π.Δ. 17/96 και του Π.Δ. 70α/88 "Προστασία των εργαζομένων που εκτίθενται σε αμίαντο κατά την εργασία"» (ΦΕΚ 157/Α/3-8-1999) και ο Ν. 2874/2000 «Προώθηση της απασχόλησης και άλλες διατάξεις» (ΦΕΚ 286/Α/29-12-00) λειτουργούν είτε συμπληρωματικά είτε τροποποιητικά ως προς αυτό (ΥΕΝ, 2006).

Η πολυπλοκότητα της λιμενικής εργασίας απαιτεί συνεχή και μεθοδική εκπαίδευση κατά τέτοιο τρόπο ώστε να γίνει βίωμα στον εργαζόμενο η τήρηση των απαραίτητων μέτρων προστασίας και η τήρηση των βασικών κανόνων στον τρόπο εκτέλεσης συγκεκριμένων εργασιών και χειρισμού του εξειδικευμένου λιμενικού εξοπλισμού. Η εκπαίδευση και η κατάρτιση καθ΄ όλη τη διάρκεια της ζωής είναι ο καλύτερος τρόπος για την αντιμετώπιση της πρόκλησης της αλλαγής. Οι άνθρωποι δεν έχουν κίνητρο να συμμετέχουν σε κάποια εκπαίδευση της οποίας το περιεχόμενο και οι μέθοδοι δεν λαμβάνουν υπόψη τις πολιτιστικές τους προοπτικές και τις προσωπικές τους εμπειρίες (Παντελόγλου, 2004:38). Είναι λοιπόν αναγκαία η επαγγελματική εκπαίδευση και κατάρτιση στα λιμενικές εργασίες και η πιστοποίηση παρακολούθησης ανάλογων προγραμμάτων πρέπει να αποτελεί προαπαιτούμενο προσόν πρόσληψης και προαγωγής.

Κρίνεται επιβεβλημένη η θέσπιση ενός νομικού πλαισίου προστασίας της λιμενικής εργασίας. Το νομικό αυτό πλαίσιο οφείλει να είναι εξειδικευμένο και να ανταποκρίνεται στις απαιτήσεις και στις ιδιαιτερότητες της εργασίας κάθε λιμένα, όπως αυτές προκύπτουν από τα χαρακτηριστικά του διακινούμενου φορτίου.

1.6.2 Ασφάλεια από φυσικά φαινόμενα.

Οι λιμένες μπορεί να πλήττονται από ποικίλα φυσικά φαινόμενα. Σε αυτά περιλαμβάνονται σύμφωνα με τον ILO (ILO, 2005:439):

- οι θυελλώδεις άνεμοι και οι μεγάλες θύελλες οι οποίες μπορεί να προκαλέσουν μεγάλες υλικές ζημιές όπως πχ μετακίνηση και καταστροφή αποθηκευμένων φορτίων, αποκλεισμός εργασίας κτλ

- οι πλημμύρες από παλίρροιες, από τα νερά ποταμών, από τα νερά εδάφους ή από ένα συνδυασμό και των δύο. Αυτό μπορεί να οδηγήσει σε καταστροφή εσωτερικών χώρων, μηχανιμάτων και σύνδεσης των συστημάτων.

- τα χιόνια και οι πάγοι. Το χιόνι και ο πάγος είναι πιθανόν να δημιουργούν ολισθηρές επιφάνειες για ανθρώπους και μηχανές, και να δημιουργούν μια παγωμένη κάλυψη σε μερικά φορτία που τα καθιστούν βαριά, πολύ ολισθηρά στη μετακίνηση και δύσκολα στο χειρισμό.

- οι ακραίες θερμοκρασίες. Μερικοί λιμένες εκτίθενται συχνά σε θερμοκρασίες κάτω από -40°C και πάνω από + 40°C. Η έκθεση στην εξαιρετικά υψηλή ή χαμηλή θερμοκρασία είναι πιθανό να έχει επιπτώσεις στη δυνατότητα των εργαζομένων να συνεχίσουν να εργάζονται με ασφάλεια και χωρίς κίνδυνο της υγείας τους.

- οι σεισμοί. Οι ζημιές μπορεί να είναι από αμελητέες έως καταστροφικές, ανάλογα με την ένταση του σεισμού.

- οι ηφαιστειακές εκρήξεις. Λιμένες που βρίσκονται κοντά σε ενεργειακά ηφαίστεια κινδυνεύον όχι μόνο από έκρηξη αλλά και από παλιροιακά κύματα που μπορεί να προκληθούν.

Μερικοί λιμένες μπορεί να εγκυμονούν υψηλούς κινδύνους λόγω της αποθήκευσης επικίνδυνων ουσιών ή της γειτνίασης με τέτοιες επικίνδυνες εγκαταστάσεις. Στις περιπτώσεις αυτές, εφαρμόζεται ο κώδικας του ILO για την πρόληψη μεγάλων βιομηχανικών ατυχημάτων (ILO, 1991). Σε κάθε λιμένα πρέπει να υπάρχει σχέδιο έκτακτης ανάγκης που να επικεντρώνεται σε τέσσερις παράγοντες (ILO 2005:440). Αυτοί είναι:

- ο κίνδυνος και η φύση ενός γεγονότος και η πιθανή έκτασή του,

- ο κίνδυνος και η πιθανότητα εμφάνισής του,

- οι συνέπειες και η πιθανή επίδραση στους ανθρώπους και το περιβάλλον,

- τα μέσα και οι ενέργειες που αναλαμβάνονται για να ελαχιστοποιηθούν τις συνέπειες του γεγονότος.

Για να είναι αποτελεσματικό το σχέδιο έκτακτης ανάγκης λιμένων πρέπει να καθορίζει με σαφήνεια και με απλούς όρους τις ενέργειες. Πρέπει να είναι εύκαμπτο και ικανό για την αποτελεσματική ανταπόκριση σε οποιαδήποτε έκτακτη ανάγκη που θα προκύψει. Το πλαίσιο πρέπει να περιλαμβάνει τον προσδιορισμό των αρμόδιων προσώπων που θα έχουν τον έλεγχο, την ύπαρξη ενός κέντρου ελέγχου, τις ρυθμίσεις για την αξιολόγηση της κατάστασης, την έναρξη των διορθωτικών μέτρων και την πρόνοια για την παρακολούθηση των γεγονότων καθώς εξελίσσονται.

Το σχέδιο αυτό πρέπει να βασιστεί στις ιδιαίτερες περιστάσεις του λιμένα, συμπεριλαμβανομένων της γεωγραφικής θέσης του, των φορτίων του, του αριθμού ατόμων που απασχολούνται στο λιμένα, την πιθανή παρουσία του κοινού ως επιβάτες ή για άλλους λόγους, και την πιθανή εγγύτητα με σχολεία, νοσοκομεία και της κατοικίες έξω από τα όρια του λιμένα.

Το βασικό σχέδιο πρέπει να προβλέπει τις γενικές διαδικασίες και τον έλεγχο. Είναι απαραίτητο να συμπληρώνεται με λεπτομερή υπο-σχέδια για κάθε συγκεκριμένο τύπο έκτακτης ανάγκης. Κάθε λεπτομερές υπο-σχέδιο διέπεται από τις ίδιες γενικές διαδικασίες και από τον ίδιο έλεγχο, αλλά οι λεπτομερείς προγραμματισμένες ενέργειες θα διαφέρουν απαραιτήτως. Για παράδειγμα, η απόκριση σε έναν θυελλώδη άνεμο θα είναι πολύ διαφορετική από την απόκριση σε μια σημαντική πυρκαγιά ή μια έκρηξη.

Το σχέδιο πρέπει να καλύψει όλους τους τύπους έκτακτων αναγκών που θα μπορούσαν να εμφανιστούν στο λιμένα και να περιλάβουν τις αντιδράσεις που είναι κατάλληλες για τη δριμύτητα του γεγονότος. Η απόκριση θα είναι ανάλογη με την εξέλιξη του γεγονότος.

Το σχέδιο έκτακτης ανάγκης πρέπει να δημοσιευθεί μέσα σε λογικό χρόνο από την ολοκλήρωσή του, και να τεθεί υπόψη όλων εκείνων που εμπλέκονται στην εφαρμογή του. Στα σχέδιο πρέπει να γίνεται άσκηση ετοιμότητας. Η συχνότητα των ασκήσεων καθορίζεται με βάση τις τοπικές περιστάσεις (ILO, 2005:448). Όλα τα σχέδια έκτακτης ανάγκης πρέπει να υπόκεινται σε αναθεώρηση.

Η χρήση του σχεδίου σε ένα πραγματικό γεγονός έκτακτης ανάγκης μπορεί να χρησιμοποιηθεί ως τμήμα μιας συστηματικής αναθεώρησης της λειτουργίας του σχεδίου. Όταν δεν λαμβάνουν χώρα πραγματικά γεγονότα, η συνήθης περίοδος αναθεώρησης είναι το δωδεκάμηνο αν και αυτό εξαρτάται από τις τοπικές περιστάσεις.

Σημαντικός είναι ο ρόλος του Κέντρου Ελέγχου Έκτακτης Ανάγκης (ILO, 2005:447). Το Κέντρο αυτό σε περίπτωση έκτακτης ανάγκης θα κατευθύνει και θα συντονίζει τις κύριες αντιδράσεις. Το κέντρο πρέπει να είναι:

- Τοποθετημένο, σχεδιασμένο και εξοπλισμένο με τέτοιο τρόπο ώστε να παραμείνει λειτουργικό σε όλη τη διάρκεια της έκτακτης ανάγκης.
- Εξοπλισμένο για να λάβει και να στείλει τις πληροφορίες και να διαχέει πληροφορίες εντός και εκτός λιμένα.

- Εξοπλισμένο με ένα ικανοποιητικό αριθμό εσωτερικών και εξωτερικών δικτύων επικοινωνίας.

- Εξοπλισμένο με τους λεπτομερείς χάρτες της περιοχής του λιμένα, με ενημερωμένο κατάλογο του προσωπικού έκτακτης ανάγκης και τη θέση του σχετικού εξοπλισμού έκτακτης ανάγκης όπως είναι ο εξοπλισμός ασφάλειας, τα συστήματα πυρόσβεσης, τα υλικά ουδετεροποίησης, τα απορροφητικά υλικά και οι αγωγοί πετρελαίου.

Επίσης πρέπει να προβλέπεται η παραχώρηση χώρου στα Μέσα Μαζικής Ενημέρωσης κατά τη διάρκεια μιας έκτακτης ανάγκης. Ο χώρος αυτός πρέπει να είναι ξεχωριστός από το κέντρο ελέγχου έκτακτης ανάγκης ώστε να μην προκαλούνται διαταραχές στη λειτουργία του κέντρου.

Το νομικό πλαίσιο ασφάλειας λιμένα από φυσικά φαινόμενα στην Ελλάδα.

Σύμφωνα με τους Ν. 2344/1995 και Ν. 3013/2002 αρμόδια για θέματα φυσικών καταστροφών είναι η Γενική Γραμματεία Πολιτικής Προστασίας (ΓΠΠΠ) η οποία έχει εκπονήσει το Γενικό Σχέδιο Πολιτικής Προστασίας γνωστό ως «ΞΕΝΟΚΡΑΤΗΣ» (ΥΑ 1299/2003, ΦΕΚ 423/Β).

Ο σκοπός του Γενικού Σχεδίου είναι η διαμόρφωση ενός συστήματος αποτελεσματικής αντιμετώπισης καταστροφικών φαινομένων για την προστασία της ζωής, της υγείας και της περιουσίας των πολιτών, καθώς και η προστασία του φυσικού περιβάλλοντος. Στο σχέδιο αυτό καθορίζονται τα είδη των καταστροφών και οι αντίστοιχοι όροι πολιτικής προστασίας και καθορίζονται ρόλοι και δίνονται κατευθύνσεις σχεδίασης σε Υπουργεία, Περιφέρειες, Νομαρχιακές Αυτοδιοικήσεις, Δήμους και Κοινότητες. Επίσης προσδιορίζονται οι εμπλεκόμενες υπηρεσίες, οι φορείς και τα όργανα που διευθύνουν και συντονίζουν τις επιχειρησιακές δυνάμεις σε όλα τα επίπεδα. Με βάση το γενικό αυτό σχέδιο παρέχονται ουσιώδη στοιχεία για την αξιολόγηση των κινδύνων, την επισήμανση των ευπαθών χώρων και την εκπόνηση ειδικών σχεδίων για κάθε κίνδυνο και κατευθυντήριες γραμμές για τη χάραξη στρατηγικών και τακτικών, την ορθή οργάνωση και εξοπλισμό των υπηρεσιών και τη διαμόρφωση επιχειρησιακής φιλοσοφίας και την έγκαιρη κινητοποίηση, δραστηριοποίηση, διεύθυνση και συντονισμό του ανθρώπινου δυναμικού και των μέσων.

Σύμφωνα με το Γενικό Σχέδιο Πολιτικής Προστασίας - Ξενοκράτης το Υπουργείο Εμπορικής Ναυτιλίας έχει την υποχρέωση να σχεδιάζει, στο πλαίσιο των αρμοδιοτήτων του και με βάση το σχέδιο αυτό, μέτρα αντιμετώπισης φυσικών, τεχνολογικών και άλλων καταστροφών. Τα σχέδια αυτά εγκρίνονται από τη Γενική Γραμματεία Πολιτικής Προστασίας.

Στο πλαίσιο αυτό οι Λιμενικές Αρχές εκπροσωπούνται στο Συντονιστικό Νομαρχιακό Όργανο που λειτουργεί σε κάθε Νομαρχιακή Αυτοδιοίκηση. Κάθε Λιμενική Αρχή καταρτίζει ανάλογα με το φυσικό κίνδυνο αντίστοιχο σχέδιο σύμφωνα με το σχέδιο «Ξενοκράτης».

Από τη μελέτη των σχετικών σχεδίων δεν προκύπτει εξειδίκευση του σχεδίου «Ξενοκράτης» για τους λιμενικούς χώρους. Η συμμετοχή της Λιμενικής Αρχής συνίσταται στην εφαρμογή των αποφάσεων που λαμβάνει το Συντονιστικό Όργανο της Νομαρχιακής Αυτοδιοίκησης και μάλιστα στην κινητοποίηση των πλοίων για την απομάκρυνση των πολιτών κατόπιν σχετικής απόφασης της Πολιτικής Προστασίας.

1.6.3 Ασφάλεια λιμένων (Port Security)

Η ασφάλεια ενός λιμένα αναφέρεται στην αποφυγή διάπραξης παράνομων ενεργειών στο χώρο του λιμένα είτε αυτές αφορούν τις εγκαταστάσεις είτε τα πρόσωπα, είτε τα πλοία που είναι παραβεβλημένα (ILO-IMO, 2004:1).

Η αξιολόγηση της ασφάλειας της λιμενικής εγκατάστασης σημαίνει μια ανάλυση που εξετάζει και αξιολογεί τις πιθανές απειλές, τις τρωτότητες και τα υπάρχοντα προστατευτικά μέτρα, τις διαδικασίες και τις λειτουργίες. Οι πιθανές απειλές στις βασικές λειτουργίες της λιμενικής εγκατάστασης και του πλοίου μπορούν να περιλάβουν την τοποθέτηση βομβών, τη δολιοφθορά, τη μη εξουσιοδοτημένη χρήση, το λαθρεμπόριο, την παραβίαση φορτίου και τους λαθρεπιβάτες.

Το νομικό πλαίσιο ασφάλειας λιμένων (port security) στην Ελλάδα.

Η αναθεωρημένη Διεθνής Σύμβαση για την Ασφάλεια της Ζωής στη Θάλασσα (SOLAS 1974), με την υιοθέτηση του Διεθνούς Κώδικα για την Ασφάλεια Πλοίων και Λιμενικών Εγκαταστάσεων από Έκνομες Ενέργειες (ISPS Code), σε συνδυασμό με τον Κανονισμό (ΕΚ) 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρωπαϊκής Ένωσης αποτελούν το βασικό πλαίσιο ασφάλειας για τις λιμενικές εγκαταστάσεις.

Σε κάθε λιμένα πρέπει να αναπτύσσεται ένα αποτελεσματικό σχέδιο ασφάλειας λιμενικών εγκαταστάσεων. Στο σχέδιο αυτό προβλέπεται με κάθε λεπτομέρεια η προετοιμασία, η πρόληψη και οι δραστηριότητες απόκρισης των αρμοδίων φορέων ανά επίπεδο απειλής. Ο φορέας διαχείρισης της λιμενικής εγκατάστασης πρέπει να τεκμηριώνει το σχέδιο ασφάλειας με γραπτή μορφή.

Στο σχέδιο αυτό πρέπει να προβλέπονται οι δραστηριότητες που είναι αναγκαίες για την πρόληψη ή την αποτροπή έκνομων γεγονότων στην ασφάλεια των μεταφορών. Για την επίτευξη του στόχου αυτού πρέπει, σύμφωνα με το Υπουργείο Εμπορικής Ναυτιλίας (ΥΕΝ 2003:10)

> α) να προσδιορισθούν επαρκείς πόροι που απαιτούνται για να εκτελεσθούν τα καθορισμένα καθήκοντα ασφάλειας,
>
> β) να καθορισθούν ζώνες περιορισμένης πρόσβασης για να εξασφαλισθεί ότι μόνο τα εξουσιοδοτημένα πρόσωπα έχουν πρόσβαση,

γ) να ελέγχονται οι προσβάσεις στη λιμενική εγκατάσταση,

δ) να εποπτεύεται η ασφάλεια του φορτίου και των εφοδίων του πλοίου και

ε) να εξασφαλίζεται ότι η επικοινωνία ασφάλειας είναι εύκολα διαθέσιμη και σε ετοιμότητα.

Έτσι το σχέδιο ασφάλειας της λιμενικής εγκατάστασης πρέπει τουλάχιστον να περιλαμβάνει (ILO-IMO, 2004:37)

α) τα καθήκοντα του προσωπικού ασφάλειας και ιδιαίτερα τα καθήκοντα του προσωπικού της Λιμενικής Εγκατάστασης αρμόδιου για θέματα ασφάλειας της εγκατάστασης, τις διαδικασίες που αφορούν τον έλεγχο των δραστηριοτήτων σε θέματα ασφάλειας, τις διαδικασίες για την εκπαίδευση, τα γυμνάσια και τις ασκήσεις, τις διαδικασίες για την απαίτηση παρουσίας προσωπικού έκτακτης ανάγκης, ασφάλειας ναυσιπλοΐας, ή προσωπικού ασφάλειας για αντιμετώπιση έκνομων ενεργειών, συμπεριλαμβανομένων τοπικών υπηρεσιών αστυνομίας και πυροσβεστικής, μονάδων πυροτεχνουργών, δυτών, νοσοκομειακών υπηρεσιών κ.λπ. και τον προσδιορισμό του υπευθύνου ασφάλειας της λιμενικής εγκατάστασης.

β) τα μέτρα πρόληψης έκνομων ενεργειών και ιδίως τα μέτρα και ο εξοπλισμός με στόχο την πρόληψη και αποτροπή της μη εξουσιοδοτημένης μεταφοράς όπλων, επικίνδυνων ουσιών, και συσκευών που προορίζονται για χρήση ενάντια σε ανθρώπους, πλοία, ή λιμένες, ο προσδιορισμός των ζωνών περιορισμένης πρόσβασης και των μέτρων ή του εξοπλισμού για την πρόληψη της μη εξουσιοδοτημένης πρόσβασης στη λιμενική εγκατάσταση και στις ζώνες περιορισμένης πρόσβασης της λιμενικής εγκατάστασης, διαδικασίες για τη διασύνδεση των δραστηριοτήτων ασφάλειας λιμένων και πλοίων και τα μέτρα που αποσκοπούν στην αποτελεσματική ασφάλεια του φορτίου και του εξοπλισμού διακίνησης του φορτίου στην λιμενική εγκατάσταση.

γ) την αναθεώρηση του Σχεδίου Ασφάλειας και ιδίως τις διαδικασίες για την περιοδική αναθεώρηση και την ενημέρωση του σχεδίου, τα μέτρα για να εξασφαλιστεί το απόρρητο των πληροφοριών που περιλαμβάνονται στο σχέδιο και τις διαδικασίες για τον έλεγχο του σχεδίου της λιμενικής εγκατάστασης.

δ) τις διαδικασίες απόκρισης στις απειλές ασφάλειας και ιδίως τις διαδικασίες απόκρισης στις απειλές ασφάλειας ή τις παραβιάσεις ασφάλειας, συμπεριλαμβανομένων των προβλέψεων για τη διατήρηση των ζωτικών λειτουργιών της λιμενικής εγκατάστασης ή της διασύνδεσης πλοίου και λιμένα, τις διαδικασίες εκκένωσης σε περίπτωση απειλών ασφάλειας ή παραβιάσεων της ασφάλειας, τις διαδικασίες απόκρισης σε περίπτωση που έχει ενεργοποιηθεί το σύστημα προειδοποίησης ασφαλείας ενός πλοίου στην λιμενική εγκατάσταση και τις διαδικασίες για την εξυπηρέτηση επαναπατρισμού του πληρώματος του πλοίου καθώς επίσης και της πρόσβασης των επισκεπτών στο πλοίο συμπεριλαμβανομένων των αντιπροσώπων των συνδικαλιστικών οργανώσεων των ναυτικών.

Σε κάθε λιμενική εγκατάσταση πρέπει να υπάρχει ένας υπεύθυνος ασφάλειας. Τα καθήκοντα και οι ευθύνες του υπεύθυνου ασφάλειας λιμενικής εγκατάστασης περιλαμβάνουν τις ακόλουθες αρμοδιότητες (YEN, 2003:9):

- Προετοιμασία μιας αρχικής γενικής αξιολόγησης ασφάλειας της λιμενικής εγκατάστασης προκειμένου να εκπονηθεί ένα σχέδιο ασφάλειας λιμενικών εγκαταστάσεων.

- Εφαρμογή και άσκηση του σχεδίου ασφάλειας λιμενικών εγκαταστάσεων.

- Τήρηση των κανονικών επιθεωρήσεων ασφάλειας της λιμενικής εγκατάστασης ώστε να εξασφαλισθεί η συνέχεια των κατάλληλων μέτρων ασφάλειας.

- Σύσταση και ενσωμάτωση, ανάλογα με την περίπτωση, των τροποποιήσεων του σχεδίου ασφάλειας λιμενικής εγκατάστασης προκειμένου να διορθωθούν οι ελλείψεις και για να ενημερωθεί το σχέδιο ώστε να λάβει υπόψη τις σχετικές αλλαγές της εγκατάστασης.

- Εξασφάλιση επαρκούς κατάρτισης για το προσωπικό που είναι αρμόδιο για την ασφάλεια της λιμενικής εγκατάστασης.

- Συντονισμένη εφαρμογή του σχεδίου ασφάλειας λιμενικής εγκατάστασης με τον πλοίαρχο ή τον Αξιωματικό ασφάλειας πλοίου ανάλογα με την περίπτωση.

- Συντονισμό με τις υπηρεσίες ασφάλειας, ανάλογα με την περίπτωση.

- Ρύθμιση για την έγκαιρη αντιμετώπιση του συμβάντος από την αρμόδια δημόσια αρχή.

Για την ανάπτυξη του σχεδίου ασφαλείας της λιμενικών εγκαταστάσεων απαραίτητη είναι η αξιολόγηση της ασφάλειας της εγκατάστασης. Εκτός από τις περιοδικές αναπροσαρμογές και τις αναθεωρήσεις, η αξιολόγηση ασφάλειας της λιμενικής εγκατάστασης παρέχει την δυνατότητα στο φορέα διαχείρισης να ελέγχει τη συμμόρφωση με το σχέδιο ασφάλειας της λιμενικής εγκατάστασης και να προβαίνει σε τροποποιήσεις ανάλογα με τις ανάγκες.

Πριν από την έναρξη της αξιολόγησης της ασφάλειας της λιμενικών εγκαταστάσεων, ο υπεύθυνος ασφάλειας εκτιμά τις τρέχουσες πληροφορίες για την αξιολόγηση της απειλής της τοπικής περιοχής και πρέπει να είναι εξοικειωμένος με τον τύπο των πλοίων που εξυπηρετεί η λιμενική εγκατάσταση. Ο υπεύθυνος προσδιορίζει και αξιολογεί τις πιθανές απειλές σε ζωτικές λειτουργίες της λιμενικής εγκατάστασης, σε στοιχεία του ενεργητικού και στην υποδομή της, και την πιθανότητα να λάβει χώρα το περιστατικό προκειμένου να καθιερωθούν μέτρα ασφαλείας και να δοθεί προτεραιότητα σε αυτά.

Ο υπεύθυνος ασφάλειας λιμενικής εγκατάστασης εξετάζει τα σημεία πρόσβασης σ΄ αυτή, όπως τη σιδηροδρομική, την οδική και τη θαλάσσια πρόσβαση και αξιολογεί την πιθανότητα να χρησιμοποιηθούν από μη εξουσιοδοτημένα άτομα που μπορούν να προκαλέσουν ένα έκνομο γεγονός στην ασφάλεια των μεταφορών. Στα άτομα αυτά περιλαμβάνονται τόσο εκείνα που διαθέτουν νόμιμη πρόσβαση όσο και εκείνα που επιδιώκουν να επιτύχουν μη εξουσιοδοτημένη είσοδο. Η αξιολόγηση ασφάλειας της λιμενικής εγκατάστασης πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία (YEN, 2003:10):

- Το γενικό σχεδιάγραμμα της λιμενικής εγκατάστασης.

- Τη θέση και τη λειτουργία κάθε πραγματικού ή πιθανού σημείου πρόσβασης της λιμενικής εγκατάστασης.

- Τα υπάρχοντα προστατευτικά μέτρα του εξοπλισμού ελέγχου και παρακολούθησης, της επικοινωνίας και των εγγράφων προσδιορισμού του προσωπικού και του συναγερμού, του φωτισμού, του ελέγχου της πρόσβασης, και των παρόμοιων συστημάτων.

- Την αριθμητική δύναμη του προσωπικού της λιμενικής εγκατάστασης.

- Τις πύλες, τα κιγκλιδώματα και το φωτισμό ασφάλειας.

- Τη θέση των περιοχών με περιορισμένη πρόσβαση, όπως των σταθμών ελέγχου, των κέντρων επικοινωνιών, των περιοχών αποθήκευσης φορτίων, κ.λπ.

- Τον εξοπλισμό έκτακτης ανάγκης και τον εφεδρικό εξοπλισμό που είναι διαθέσιμοι για να υποστηρίξουν τις ουσιώδεις υπηρεσίες.

- Τις διαδικασίες δράσης για πυρκαγιά ή για άλλες καταστάσεις έκτακτης ανάγκης.

- Τον υπάρχοντα εξοπλισμό προστασίας και ασφάλειας για την προστασία του προσωπικού και των επισκεπτών.

- Το επίπεδο επίβλεψης του προσωπικού της λιμενικής εγκατάστασης, των προμηθευτών, των τεχνικών επισκευής, των εργαζομένων στις αποβάθρες, κ.λπ.

- Τις υπάρχουσες συμφωνίες με ιδιωτικές επιχειρήσεις ασφάλειας που παρέχουν υπηρεσίες ασφάλειας εγκαταστάσεων και παραβεβλημένων πλοίων.

- Τις διαδικασίες φορτίου και εφοδίων πλοίου.

- Την ικανότητα απόκρισης στα γεγονότα.

Η αξιολόγηση της ασφάλειας μιας λιμενικής εγκατάστασης πρέπει να τεκμηριωθεί και να διατηρηθεί από την εγκατάσταση. Η αξιολόγηση ασφάλειας της εγκατάστασης πρέπει να εκτελείται περιοδικά, λαμβάνοντας υπόψη τις μεταβαλλόμενες απειλές ή τις σημαντικές αλλαγές στην εγκατάσταση. Για το σκοπό αυτό πραγματοποιούνται γυμνάσια και ασκήσεις ώστε να εξασφαλίζεται η επάρκεια των εκπονηθέντων σχεδίων ασφάλειας των λιμενικών εγκαταστάσεων.

ΚΕΦΑΛΑΙΟ 2 Εργαλεία Ανάλυσης Κινδύνων

Η ανάλυση κινδύνων είναι μια σύνθετη διαδικασία. Η διαχείριση των πληροφοριών που συλλέγονται είναι ανάλογη με το εύρος της. Για τη διευκόλυνση της ανάλυσης κίνδυνων, ορισμένες εταιρίες ανέπτυξαν διάφορες μεθόδους. Αυτό ήταν ένα σημαντικό βήμα για να ελαχιστοποιηθεί η παρέμβαση εξωτερικών ειδικών συνεργατών στα εσωτερικά μιας εταιρείας ή ενός οργανισμού. Αρχικά τα προγράμματα που σχεδιάστηκαν ήταν απλά και περιορίζονταν σε απλούς υπολογισμούς. Στην συνέχεια, όμως, λόγω της αύξησης της πολυπλοκότητας των πληροφοριακών συστημάτων καθώς και των προβλημάτων ασφαλείας, τα προγράμματα για ανάλυση κινδύνων έλαβαν πιο ενεργό ρόλο αναλαμβάνοντας την διευκόλυνση του συνόλου της ανάλυσης κινδύνων με πολλά διαφορετικά εργαλεία. Μάλιστα, κατά την δεκαετία του ’90 που τέτοια προγράμματα βγήκαν στην ελεύθερη αγορά, ο ανταγωνισμός οδήγησε τις εταιρίες ανάπτυξής τους να προσθέσουν νέα χαρακτηριστικά ώστε τελικά να καταλήξουν σε μεγάλα πακέτα εφαρμογών. Παρακάτω περιγράφονται οι δυνατότητες, τα χαρακτηριστικά και τα εργαλεία που έχουν αναπτυχθεί όλα αυτά τα χρόνια για το λογισμικό ανάλυσης κινδύνων.

2.1 Callio Secura 17799

Το Callio Secura 17799 είναι ένα σύστημα διαχείρισης ασφάλειας πληροφοριακών συστημάτων με έμφαση στην συμμόρφωση με το διεθνές πρότυπο BS7799 / ISO 17799. Βασίζεται σε μια δική του μέθοδο για την ανάλυση κινδύνων που είναι σχετικά απλή, βήμα προς βήμα, ώστε να γίνεται εύκολα κατανοητή και να μην απαιτεί ειδικευμένο προσωπικό για την χρήση του. Ανήκει δε στην κατηγορία των ποιοτικών μεθόδων. Αναπτύχθηκε το 2001 στον Καναδά. Το πρόγραμμα δημιουργεί έναν ιστότοπο στον οποίο μπορούν να έχουν πρόσβαση από παντού όσοι συμμετέχουν στην ανάλυση κινδύνων και χρησιμοποιείται επίσης για την ενημέρωση και εκπαίδευση του προσωπικού για θέματα ασφαλείας, τις υπάρχουσες πολιτικές ασφαλείας, τις διαδικασίες κτλ. Περιέχει όλα εκείνα τα εργαλεία που χρειάζονται για την συνεχή διαχείριση και βελτίωση όλων των εγγράφων ασφαλείας του οργανισμού (πχ. version control). [14]

2.2 MEHARI (Méthode Harmonisée d’analyse de Risques Informatiques)

Σχεδιάστηκε από ειδικούς ασφάλειας του CLUSIF (Club de la Sécurité Informatique Français) και αντικατέστησε τις προηγούμενες μεθόδους MARION και MELISA. Αναπτύχθηκε το 1996. Παρέχει ένα μοντέλο αποτίμησης επικινδυνότητας και αρθρωτά συστατικά και διαδικασίες. Περιέχει τύπους που διευκολύνουν την αναγνώριση και χαρακτηρισμό των απειλών και τη βέλτιστη επιλογή διορθωτικών μέτρων. Έχει λίστα σημείων ευπαθειών που πρέπει να ελεγχθούν και είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 13335.

2.3 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Ανακοινώθηκε το 1999, από το Software Engineering Institute του Carnegie- Mellon University. Η OCTAVE είναι αυτοκατευθυνόμενη, με την έννοια ότι μια μικρή ομάδα ατόμων από τις επιχειρησιακές μονάδες και τη Διεύθυνση Πληροφορικής εργάζονται μαζί για να ικανοποιήσουν τις ανάγκες ασφάλειας του οργανισμού. Η OCTAVE-S είναι μια παραλλαγή της μεθόδου για μικρούς (λιγότερα από 100 άτομα) οργανισμούς. Το Octave Automated Tool αναπτύχθηκε από το Advanced Technology Institute (ATI) προκειμένου να υποστηρίζει τους χρήστες της OCTAVE

2.4 COBRA

'Ενα από τα πλεονεκτήματα της COBRA είναι η αυτόματη προσαρμογή της ανάλυσης στις ανάγκες της εκάστοτε εταιρείας, καθώς χρησιμοποιεί τη δική της μέθοδο για να επιτευχθεί η αρμονία με το διεθνές προτυπο ISO/IEC 17799. Παρ 'όλο ότι είναι ένα από τα πιο παλιά προγράμματα που έχουν κυκλοφορήσει, έχει το πλεονέκτημα της αυτόματης προσαρμογής της ανάλυσης κινδύνων στα προβλήματα της εκάστοτε εταιρείας. Έχει την δυνατότητα, επίσης, για την δημιουργία αναφορών επαγγελματικού επιπέδου είτε για την διοίκηση της εταιρείας, είτε για το τεχνικό προσωπικό. Τρέχει σε λειτουργικό σύστημα Windows με κάποια διεπαφή χρήστη (User Interface). Επίσης, για πιο απαιτητικές αναλύσεις επιτρέπεται η πλήρης παραμετροποίηση των γνωσιακών βάσεων (base of knowledge) που περιέχει. Περιλαμβάνεται επιπλέον και η λεγόμενη «What if» ανάλυση, κατά την οποία ελέγχονται υποθετικά σενάρια ώστε να διαπιστωθεί δυναμικά η επίδραση που θα έχουν συγκεκριμένα αντίμετρα στους βαθμούς κινδύνου. Έχει σχεδιαστεί από την εταιρεία C&A System Security Ltd. Μετρά το βαθμό επικινδυνότητας για κάθε περιοχή ενός συστήματος και τον συνδέει με την πιθανή επιχειρησιακή επίπτωση. Προσφέρει επίσης λεπτομερείς λύσεις και συστάσεις μείωσης της επικινδυνότητας.

2.5 IT-Grundschutz

Αναπτύχθηκε το 1994. Περιέχει και γενικές συστάσεις για την δημιουργία μιας εφαρμόσιμης διαδικασίας ασφάλειας και λεπτομερείς τεχνικές οδηγίες για την επίτευξη του απαραίτητου επιπέδου ασφάλειας σε συγκεκριμένα πεδία. Η διαδικασία ασφάλειας που προβλέπει η IT-Grundschutz αποτελείται από τα εξής βήματα: αρχικοποίηση της διαδικασίας, καθορισμός στόχων ασφάλειας και επιχειρησιακού περιβάλλοντος, καθιέρωση οργανωτικής δομής για την ασφάλεια, παροχή των απαραίτητων πόρων, δημιουργία της έννοιας της ασφάλειας, ανάλυση της πληροφοριακής υποδομής, αποτίμηση απαιτήσεων προστασίας, μοντελοποίηση, έλεγχος ασφάλειας, συμπληρωματική ανάλυση ασφάλειας, σχεδιασμός υλοποίησης και υλοποίηση, συντήρηση, παρακολούθηση και βελτίωση της διαδικασίας και πιστοποίηση (προαιρετικά). Η IT-Grundschutz υποστηρίζεται από το εργαλείο Gstool που αναπτύχθηκε από το Federal Office for Information Security (BSI). Η μέθοδος αυτή είναι συμβατή με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001

2.6 EBIOS

Η EBIOS αναπτύχθηκε το 1995 από την DCSSI (Direction Centrale de la Sécurité des Systèmes d' Information) της Γαλλικής κυβέρνησης. Λαμβάνει υπόψη τόσο τεχνικές όσο και μη τεχνικές οντότητες. Επιτρέπει σε όλο το προσωπικό που χρησιμοποιεί το ΠΣ να εμπλακεί στα θέματα ασφάλειας και προσφέρει μια δυναμική προσέγγιση που ενθαρρύνει τη διάδραση ανάμεσα στις διάφορες λειτουργίες του οργανισμού, εξετάζοντας το συνολικό κύκλο ζωής του συστήματος.

Η EBIOS είναι συμβατή με τα πρότυπα ISO/IEC 27001, ISO/IEC 13335 (GMITS), ISO/IEC 15408 (Common Criteria), ISO/IEC 17799 και ISO/IEC 21827.

Το 2002, διεθνείς συγκρίσεις τοποθετούν την EBIOS μεταξύ των τριών καλύτερων μεθόδων για την ανάλυση πληροφοριακών κινδύνων. Πολλές οργανώσεις του δημόσιου και του ιδιωτικού τομέα καθώς και Υπουργεία Άμυνας πολλών χωρών χρησιμοποιούν τη μέθοδο για να πραγματοποιούν τις δικές τους αναλύσεις πληροφοριακού κινδύνου.

2.7 CounterMeasures

Η CounterMeasures είναι προϊόν της Allion για διαχείριση επικινδυνότητας βασισμένο στις σειρές αμερικανικών προτύπων US-NIST 800 και OMB Circular A-130. Ο χρήστης αρχικοποιεί τα κριτήρια αξιολόγησης και χρησιμοποιώντας μια "tailor-made" λίστα ελέγχου αποτίμησης, το λογισμικό παρέχει αντικειμενικά κριτήρια αξιολόγησης για να αποφασίσει ο χρήστης τον βαθμό ασφάλειας και συμμόρφωσης με τα πρότυπα.

2.8 PROTEUS

Η Proteus είναι σύνολο προϊόντων της Infogov, που αναπτύχθηκε το 1999. Επιτρέπει τη διεξαγωγή ανάλυσης κενών στη συμμόρφωση με πρότυπα όπως το ISO 17799 ή τη δημιουργία και διαχείριση ενός συστήματος διαχείρησης ασφάλειας πληροφοριών (ISMS – Information Security Management System) σύμφωνα με το πρότυπο ISO 27001 (BS 7799-2). Το Proteus Enterprise είναι μια πλήρως ολοκληρωμένη Web-based εφαρμογή για διαχείριση επικινδυνότητας για μεγάλες επιχειρήσεις. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001.

2.9 RA2 Art of Risk

Η RA2 Art of Risk είναι εργαλείο της AEXIS, που αντικατέστησε το RA Software Tool και ανακοινώθηκε το 2000. Είναι σχεδιασμένο για να βοηθήσει τις επιχειρήσεις να αναπτύξουν ένα ISMS συμβατό με το πρότυπο ISO/IEC 27001:2005 (προηγουμένως BS 7799 Part 2:2002) και τον κώδικα πρακτικής ISO/IEC 27002.

Το RA2 Information Collection Device, ένα συστατικό που διανέμεται μαζί με το εργαλείο, μπορεί να εγκατασταθεί οπουδήποτε στον οργανισμό υπάρχει ανάγκη για συλλογή πληροφορίας προς χρήση από τη διαδικασία αποτίμησης επικινδυνότητας. Είναι συμβατό με τα πρότυπα ISO/IEC 17799 και ISO/IEC 27001

2.10 CRAMM

Το CRAMM είναι ένα εργαλείο ποιοτικής ανάλυσης κινδύνων που αναπτύχθηκε από το CCTA (Central Computer and Telecommunications Agency) της βρετανικής κυβέρνησης το 1985 ώστε να εφοδιάσει τα διάφορα τμήματα της κυβέρνησης με μια κοινή μέθοδο ανάλυσης κινδύνων Πληροφοριακών Συστημάτων. Το πρόγραμμα, το οποίο έχει υποστεί σημαντικές αναθεωρήσεις και βρίσκεται σήμερα στην έκδοση 5, συνεχίζει να αναπτύσσεται πλέον από την εμπορική εταιρία Insight Consulting που έχει έδρα στην Αγγλία. Το CRAMM έχει μεγάλο κύρος, καθώς χρησιμοποιείται σε παραπάνω από 500 οργανισμούς σε 23 χώρες, συμπεριλαμβανομένου και του NATO. Το πρόγραμμα ακολουθεί την δική του μέθοδο, η οποία αποτιμά και βοηθάει τους οργανισμούς να επιτύχουν συμμόρφωση με το διεθνές πρότυπο ISO17799/BS7799. Τα βασικά χαρακτηριστικά του προγράμματος είναι :

- Μεγάλη βάση αντιμέτρων που ανανεώνεται συνεχώς και καλύπτει όλες τις πτυχές της ασφάλειας πληροφοριακών συστημάτων.
- «What if» ανάλυση
- Εργαλεία για την δημιουργία σχεδίων Επιχειρηματικής Συνέχειας (Business Continuity)
- Οδηγούς για την δημιουργία πολιτικών ασφαλείας
- Οδηγούς για την δημιουργία αναφορών
- Σχετικά σύγχρονο περιβάλλον σε πλατφόρμα MS Windows
- Δυνατότητα προσαρμογής του προγράμματος στις ανάγκες του κάθε οργανισμού σε συνεννόηση με την εταιρία.

Υπάρχει και η έκδοση CRAMM Express η οποία δεν περιλαμβάνει όλα τα εργαλεία της κανονικής έκδοσης αλλά είναι πιο απλή στην χρήση και οδηγεί σε πιο γρήγορα αλλά λιγότερο αναλυτικά αποτελέσματα.

2.11 Ezrisk

Το Ezrisk είναι ένα προϊόν που σχεδιάστηκε από την εταιρία Ezrisk Limited και στοχεύει κυρίως στις μικρομεσαίες επιχειρήσεις. Οι επιχειρήσεις αυτές συνήθως δεν έχουν ειδικούς για να διεξάγουν τις δικές τους αναλύσεις κινδύνων και ούτε έχουν τους πόρους για να αγοράσουν ανάλογες υπηρεσίες. Το πρόγραμμα Ezrisk είναι φθηνό και εξαιρετικά απλό, ώστε να μην χρειάζεται ειδική εκπαίδευση για την χρήση του. Περιέχει αλγορίθμους που ελέγχουν τα δεδομένα που εισάγει ο χρήστης, αναγνωρίζουν τυχόν σφάλματα ή αντιφάσεις και βοηθούν στην επίλυσή τους. Είναι συμβατό με το διεθνές πρότυπο ISO17799/BS7799 και βοηθάει στην επίτευξη συμμόρφωσης με αυτό. Μπορεί να παράγει αναφορές σε απλή και κατανοητή μορφή, εξηγώντας τους κινδύνους και τα αντίμετρα που προτείνονται σε κάθε περίπτωση. Τέλος, δημιουργεί ένα σχέδιο δράσης που δείχνει τα βήματα που πρέπει να ακολουθηθούν

μέχρι την επίτευξη συμμόρφωσης με το διεθνές πρότυπο ISO17799/BS7799, βάσει της προτεραιότητάς τους.

2.12 RiskWatch for Information Systems & ISO 17799

Η εταιρία RiskWatch ειδικεύεται στην δημιουργία προγραμμάτων ανάλυσης κινδύνων για πολλούς τομείς, μεταξύ των οποίων και ο τομέας της ασφάλειας πληροφοριακών συστημάτων. Η κύρια διαφορά του σε σχέση με τα περισσότερα προγράμματα του ανταγωνισμού είναι η χρήση μιας ποσοτικής μεθόδου ανάλυσης κινδύνων. Το πρόγραμμα περιέχει πολυετή δεδομένα ποσοτικής ανάλυσης που χρησιμοποιούνται έτοιμα για την εξοικονόμηση χρόνου και προσπάθειας. Εναι ιδιαίτερα δημοφιλής στις ΗΠΑ και έχει μεγάλο κύρος καθώς χρησιμοποιείται σε πολλές κυβερνητικές υπηρεσίες και μεγάλους ιδιωτικούς οργανισμούς. Μερικοί από αυτούς είναι : το Υπουργείο Αμύνης των ΗΠΑ, το Πεντάγωνο, η NSA (National Security Agency), η AT&T και η Vodafone

2.13 Security by Analysis (SBA)

Αναπτύχθηκε στη Σουηδία στις αρχές του ’80. Χρησιμοποιείται έκτοτε με επιτυχία σχεδόν αποκλειστικά στις Σκανδιναβικές χώρες. Δέχεται ότι οι άνθρωποι που συμμετέχουν στην καθημερινή λειτουργία του Πληροφοριακού Συστήματος έχουν τις περισσότερες πιθανότητες να εντοπίσουν τα προβλήματα και να προτείνουν λύσεις. Αποτελείται από ένα σύνολο μεθόδων με κυριότερες τις SBA Check και SBA Scenario. Η SBA Check προσφέρει ταχεία αποτίμηση του επιπέδου ασφάλειας του Π.Σ., στηρίζεται σε ερωτηματολόγια, εχει ως σημείο αναφοράς το ISO/IEC 17799 και υποστηρίζεται από ειδικό λογισμικό.

2.14 CYSM

Το εργαλείο CYSM στοχεύει στην ασφάλεια των λιμένων. Σκοπός του είναι να προσφέρει στους λιμένες την δυνατότητα να βελτιώσουν την τρέχουσα ασφάλειά τους και το επίπεδο ασφάλειας, παρέχοντάς τους καινοτόμες, φιλικές προς το χρήστη, εξατομικευμένες υπηρεσίες διαχείρισης της ασφάλειας, που μπορούν να τους βοηθήσουν να λύσουν προβλήματα στον κυβερνοχώρο ή στην φυσική υποδομή τους.

Το CYSM είναι ένα καινοτόμο συνεργατικό και ολοκληρωμένο εργαλείο με σκοπό την συνεχή αναγνώριση (identification), αξιολόγηση (assessment) και “θεραπεία ” (treatment) των κινδύνων που επικρατούν στα λιμάνια.

ΚΕΦΑΛΑΙΟ 3 Λοιποί κώδικες και η μέθοδός CRAMM

3.1 Λιμενικές εγκαταστάσεις και εφαρμογή του Κώδικα ISPS

Σχεδόν 10 χρόνια μετά την υιοθέτηση του Κώδικα ISM (Διεθνής Κώδικας Ασφαλούς Διαχείρισης Πλοίων) ένας νέος, υποχρεωτικός Κώδικας δημιουργεί νέες απαιτήσεις για τη ναυτιλία προκαλώντας μεγάλες συζητήσεις και ερωτηματικά για το νέο πλαίσιο λειτουργίας των ποντοπόρων πλοίων. Ο Διεθνής Κώδικας ISPS (Διεθνής Κώδικας για την Ασφάλεια των Πλοίων και Λιμενικών Εγκαταστάσεων από έκνομες ενέργειες – International Ship and Port Facility Security Code) χτύπησε την πόρτα της ναυτιλιακής βιομηχανίας το Δεκέμβριο του 2002 σχεδόν 10 ολόκληρα χρόνια μετά την υιοθέτηση του Κώδικα ISM (ως Απόφαση της Ολομέλειας του IMO και ως νέο Κεφάλαιο στη Διεθνή Σύμβαση SOLAS).

Τότε, πολλοί εκπρόσωποι της ναυτιλίας αντιμετώπισαν με σκεπτικισμό τη μονομερή εφαρμογή μέτρων από τα πλοία, που σκόπευαν στη δημιουργία ενός μοντέλου λειτουργίας των ναυτιλιακών εταιρειών, με απώτερο στόχο την ασφάλεια και την προστασία του περιβάλλοντος, τη στιγμή που η γνωστή αλυσίδα της ευρύτερης ναυτιλίας περιλαμβάνει τα λιμάνια, τους τερματικούς σταθμούς, τους νηογνώμονες, τα ναυπηγεία, τους προμηθευτές καυσίμων, τους κατασκευαστές ναυτικού τύπου εξοπλισμού, τα P&I (Protection & Indemnity) Clubs κλπ, όλους δηλαδή αυτούς που επηρεάζουν με κάποιο τρόπο την ασφαλή λειτουργία των πλοίων.

Από τους κρίκους εκείνους της αλυσίδας που δέχθηκαν επικρίσεις για τη μη εφαρμογή ενός παρόμοιου μοντέλου λειτουργίας ήταν τα λιμάνια, η λειτουργία, ο εξοπλισμός και η συντήρηση των οποίων συνδέεται άμεσα με την ασφάλεια της ναυσιπλοΐας και την προστασία του περιβάλλοντος στην ευρύτερη περιοχή δικαιοδοσίας τους. Η απαίτηση για την προέκταση ενός ανάλογου Κώδικα Διαχείρισης Διεθνούς Ασφάλειας (International Safetey Mnagement ή ISM) στους φορείς διαχείρισης λιμένων θεωρήθηκε άστοχη αφού το ζητούμενο εκείνη την εποχή ήταν η βελτίωση της λειτουργίας των πλοίων ιδιαίτερα μετά τα τις τραγωδίες του Estonia (1994), του Herald of Free Enterprise (1987) κ.α.

Ο νέος Κώδικας ISPS που υιοθετήθηκε στις 12 Δεκεμβρίου 2002 (ένα χρόνο μόλις μετά τις τρομοκρατικές επιθέσεις στις Η.Π.Α.) έχει ως πεδίο εφαρμογής όχι μόνο τα φορτηγά πλοία διεθνών πλόων άνω των 500 κόρων ολικής χωρητικότητας (κοχ). και όλα τα επιβατηγά πλοία επίσης διεθνών πλόων, αλλά και τις λιμενικές εγκαταστάσεις στις οποίες καταπλέουν τα παραπάνω πλοία. Ο Κώδικας, προϊόν πολιτικής συναίνεσης των κρατών μελών που συμμετέχουν στις εργασίες του Διεθνούς Ναυτιλιακού Οργανισμού, συμπεριλήφθηκε στις τροποποιήσεις του Κεφαλαίου XI της SOLAS ώστε να καταστεί υποχρεωτικός και αποτελεί πλέον ένα νέο πλαίσιο για την αναγνώριση και διαχείριση απειλών κατά της ασφάλειας πλοίων και λιμανιών με στόχο τον περιορισμό του κινδύνου και των πιθανών επιπτώσεων. Από πλευράς λιμενικών εγκαταστάσεων οι βασικές υποχρεώσεις των φορέων διαχείρισής τους είναι οι εξής:

- τους όρους που θέτει ο Κώδικας ISPS, με αντικειμενικό στόχο τον προσδιορισμό των πιθανών απειλών και των ευαίσθητων σημείων στα οποία ο λιμένας είναι ευάλωτος αλλά και την ανεύρεση τρόπων και μεθόδων εξάλειψης αυτών των αδυναμιών. Ουσιαστικά πρόκειται για μια μελέτη εκτίμησης των μέτρων και του κόστους υλοποίησης αυτών για την εφαρμογή των διατάξεων του Κώδικα στη βάση των ιδιαιτεροτήτων θέσης και λειτουργίας των λιμενικών εγκαταστάσεων. Η παραπάνω Αξιολόγηση γίνεται από αναγνωρισμένους από την Αρχή του κράτους (Υπουργείο Εμπορικής Ναυτιλίας για τα λιμάνια της Ελλάδος) Οργανισμούς Ασφαλείας (ΑΟΑ) οι οποίοι βέβαια πρέπει να πληρούν συγκεκριμένους όρους και προϋποθέσεις που αναφέρονται λεπτομερώς στον Κώδικα. Το τελευταίο χρονικό διάστημα, αιχμές κυρίως από τον περιοδικό τύπο του εξωτερικού εξαπολύθηκαν για την καθυστέρηση της συμμόρφωσης των Ολυμπιακών λιμανιών της χώρας μας, ωστόσο η προπαρασκευή των λιμανιών αυτών έχει ξεκινήσει αρκετά νωρίτερα αφού εκτιμάται ότι στην ουσία αξιοποιείται ο εκπονημένος σχεδιασμός θωράκισης της ασφάλειάς τους κατά τη διάρκεια των Ολυμπιακών Αγώνων. Οι πιθανές απειλές στις ζωτικές λειτουργίες μιας λιμενικής εγκατάστασης που πρέπει να αξιολογηθούν περιλαμβάνουν για παράδειγμα δολιοφθορές, τοποθέτηση βόμβας, λαθρεμπόριο, κλπ. Η μελέτη που γίνεται δεν έχει στατικό χαρακτήρα αλλά πρέπει να γίνεται περιοδικά λαμβάνοντας υπόψη τυχόν αλλαγές στην υποδομή και τη λειτουργία της εγκατάστασης και συνεκτιμώντας τα τυχόν,διαθέσιμα μέτρα ασφαλείας ή τον εγκατεστημένο εξοπλισμό ελέγχου και παρακολούθησης, το σχεδιασμό κατάσβεσης πυρκαγιάς, αντιμετώπισης περιστατικού ρύπανσης της θάλασσας, το σχεδιασμό παραλαβής και διαχείρισης των αποβλήτων των πλοίων κλπ.

- Η κατάρτιση σχεδίου ασφάλειας Λιμενικής Εγκατάστασης, με βάση την Αξιολόγηση Ασφαλείας το οποίο καλύπτει αποτελεσματικά τη διασύνδεση πλοίου/λιμένα (ship – port interface), προβλέποντας τρία επίπεδα ασφαλείας. Τα όρια της λιμενικής εγκατάστασης επεκτείνονται από τη διεπαφή πλοίου – λιμένα μέχρι μια νοητή περίμετρο ασφαλείας που περιλαμβάνει τις περιοχές εκείνες στις οποίες λαμβάνει χώρα ο χειρισμός, η στοιβασία και η αποθήκευση των φορτίων, τις ζώνες περιορισμένης πρόσβασης και τις ζώνες όπου γίνεται η αποβίβαση/επιβίβαση επιβατών. Οι ζώνες περιορισμένης πρόσβασης αποτελούν τις περιοχές εκείνες μιας εγκατάστασης που προσδιορίζονται από τον διαχειριστή της ως ουσιαστικές για την ασφάλεια των λειτουργιών και του ελέγχου, των εργασιών χειρισμού φορτίων, όπως για παράδειγμα τα κέντρα επικοινωνιών, τα αντλιοστάσια, τις δεξαμενές και το δίκτυο σωληνώσεων που τις εξυπηρετεί, οι χώροι αποθήκευσης επικίνδυνων φορτίων, τους χώρους παρακολούθησης κλειστών συστημάτων, κ.α. Το επίπεδο ασφάλειας 1 είναι το επίπεδο για το οποίο τηρούνται πάντα και συστηματικά τα ελάχιστα μέτρα προστασίας και ετοιμότητας. Το επίπεδο 2 χαρακτηρίζει πρόσθετα, κατάλληλα μέτρα ασφάλειας τα οποία διατηρούνται για μια χρονική περίοδο ως αποτέλεσμα ενός αυξημένου κινδύνου. Το 3 σημαίνει πρακτικά το επίπεδο εκείνο για το οποίο τα περαιτέρω μέτρα θα διατηρηθούν για μια περιορισμένη χρονικά περίοδο όταν ένα γεγονός ασφάλειας των μεταφορών είναι πιθανό και επικείμενο.

Το σχέδιο προβλέπει όχι μόνο τον τρόπο αντιμετώπισης ενός περιστατικού που δύναται να θέσει σε κίνδυνο την εγκατάσταση και το πλοίο που είναι ελλιμενισμένο σε αυτή, αλλά συγχρόνως οργανώνει το μηχανισμό πρόληψης προσδιορίζοντας τους αναγκαίους πόρους, το ανθρώπινο δυναμικό και τα μέσα για τον έλεγχο και την επιτήρηση των ζωνών περιορισμένης πρόσβασης και γενικά όλα τα κρίσιμα σημεία της εγκατάστασης, Πρέπει επίσης να περιλαμβάνει τουλάχιστον:

- Μέτρα ή/και εξοπλισμό αποφυγής μη εξουσιοδοτημένης μεταφοράς επικίνδυνων ουσιών, όπλων και συσκευών που προορίζονται για χρήση ενάντια σε ανθρώπους, πλοία και εγκαταστάσεις,

- Διαδικασίες ανταπόκρισης στις απειλές ασφάλειας, εκκένωσης σε περίπτωση απειλών ή παραβιάσεων της ασφάλειας

- Διαδικασίες αναφοράς έκνομων γεγονότων κατά της ασφάλειας των μεταφορών

- Διαδικασίες εκτέλεσης ενεργειών σε περίπτωση που ενεργοποιείται το σύστημα αναγγελίας ασφάλειας ενός πλοίου που βρίσκεται εντός της λιμενικής εγκατάστασης

- Διορισμό του Υπεύθυνου Ασφαλείας Λιμενικής Εγκατάστασης.

Για να επιτευχθούν τα παραπάνω ορίζεται ένας Υπεύθυνος Ασφαλείας που μπορεί να έχει παράλληλα καθήκοντα και για άλλους ρόλους και εργασίες υπό τον όρο ότι είναι πλήρως ικανός να φέρει σε πέρας το έργο που του έχει ανατεθεί στο πλαίσιο της υλοποίησης του Σχεδίου (προπαρασκευή για τη διενέργεια της αρχικής ή άλλης περιοδικής Αξιολόγησης Ασφάλειας, εξασφάλιση επαρκούς εκπαίδευσης του προσωπικού που έχει ρόλο στην ασφάλεια της εγκατάστασης, υποβολή έκθεσης προς τις υπεύθυνες αρχές και τήρηση στοιχείων που σκιαγραφούν περιστατικά που έθεσαν σε κίνδυνο την εγκατάσταση, κ.α.)

Ο φορέας διαχείρισης ενός τερματικού σταθμού που βρίσκεται εντός ενός εκτενούς λιμενικού συγκροτήματος δεν απαλλάσσεται της ευθύνης εφαρμογής των διατάξεων του Κώδικα ISPS, αφού ουσιαστικά υποδέχεται και εξυπηρετεί πλοία για τις δικές του ανάγκες (π.χ. εισαγωγή πρώτων υλών, εξαγωγές έτοιμων προϊόντων προς/από το γειτνιάζον εργοστασιακό συγκρότημα, τερματικούς σταθμούς χύδην φορτίων, κ.α.)

Η ικανότητα προσαρμογής ενός φορέα διαχείρισης λιμένα στον οποίο καταπλέουν πλοία SOLAS στο νέο πλαίσιο λειτουργίας που διαμορφώνεται από τις διεθνείς εξελίξεις για την ασφάλεια, εξαρτάται από πολλούς παράγοντες. Υπάρχει εύκολη προσαρμογή και ωριμότητα για τα λιμάνια στα οποία γίνεται χειρισμός και αποθήκευση επικίνδυνων φορτίων ή γενικά σε αυτά στα οποία έχουν εκπονηθεί και υλοποιούνται σχέδια αντιμετώπισης τεχνολογικών ατυχημάτων (υπόχρεες εγκαταστάσεις των Οδηγιών Seveso I/II) καθώς και σχέδια αντιμετώπισης περιστατικών ρύπανσης από πετρέλαιο και άλλες υγρές χημικές, επιβλαβείς ουσίες.[2]

3.2 Το διεθνές πρότυπο ISO 27001:2005

3.2.1 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

Το ISO/IEC 27001 είναι το μόνο διεθνές πρότυπο που μπορεί να επιθεωρηθεί και το οποίο καθορίζει τις απαιτήσεις για ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ-ISMS).

Η πληροφορία είναι αποφασιστικής σημασίας για τη λειτουργία και πιθανόν και για την επιβίωση ενός οργανισμού. Η πιστοποίηση κατά ISO/IEC 27001 βοηθά έναν οργανισμό να διαχειριστεί και να προστατεύσει τα πολύτιμα περιουσιακά του στοιχεία που περιέχουν πληροφορίες. Το πρότυπο είναι σχεδιασμένο έτσι ώστε να διασφαλίζει την επιλογή επαρκών και ισορροπημένων ελέγχων ασφάλειας. Αυτή η επιλογή βοηθά ένα οργανισμό να προστατεύσει τα περιουσιακά του στοιχεία πληροφοριών και να τον εμπιστεύονται τα ενδιαφερόμενα μέρη και ιδιαίτερα οι πελάτες του. Το πρότυπο είναι βασισμένο στη διεργασιακή προσέγγιση για την εδραίωση, εφαρμογή, λειτουργία, παρακολούθηση, ανασκόπηση, συντήρηση και βελτίωση ενός ΣΔΑΠ.

Το ISO/IEC 27001 είναι κατάλληλο για όλους τους οργανισμούς, μικρούς ή μεγάλους και σε κάθε εργασιακό χώρο. Είναι ιδιαίτερα κατάλληλο για οργανισμούς που η προστασία της πληροφορίας είναι κρίσιμη, όπως σε χρηματοπιστωτικούς οργανισμούς, τηλεπικοινωνίες, υγεία, δημόσιο και πληροφορική.

Το ISO/IEC 27001 είναι επίσης κατάλληλο για εταιρείες που διαχειρίζονται πληροφορίες για λογαριασμό άλλων, όπως εταιρείες παροχής υπηρεσιών πληροφορικής και μπορεί να λειτουργήσει σαν εγγύηση ότι οι πληροφορίες των πελατών τους προστατεύονται.

3.2.2 Οφέλη του ISO/IEC 27001

Η πιστοποίηση ενός ΣΔΑΠ σύμφωνα με τις απαιτήσεις του ISO/IEC 27001 μπορεί να προσφέρει τα παρακάτω οφέλη σε ένα οργανισμό:

— Αποδεικνύει ότι οι εσωτερικοί έλεγχοι του οργανισμού πραγματοποιούν και ικανοποιούν τους εταιρικούς στόχους και στρατηγικές.

— Αποδεικνύει ότι οι απαιτήσεις για σωστή διακυβέρνηση και επιχειρησιακή συνέχεια ικανοποιούνται.

— Αποδεικνύει ότι η σχετική νομοθεσία και οι τυποποιημένοι κανονισμοί εφαρμόζονται.

— Παρέχει ανταγωνιστικό πλεονέκτημα στην ικανοποίηση συμβατικών υποχρεώσεων και επιδεικνύει στους πελάτες του οργανισμού ότι η ασφάλεια των πληροφοριών τους είναι πρωταρχικής σημασίας για τον οργανισμό.

— Αποδεικνύει μέσω ενός ανεξάρτητου φορέα ότι τα οργανωτικά ρίσκα έχουν αναγνωριστεί, αξιολογηθεί και διαχειριστεί ικανοποιητικά και σωστά.

— Αναδεικνύει την ύπαρξη ενός επίσημου και λειτουργικού συστήματος διαχείρισης ασφάλειας πληροφοριών.

— Αποδεικνύει τη δέσμευση της ανώτατης διοίκησης του οργανισμού στην ασφάλεια των πληροφοριών του

— Αποδεικνύει ότι μέσω τακτικών αξιολογήσεων βοηθά τον οργανισμό να παρακολουθεί την απόδοσή του και να βελτιώνεται

— Αναδεικνύει ότι όλες οι πληροφορίες που αποθηκεύονται, επεξεργάζονται ή επικοινωνούν μέσω των πληροφοριακών συστημάτων έχουν αξία για τον οργανισμό

Το ISO/IEC 27001 χρησιμοποιεί την αξιολόγηση των ρίσκων ώστε να δημιουργηθεί ένα σύστημα διαχείρισης που παρέχει:

- Μεγιστοποίηση της διαθεσιμότητας των συστημάτων
- Διαβεβαίωση ότι η ακεραιότητα των συστημάτων, των συστημάτωνεπεξεργασίας και της πληροφορίας συντηρείται
- Επιβεβαίωση ότι η εμπιστευτικότητα της πληροφορίας διατηρείται. [4]

3.2.3 Ποιες είναι οι διαφορές μεταξύ ISO 27001 και ISO 27002;

Το πρότυπο ISO 27001 είναι μια πιστοποίηση και σε αυτό περιγράφονται οι απαιτήσεις που πρέπει να πληροί ένας οργανισμός προκειμένου να διαχειριστεί συνολικά και αποτελεσματικά την ασφάλεια της πληροφορίας του. Το πρότυπο ISO 27002 παρέχει τις κατευθυντήριες οδηγίες για την κάλυψη του προτύπου. [5]

3.3 Το διεθνές πρότυπο ISO 27001:2013

Το ISO/IEC 27001:2013 [33] παρέχει και καθορίζει τις απαιτήσεις για την εγκατάσταση, υλοποίηση, διατήρηση και βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών και την αξιολόγηση και επεξεργασία κινδύνων της ασφάλειας πληροφοριών ενός οργανισμού. Οι απαιτήσεις που καθορίζει το διεθνές αυτό πρότυπο μπορούν να εφαρμοστούν σε κάθε οργανισμό. Το πρότυπο μπορεί να χρησιμοποιηθεί από φορείς, εντός ή εκτός του οργανισμού, για την αξιολόγηση της ικανότητας του να καλύψει της απαιτήσεις ασφάλειας του. Το πρότυπο διατηρεί συμβατότητα με τα υπόλοιπα τις ίδιας ομάδας (π. χ. ISO/IEC 27001:2005, ISO/IEC 27002:2005) και περιέχει μία ολοκληρωμένη λίστα αντιμέτρων, συμβατή με αυτήν του ISO/IEC 27001:2005, στην οποία προσθέτει ορισμένους νέους ελέγχους.

3.4 Λοιπή Νομοθεσία και Εγκύκλιοι σχετικά με την Ασφάλεια στην Θάλασσα

Όλες οι δραστηριότητες και οι λειτουργίες σε ένα λιμάνι θα πρέπει να διεξάγονται σύμφωνα με τους ισχύοντες διεθνείς, ευρωπαϊκούς και εθνικούς κανονισμούς και τα αντίστοιχα πρότυπα. Παρακάτω παρουσιάζονται μια σειρά από τους βασικούς αυτούς κανονισμούς και πρότυπα.

3.4.1 Παγκόσμια Πρότυπα Ασφάλειας

Στον τομέα της Ναυτιλίας οι ζημιές συνεχίζουν τη μακρόχρονη πτωτική τους τάση, όμως οι οικονομικές πιέσεις, οι κυβερνοεπιθέσεις και τα ακραία καιρικά φαινόμενα όπως οι πολύ δυνατές καταιγίδες αποτελούν πρόκληση για την πρόοδο στον τομέα της ασφάλειας. Στο Λονδίνο, στη Νέα Υόρκη και στο Μόναχο για το έτος 2016 για παράδειγμα οι ζημιές στον τομέα της ναυτιλίας συνέχισαν τη μακρόχρονη πτωτική τάση τους με 85 καταγεγραμμένες ολικές απώλειες σε όλο τον κόσμο το 2015, σύμφωνα με την τέταρτη ετήσια έκθεση της Allianz Global Corporate & Specialty SE (AGCS) "Ασφάλεια και Ναυτιλία 2016", η οποία αναλύει καταγεγραμμένες ζημιές σε πλοία άνω της χωρητικότητας των 100 τόνων.

- **Διεθνής Σύμβαση για την Ασφάλεια της ζωής στη θάλασσα (international Convention for the Safety of Life at Sea (SOLAS), 1974**)

Η σύμβαση SOLAS είναι η πιο σημαντική από όλες τις σχετικές διεθνείς συνθήκες και καθορίζει την νομική βάση και τις ελάχιστες προδιαγραφές ασφάλειας για την κατασκευή, τον εξοπλισμό και την λειτουργία των εμπορικών και των επιβατηγών πλοίων. Η πρώτη έκδοση υιοθετήθηκε το 1914, ως συνέπεια του καταστροφικού ναυαγίου του Τιτανικού. Έκτοτε αναπτύχθηκαν αρκετές εκδόσεις του με πιο γνωστή αυτή του 1974 η οποία τέθηκε σε εφαρμογή το 1980. Η σύμβαση του 1974 έχει ανανεωθεί και τροποποιηθεί επανειλημμένως [28]. Η σύμβαση αυτή είναι ένας από τους σημαντικότερους και παλαιότερους κανονισμούς που θεσπίζει κανόνες ασφαλείας για τις θαλάσσιες δραστηριότητες και αυτός είναι ο λόγος που αναφέρεται σε αυτό το κεφάλαιο παρά το γεγονός ότι τα κεφάλαια της που είναι αφιερωμένα στην μεταφορά των φορτίων, επικίνδυνων εμπορευμάτων και τη διαχείριση ασφαλών λειτουργιών, σχετίζονται με τα πλοία και όχι με τις λιμενικές εγκαταστάσεις ή την διεπαφή πλοίου / λιμένα. Στην SOLAS οι λιμενικές εγκαταστάσεις θεωρούνται χώροι εργασίας, βιομηχανικές περιοχές, περιοχές αποθήκευσης, παραγωγής και διακίνησης και εμπίπτουν στο πεδίο εφαρμογής των γενικών κανόνων και της νομοθεσίας που εκδίδεται από τις χώρες και τους διεθνείς οργανισμούς.

- Κώδικας Πρακτικής για την Ασφάλεια και την Υγεία στους Λιμένες (Διεθνής Οργανισμός Εργασίας International Labour Organization (ILO) Code of Practice on Safety and Health in Ports)

Εκδόθηκε το 2005 και καλύπτει όλες τις πτυχές της εργασίας στους λιμένες που αφορούν την φορτοεκφόρτωση αγαθών και επιβατών, την κυκλοφορία των οχημάτων κάθε τύπου, τις δραστηριότητες στην ακτή και εντός των πλοίων, τον φωτισμό, τον ατομικό εξοπλισμό προστασίας, ειδικές προβλέψεις για άτομα με αναπηρία και λεπτομέρειες για τον χειρισμό ορισμένων φορτίων.

- General Conference of the International ILO Convention and Recommendation concerning Occupational Safety and Health in Dock Work, C-152, (1979)

Η συνθήκη τέθηκε σε ισχύ το 1979 και προβλέπει μέτρα σχετικά με τον εξοπλισμό και τη συντήρηση των υποδομών, με στόχο την αύξηση της ασφάλειας και τη μείωση των τραυματισμών. Περιλαμβάνει μέτρα για την ασφαλή πρόσβαση στις εργασίας και παρέχει, πληροφορίες σχετικές με την ασφάλεια των

εργαζομένων όπως η κατάλληλη ένδυση ασφαλείας, ο εξοπλισμός διάσωσης, η προσφορά πρώτων βοηθειών και η αντιμετώπιση περιστατικών ασφαλείας.

- Διεθνής Ναυτιλιακός Κώδικας Στερεών Φορτίων Χύδην (International Maritime Solid Bulk Cargoes Code - IMSBC Code)

Ο κώδικας IMSBC υιοθετήθηκε από την Επιτροπή Ναυτικής Ασφάλειας του IMO το 2008 και αντικαθιστά τον «Κώδικα Ασφαλούς Πρακτικής για Στερεά Φορτία Χύδην (Code of Safe Practice for Solid Bulk Cargoes (BC Code))». Σκοπός του κώδικα είναι να διευκολύνει την ασφαλή στοιβασιά και μεταφορά των στερεών χύδην φορτίων παρέχοντας πληροφορίες για τους κινδύνους που σχετίζονται με την μεταφορά τους καθώς και οδηγίες σχετικές με τις ενδεδειγμένες διαδικασίες που πρέπει να υιοθετηθούν. Στην Ελλάδα ο κώδικας υιοθετήθηκε με το Προεδρικό Διάταγμα υπ' αριθμόν 52 τον Απρίλιο του 2013 (ΠΔ52_2013).

- Διεθνής Κώδικας για την Κατασκευή και τον Εξοπλισμό των Πλοίων που Μεταφέρουν Επικίνδυνα Χημικά Χύδην (International Code for the Construction and Equipment of Ships carrying Dangerous Chemicals in Bulk (IBC Code))

Ο κώδικας IBC, θέτει το διεθνές πρότυπο για την ασφαλή μεταφορά διά θαλάσσης επικίνδυνων και επιβλαβών χύδην υγρών χημικών ουσιών. Ο κώδικας ορίζει το σχεδιασμό και τα πρότυπα κατασκευής των πλοίων και τον αντίστοιχο εξοπλισμό που πρέπει αυτά να φέρουν, λαμβάνοντας δεόντως υπόψη τη φύση των σχετικών προϊόντων που μεταφέρονται [25]. Από το 1985 ο κώδικας έχει επεκταθεί για να καλύπτει θέματα θαλάσσιας ρύπανσης. Στην Ελλάδα ο κώδικας υιοθετήθηκε με το προεδρικό διάταγμα ΠΔ41_1994 (ΦΕΚ 31/Α/10.3.1994).

- Διεθνής Σύμβαση για την Αποφυγή της Ρύπανσης από Πλοία (International Convention for the Prevention of Pollution from Ships (MARPOL))

Η σύμβαση MARPOL υιοθετήθηκε στις 2 Νοεμβρίου 1973 στον IMO, τέθηκε σε εφαρμογή τον Οκτώβριο του 1983 και είναι η κύρια διεθνής σύμβαση που καλύπτει την πρόληψη της ρύπανσης του θαλάσσιου περιβάλλοντος από τα πλοία. Η σύμβαση, η οποία έχει αναβαθμισθεί με διάφορες τροποποιήσεις μέσα στα χρόνια, περιλαμβάνει έξι τεχνικά παραρτήματα τα οποία στοχεύουν στην πρόληψη και την ελαχιστοποίηση της ρύπανσης, ακούσιας ή από συνήθεις λειτουργίες, που μπορεί να προκαλέσει ένα πλοίο [27].

- Διεθνής Σύμβαση για τα Πρότυπα Εκπαίδευσης, Έκδοσης Πιστοποιητικών και Τήρησης Φυλακών των Ναυτικών (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW))

Η Σύμβαση STCW που υιοθετήθηκε το 1978 και τέθηκε σε εφαρμογή το 1984, είναι η πρώτη που θέτει τις βασικές προϋποθέσεις για την εκπαίδευση, την πιστοποίηση και την τήρηση Φυλακών των ναυτικών

σε διεθνές επίπεδο. Η σύμβαση ορίζει τις ελάχιστες προδιαγραφές σχετικά με αυτά τα θέματα τις οποίες οι χώρες είναι υποχρεωμένες να πληρούν [19].

- Διεθνής Σύμβαση για τη Ναυτική Έρευνα και Διάσωση (International Convention on Maritime Search and Rescue (SAR))

Στόχος της σύμβασης του 1979, που εγκρίθηκε κατά την διάσκεψη του Αμβούργου ήταν η διεθνής ανάπτυξη ενός σχεδίου έρευνας και διάσωσης, έτσι ώστε, ανεξάρτητα από το πού συμβαίνει ένα ατύχημα, η διάσωση των ανθρώπων που βρίσκονται στην θάλασσα να συντονίζεται από έναν οργανισμό έρευνας και διάσωσης (SAR organisation) ή/και, όταν κρίνεται αναγκαίο, από συνεργαζόμενους τέτοιους οργανισμούς. Μέχρι την έκδοση της σύμβασης SAR, δεν υπήρχε διεθνές σύστημα που να καλύπτει επιχειρήσεις έρευνας και διάσωσης [20].

- Μνημόνιο Συνεννόησης των Παρισίων (Paris Memorandum of Understanding of port state control (Paris MoU))

Το Paris MoU αποτελεί ένα πρωτόκολλο σύμβασης μεταξύ είκοσι επτά διαφορετικών Λιμενικών Αρχών. Υπογράφηκε από 14 Ευρωπαϊκές χώρες τον Ιανουάριο του 1982 στο Παρίσι και τέθηκε σε εφαρμογή τον Ιούλιο του ίδιου έτους. Το μνημόνιο καλύπτει την ασφάλεια της ζωής στη θάλασσα, την πρόληψη της ρύπανσης από τα πλοία και τις συνθήκες διαβίωσης και εργασίας επί των πλοίων. Το Paris MoU έχει τροποποιηθεί αρκετές φορές ώστε να ανταποκριθεί στις εκάστοτε απαιτήσεις ασφαλείας που θέτει ο IMO [21].

Ευρώπη

- Κανονισμός (ΕΚ) αριθ.725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαρτίου 2004 για την ενίσχυση της ασφάλειας στα πλοία και στις λιμενικές εγκαταστάσεις (Regulation 725/2004/EC).

Ο κύριος στόχος του κανονισμού αυτού είναι η θέσπιση και εφαρμογή μέτρων που αποσκοπούν στη βελτίωση της ασφάλειας στα πλοία που εκτελούν διεθνή δρομολόγια και στην διεθνή θαλάσσια κυκλοφορία, συμπεριλαμβανομένων των σχετικών λιμενικών εγκαταστάσεων [22]. Ωστόσο, ο κανονισμός περιλαμβάνει διατάξεις που επεκτείνουν τα μέτρα αυτά και σε πλοία που εκτελούν εθνικά δρομολόγια εντός της ΕΕ, καθώς και τις συναφείς λιμενικές εγκαταστάσεις που εξυπηρετούν τα πλοία αυτά. Ο κανονισμός παρέχει τη βάση για την εναρμονισμένη ερμηνεία και εφαρμογή, των ειδικών μέτρων για την ενίσχυση της ασφάλειας στη θάλασσα, που εγκρίθηκαν από τον IMO το 2002 ως τροποποίηση της σύμβασης SOLAS και την εφαρμογή του κώδικα ISPS. Ο κανονισμός καθιστά υποχρεωτική μια σειρά συστάσεων του μέρους Β του κώδικα ISPS [23].

- Οδηγία 2005/65/ΕΚ σχετικά με την ενίσχυση της ασφάλειας των λιμένων (Directive 2005/65/EC)

Η οδηγία συμπληρώνει τα μέτρα ασφάλειας που θεσπίστηκαν από τον παραπάνω κανονισμό (ΕΚ/725/2004) θέτοντας έναν ολόκληρο λιμένα σε ένα καθεστώς ασφαλείας. Προκειμένου να επιτευχθεί η μέγιστη δυνατή προστασία για θαλάσσιες και λιμενικές δραστηριότητες, πρέπει να ληφθούν μέτρα που να καλύπτουν όλους τους λιμένες σε περίμετρο που ορίζεται από το εν λόγω κράτος μέλος. Τα μέτρα αυτά πρέπει να εφαρμόζονται σε όλους τους λιμένες και τις λιμενικές εγκαταστάσεις που εμπίπτουν στο πλαίσιο του κανονισμού. Η οδηγία προβλέπει επίσης μηχανισμούς για την εφαρμογή αυτών των μέτρων και τον έλεγχο της συμμόρφωσης προς αυτούς.

- Οδηγία 2010/65/ΕΕ (Directive 2010/65/EU)

Η συγκεκριμένη οδηγία αφορά στην απλούστευση και την εναρμόνιση των διοικητικών διαδικασιών που εφαρμόζονται στις θαλάσσιες μεταφορές, μέσω της τυποποίησης της ηλεκτρονικής διαβίβασης πληροφοριών και την εξυγίανση των διατυπώσεων υποβολής δηλώσεων. Ορίζει συγκεκριμένα ότι οι πληροφορίες για το φορτίο, το πλήρωμα ή/και τους επιβάτες που μεταδίδονται κατά την άφιξη πλοίων σε ευρωπαϊκά λιμάνια πρέπει να κοινοποιούνται σε ηλεκτρονική μορφή (emessages) [24] μέσω μιας Ενιαίας θύρας (single window). Ο κανονισμός πρέπει να έχει εκτελεστεί από τα κράτη μέλη μέχρι την 1η Ιουνίου 2015. Αυτή η Ενιαία Θύρα είναι ο μόνος τρόπος όπου όλες οι πληροφορίες θα δηλώνονται και απ' όπου θα διατίθενται στις διάφορες αρμόδιες αρχές και στα άλλα κράτη μέλη.

- Οδηγία 96/98/ΕΚ σχετικά με τον εξοπλισμό των πλοίων (Directive 96/98/EC)

Με αυτήν την ντιρεκτίβα η Ευρωπαϊκή Ένωση (ΕΕ) θεσπίζει πρότυπα για τη διασφάλιση της ασφάλειας και της ποιότητας του θαλάσσιου εξοπλισμού των πλοίων. Τα πρότυπα αυτά συμβάλλουν επίσης στην αντιμετώπιση της θαλάσσιας ρύπανσης και στη διασφάλιση της ελεύθερης κυκλοφορίας του θαλάσσιου εξοπλισμού εντός της εσωτερικής αγοράς.

- Κανονισμός (ΕΚ) αριθ. 324/2008 σχετικά με τις διαδικασίες για τη διενέργεια των επιθεωρήσεων της Επιτροπής στο πεδίο της ασφάλειας της ναυσιπλοΐας (Regulation 324/2008/EC)

Προκειμένου να παρακολουθεί την εφαρμογή της Ευρωπαϊκής νομοθεσίας στον τομέα της ασφάλειας στην θάλασσα, η επιτροπή διενεργεί επιθεωρήσεις. Ο κανονισμός αυτός θεσπίζει τις διαδικασίες, για την επιτήρηση, από μέρους της Επιτροπής, της εφαρμογής της ντιρεκτίβας 2005/65/ΕΚ καθώς και για τις επιθεωρήσεις που προβλέπονται για τα πλοία και τις λιμενικές εγκαταστάσεις [25].

3.4.2 Ελληνική Εθνική Νομοθεσία

Παρακάτω αναφέρονται οι σημαντικότεροι νόμοι που ισχύουν στην Ελλάδα, οι οποίοι διευθετούν θέματα ασφαλείας στην θάλασσα και εξασφαλίζουν την ευθυγράμμιση της χώρας με τις διεθνείς και ευρωπαϊκές απαιτήσεις σε αυτόν τον τομέα.

- Νόμος 1045/1980 – (ΦΕΚ 95)

Ο νόμος αυτός αποτελεί την πρώτη πράξη κύρωσης της Διεθνούς Σύμβασης Περί Ασφαλείας της Ανθρώπινης Ζωής στη Θάλασσα (ΠΑΑΖΕΘ (SOLAS, 1974)) και εκδόθηκε στις 25 Απριλίου 1980. Έκτοτε έχουν εκδοθεί πολυάριθμοι νόμοι και Προεδρικά Διατάγματα που επικυρώνουν τις διάφορες τροποποιήσεις της ΠΑΑΖΕΘ με τελευταίο το ΠΔ98/2009 – (ΦΕΚ 124) [26].

- Νόμος 3622/2007 – ΦΕΚ 281/Α΄/20.12.2007

Στόχος του νόμου αυτού αποτελεί ο καθορισμός των αρμοδιοτήτων, ο σχεδιασμός δράσεων σε εθνικό επίπεδο, καθώς και ο συντονισμός αυτών για τη διασφάλιση της εφαρμογής του Κανονισμού ΕΚ/725/2004 (L129/6 της 29.4.2004) και της Ευρωπαϊκής Οδηγίας 2005/65 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (L130 της 25.11.2005) για την ενίσχυση της ασφάλειας των πλοίων, των λιμενικών εγκαταστάσεων και των λιμένων [18].

- ΠΔ241/2006

Το συγκεκριμένο Προεδρικό Διάταγμα προχωρά στην αποδοχή των τροποποιήσεων της Διεθνούς Σύμβασης «Για πρότυπα εκπαίδευσης, έκδοσης πιστοποιητικών και τήρησης φυλακών των ναυτικών, 1978», η οποία κυρώθηκε με τον ν.1314/1983 (Α’2), όπως αυτή τροποποιήθηκε.

- ΠΔ56/2004

Το Προεδρικό Διάταγμα υπ’αριθ.56 εκδόθηκε την 11η Φεβρουαρίου 2004 και προχωρά στην κύρωση των τροποποιήσεων της «ΠΑΑΖΕΘ, 1974» που υιοθετήθηκαν στην Διάσκεψη των Συμβαλλομένων Κυβερνήσεων της Διεθνούς Σύμβασης την 12η Δεκεμβρίου 2002 [26], εφαρμόζοντας πρακτικά τον ISPS κώδικα για τα ελληνικά πλοία και τις ελληνικές λιμενικές εγκαταστάσεις.

- ΠΔ125/2012

Το διάταγμα αυτό είναι η προσαρμογή της ελληνικής νομοθεσίας στις διατάξεις της Οδηγίας 2010/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις διατυπώσεις υποβολής δηλώσεων για τα πλοία κατά τον κατάπλου ή/και απόπλου από τους λιμένες των κρατών μελών.

- ΠΔ347/1998

Το διάταγμα αυτό είναι η προσαρμογή της ελληνικής νομοθεσίας για την αποδοχή των διατάξεων της οδηγίας 96/98/ΕΚ της Κομισιόν και στοχεύει στη βελτίωση της ασφάλειας στην θάλασσα και την πρόληψη της θαλάσσιας ρύπανσης εφαρμόζοντας διεθνή κανονισμούς που αφορούν τον εξοπλισμό των πλοίων.

2.5 Αυτόματο σύστημα εντοπισμού - (Automatic Identification System - AIS)

Το σύστημα AIS σχεδιάστηκε αρχικά για να βοηθήσει την αποφυγή συγκρούσεων πλοίων, καθώς και να υποστηρίξει τις λιμενικές αρχές στην επίτευξη του καλύτερου έλεγχου της θαλάσσιας κυκλοφορίας. Οι πομποί AIS που είναι εγκατεστημένοι στα πλοία περιλαμβάνουν έναν δέκτη εντοπισμού θέσης GPS (Global Positioning System) που υπολογίζει τις συντεταγμένες της θέσης του πλοίου, την ταχύτητά του και την πορεία του. Περιλαμβάνει επίσης έναν πομπό VHF, ο οποίος μεταδίδει περιοδικά τις πληροφορίες αυτές σε δυο κανάλια VHF (συχνότητες 161,975 MHz και 162,025 MHz – παλιά VHF κανάλια 87 & 88). Άλλα πλοία ή σταθμοί βάσης μπορούν να λάβουν τις πληροφορίες αυτές χρησιμοποιώντας έναν δέκτη AIS. Στη συνέχεια, με χρήση ειδικού λογισμικού που επεξεργάζεται τα δεδομένα, τα πλοία εμφανίζονται στις οθόνες των συστημάτων πλοήγησης ή σε υπολογιστή.

Τυπικά, τα σκάφη με δέκτη AIS με μια εξωτερική κεραία που τοποθετείται 15 μέτρα πάνω από το επίπεδο της θάλασσας, λαμβάνουν τις πληροφορίες AIS εντός μιας ακτίνας 15-20 ναυτικών μιλίων. Οι σταθμοί βάσης που εγκαθίστανται σε μεγαλύτερο υψόμετρο, μπορούν να επεκτείνουν την εμβέλεια μέχρι τα 40-60 ναυτικά μίλια., ακόμη και πίσω από απομακρυσμένα βουνά. Η εμβέλεια εξαρτάται από το ύψος της κεραίας, τα εμπόδια γύρω από την κεραία και τις καιρικές συνθήκες. Ο σημαντικότερος παράγοντας είναι βέβαια το υψόμετρο. Είναι δυνατόν να παρατηρηθούν πλοία σε απόσταση έως 150 ναυτικά μίλια μακριά με μια μικρή φορητή κεραία τοποθετημένη σε βουνό νησιού με υψόμετρο έως 700 μέτρων. Οι σταθμοί βάσης μας καλύπτουν πλήρως μια ακτίνα 40 μιλίων και περιοδικά λαμβάνουν πληροφορίες από πλοία που βρίσκονται μέχρι και 100 μίλια μακριά.

Κάθε σταθμός βάσης είναι εξοπλισμένος με έναν δέκτη AIS, έναν ηλεκτρονικό υπολογιστή και μια σύνδεση στο Διαδίκτυο. Ο δέκτης AIS λαμβάνει δεδομένα, τα οποία υποβάλλονται σε επεξεργασία από ένα απλό λογισμικό στον υπολογιστή και στη συνέχεια αποστέλλονται σε μια κεντρική βάση δεδομένων μέσω μιας Υπηρεσίας Ιστού. Αυτό το λογισμικό είναι ελεύθερο για όσους ενδιαφέρονται, με άδεια χρήσης GNU.Τα δεδομένα που λαμβάνονται από τον δέκτη AIS είναι κωδικοποιημένα σε μηνύματα NMEA (6-bit απλό κείμενο).

παράδειγμα:!AIVDM,1,1,,B,1INS<8@P001cnWFEdSmh00bT0000,0*38

Τα μηνύματα AIS περιλαμβάνουν τους παρακάτω βασικούς τύπους πληροφορίας:

1. Δυναμική πληροφορία, όπως η θέση του πλοίου, η ταχύτητα, η πορεία, και η ταχύτητα στροφής.

2. Στατική πληροφορία, όπως το όνομα του πλοίου, ο αριθμός IMO, ο αριθμός MMSI (Maritme Mobile Service Identity) και οι διαστάσεις του.

3. Πληροφορίες που σχετίζονται με το συγκεκριμένο ταξίδι που εκτελεί, όπως προορισμός, εκτιμώμενη άφιξη και βύθισμα.

Η κεντρική βάση δεδομένων λαμβάνει και επεξεργάζεται ένα σημαντικό όγκο δεδομένων. Από αυτά αποθηκεύει τα πιο σημαντικά, τα οποία είναι απαραίτητα να δώσουν μια καλή εικόνα των θέσεων των

πλοίων. Περιλαμβάνει επίσης γεωγραφικές πληροφορίες για τα λιμάνια και για άλλες περιοχές, φωτογραφίες πλοίων και άλλες χρήσιμες πληροφορίες. [3]

3.5 Η μέθοδος CRAMM

Η μέθοδος Ανάλυσης και Διαχείρισης Επικινδυνότητας πληροφοριακών συστημάτων που θα περιγράφει στην παρούσα διπλωματική διατριβή είναι η CRAMM (**CCTA Risk Analysis and Management Methodology**). Η CRAMM αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (**Central Computer and Telecommunications Agency – CCTA**) του Ηνωμένου Βασιλείου το 1987 και αποτελεί πρότυπο για τους οργανισμούς του ευρύτερου δημόσιου τομέα στο Ηνωμένο Βασίλειο. Η CRAMM έχει κερδίσει διεθνή αναγνώριση για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε χιλιάδες περιπτώσεων, συνεπώς είναι ώριμη μεθοδολογία ευρισκόμενη ήδη στην πέμπτη εκδοχή της (version 5,1).
- Συνοδεύεται από ένα αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια της εφαρμογής της, καθώς και την επιλογή αντιμέτρων.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας και της ασφάλειας δικτύων.

Το λογισμικό υποστήριξης της CRAMM υποστηρίζει το σύνολο της μεθόδου και αποτελεί αναπόσπαστο τμήμα της. Μέσω του εργαλείου αυτού παρακολουθείται η ορθή, βήμα-προς-βήμα, εφαρμογή της μεθοδολογίας Ανάλυσης και Διαχείρισης Επικινδυνότητας, ενώ αποθηκεύονται και ενημερώνονται όλα τα στοιχεία που συλλέγονται κατά την εφαρμογή της μεθοδολογίας. Επίσης, το εργαλείο CRAMM υποστηρίζει όλους τους σύνθετους υπολογισμούς που απαιτούνται για τον προσδιορισμό της επικινδυνότητας, ενσωματώνει τη βάση των αντιμέτρων και τους μηχανισμούς συμπερασματολογίας που προτείνουν τα αντίμετρα.

Το εργαλείο της CRAMM υλοποιεί ένα υποσύνολο των βημάτων της μεθόδου CRAMM και δε μπορεί να θεωρηθεί ότι δύναται να αντικαταστήσει την εμπειρία ή τη γνώση των μελετητών. Αυτό που πετυχαίνει είναι να υποβοηθήσει την διεξαγωγή της μελέτης. Τα αποτελέσματα που παράγει θα πρέπει να ελέγχονται, αναλύονται και τροποποιούνται κατάλληλα από τους αναλυτές ώστε να ταιριάξουν στις ιδιαιτερότητες του Π.Σ. που μελετάται.

3.6 Αναλυτική Περιγραφή της CRAMM

Η CRAMM αποτελείται από τρία βασικά στάδια (πινακας 1):

- Προσδιορισμός-αξιολόγηση των αγαθών (**identification and valuation of assets**).
- Ανάλυση επικινδυνότητας (**risk analysis**).
- Διαχείριση επικινδυνότητας (**risk management**).

Στάδιο	**Βήματα σταδίου**
Προσδιορισμός και αξιολόγηση των αγαθών (**identification and valuation of assets**)	**Βήμα 1.1**: Δημιουργία Μοντέλου Π.Σ. **Βήμα 1.2**: Αποτίμηση αγαθών **Βήμα 1.3**: Επιβεβαίωση και επικύρωση της αποτίμησης
Ανάλυση επικινδυνότητας (**Risk analysis**)	**Βήμα 2.1**: Προσδιορισμός των απειλών που αφορούν κάθε Αγαθό (**asset**) **Βήμα 2.2**: Εκτίμηση απειλών (**threat assessment**) και αδυναμιών (**vulnerability assessment**) **Βήμα 2.3**: Υπολογισμός επικινδυνότητας για κάθε συνδυασμό **Αγαθό-Απειλή-Αδυναμία** **Βήμα 2.4**: Επιβεβαίωση και επικύρωση του βαθμού επικινδυνότητας
Διαχείριση επικινδυνότητας (**Risk management**)	**Βήμα 3.1**: Προσδιορισμός της λίστας των προτεινόμενων αντιμέτρων **Βήμα 3.2**: Σχεδιασμός του Σχεδίου Ασφάλειας

Πίνακας 1: Στάδια της μεθόδου CRAMM

Κάθε στάδιο εκτελείται σε συγκεκριμένα βήματα. Τα στάδια και τα βήματα αυτά περιγράφονται λεπτομερώς στη συνέχεια.

3.6.1 Στάδιο 1: Προσδιορισμός και αξιολόγηση των αγαθών

Το πρώτο στάδιο αναφέρεται στον προσδιορισμό και την αξιολόγηση των στοιχείων των Π.Σ. που χρειάζονται προστασία. Αποτελείται από τα εξής βήματα:

- Δημιουργία ενός συνοπτικού μοντέλου των Π.Σ.
- Αποτίμηση των στοιχείων των Π.Σ.
- Επιβεβαίωση και επικύρωση της αποτίμησης.

Στάδιο1, Βήμα 1: Δημιουργία μοντέλου Πληροφοριακού Συστήματος

Το πρώτο βήμα αναφέρεται στον προσδιορισμό των στοιχείων των Πληροφοριακών Συστημάτων που απαιτούν προστασία. Τα στοιχεία αυτά είναι, μεταξύ άλλων, τα δεδομένα που χειρίζονται, όπως επίσης

το λογισμικό και το υλικό των Πληροφοριακών Συστημάτων. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση.

Η συλλογή των απαραίτητων στοιχείων βασίζεται στην τεκμηρίωση του συστήματος και στον πρώτο κύκλο συνεντεύξεων που αφορά το τεχνικό προσωπικό και τους κύριους χρήστες του Π.Σ. Αυτές οι κατηγορίες προσωπικού μπορούν να προσφέρουν πλήρη εικόνα για τη λειτουργικότητα των Πληροφοριακών Συστημάτων του οργανισμού. Το μοντέλο του συστήματος εισάγεται στο εργαλείο λογισμικού της CRAMM και ελέγχεται η συνέπειά του.

Στάδιο1, Βήμα 2: Αποτίμηση αγαθών

Κατά την αποτίμηση των στοιχείων των πληροφοριακών συστημάτων, δίνεται ιδιαίτερη έμφαση στην αποτίμηση των δεδομένων που διαχειρίζεται προκειμένου να προσδιοριστεί η σπουδαιότητα που έχουν αυτά για την υπηρεσία. Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την Επίπτωση (**impact**) που θα είχε η απώλειά της. Εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις καταστροφής, μη εξουσιοδοτημένης μεταβολής (**modification**), αποκάλυψης (**disclosure**) και μη-διαθεσιμότητας (**unavailability**). Συγκεκριμένα εξετάζονται οι εξής περιπτώσεις:

- **Μη-διαθεσιμότητα** [Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο].
- **Καταστροφή** [Απώλεια των δεδομένων μετά τη λήψη του τελευταίου αντιγράφου ασφαλείας, Απώλεια όλων των δεδομένων μαζί με το τηρούμενο αντίγραφο].
- **Αποκάλυψη** [Αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού, Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού, Αποκάλυψη των δεδομένων σε παρόχους υπηρεσιών].
- **Μη-εξουσιοδοτημένη μεταβολή** [Μικρής έκτασης σφάλματα, Μεγάλης έκτασης σφάλματα].
- **Εκούσια μεταβολή των δεδομένων**.
- **Σφάλματα μετάδοσης δεδομένων** [Παρεμβολή λανθασμένων μηνυμάτων, Άρνηση αποστολής μηνύματος (**repudiation of origin**), Άρνηση παραλαβής μηνύματος (**repudiation of receipt**), Αποτυχία αποστολής μηνύματος, Επανάληψη μηνύματος (**replay**), Λανθασμένη δρομολόγηση (**misrouting**), Παρακολούθηση κίνησης (**traffic monitoring**), Απώλεια ακολουθίας μηνυμάτων (**out of sequence**)].

Για κάθε περίπτωση εκτιμάται το δυσμενέστερο πιθανό σενάριο και υπολογίζονται οι επιπτώσεις από την πραγματοποίησή του. Το μέγεθος της επίπτωσης εκτιμάται αριθμητικά με βάση κλίμακα 1-10. Η CRAMM παρέχει οδηγίες (**guidelines**) για την αποτίμηση των Επιπτώσεων που ανήκουν στις παρακάτω κατηγορίες (βλέπε **Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.**):

- Επιπτώσεις στη σωματική ακεραιότητα και τη ζωή φυσικών προσώπων
- Επιπτώσεις από την αποκάλυψη προσωπικών ή και ευαίσθητων προσωπικών δεδομένων

- Νομικές επιπτώσεις
- Παρεμπόδιση εφαρμογής της δικαιοσύνης και της εξιχνίασης παρανομιών
- Οικονομικές απώλειες
- Διατάραξη της δημόσιας τάξης
- Διεθνείς σχέσεις
- Άμυνα και εθνική ασφάλεια
- Εφαρμογή της πολιτικής του οργανισμού
- Απώλεια της εμπιστοσύνης του κοινού στον οργανισμό.

Ακολούθως, η CRAMM μέσω του αυτοματοποιημένου εργαλείου υπολογίζει την έμμεση αξία (**implied value**) των στοιχείων των πληροφοριακών συστημάτων.

Η αποτίμηση των πληροφοριακών συστημάτων βασίζεται σε συνεντεύξεις που γίνονται με στελέχη που εμπλέκονται στην αξιοποίηση του Π.Σ. Στην περίπτωση της παρούσας μελέτης ασφάλειας διεξήχθησαν συνεντεύξεις με το τεχνικό και διοικητικό προσωπικό της Γ.Γ.Π.Π.

Το λογισμικό της CRAMM αποθηκεύει και επεξεργάζεται τα δεδομένα που συλλέγονται και πραγματοποιεί το συσχετισμό της αποτίμησης των επιμέρους στοιχείων του συστήματος με το μοντέλο του συστήματος. Έτσι, υπολογίζεται η έμμεση αξία των στοιχείων του συστήματος, υπολογισμός που δε θα μπορούσε να διεξαχθεί με εμπειρικές μεθόδους.

Στάδιο1, Βήμα 3: Επιβεβαίωση και επικύρωση της αποτίμησης

Η αποτίμηση των αγαθών των πληροφοριακών συστημάτων αποτελεί κρίσιμο παράγοντα για τη συνέχεια της μελέτης ανάλυσης και διαχείρισης επικινδυνότητας. Γι' αυτό το λόγο, πριν προχωρήσουν οι μελετητές στα επόμενα στάδια θα πρέπει πρώτα να επικυρωθεί η αποτίμηση.

Το κύριο προϊόν αυτού του σταδίου είναι η **αποτίμηση των Αγαθών** των πληροφοριακών συστημάτων. Τα αποτελέσματα του πρώτου σταδίου παρουσιάζονται σε σχετική έκθεση η οποία περιλαμβάνει:

- Τον ορισμό του προς ανάλυση συστήματος και των ορίων του.
- Τη μέθοδο εργασίας που ακολουθήθηκε.
- Την αποτίμηση των περιουσιακών στοιχείων των Π.Σ.
- Γενικά συμπεράσματα του πρώτου σταδίου.

3.6.2 Στάδιο 2: Ανάλυση επικινδυνότητας (Risk analysis)

Πιο συγκεκριμένα, στο πρώτο στάδιο της ανάλυσης υπολογίζεται ένας από τους τρεις παράγοντες που συνθέτουν την επικινδυνότητα. Αποτιμάται η αξία των στοιχείων των πληροφοριακών συστημάτων τα οποία εφόσον έχουν αξία ονομάζονται Αγαθά ή Περιουσιακά Στοιχεία. Στο δεύτερο στάδιο υπολογίζονται οι άλλοι δύο παράγοντες, το επίπεδο των απειλών (**threat level**) και το επίπεδο των

αδυναμιών του συστήματος (**vulnerability level**). Ο συνδυασμός των τριών παραγόντων δίδει το βαθμό επικινδυνότητας του συστήματος, έτσι ώστε να επιλεγούν τα κατάλληλα αντίμετρα. Τα βήματα που ακολουθούνται είναι:

- Προσδιορισμός των απειλών που αφορούν το κάθε Αγαθό
- Εκτίμηση απειλών (**threat assessment**) και αδυναμιών (**vulnerability assessment**)
- Υπολογισμός της επικινδυνότητας για κάθε συνδυασμό **Αγαθό-Απειλή-Αδυναμία**
- Επιβεβαίωση και επικύρωση του βαθμού επικινδυνότητας.

Στάδιο2, Βήμα 1: Προσδιορισμός των απειλών που αφορούν κάθε Αγαθό (Asset)

Η μέθοδος CRAMM δεν περιορίζεται στον προσδιορισμό των πιθανών απειλών που υφίσταται ένα πληροφοριακό σύστημα, αλλά επικεντρώνεται στον προσδιορισμό συγκεκριμένων απειλών για κάθε Αγαθό. Η CRAMM παρέχει μία ενδεικτική λίστα απειλών, καθώς και συστάσεις για το ποιες κατηγορίες στοιχείων ενός πληροφοριακού συστήματος αντιμετωπίζουν συνήθως τη συγκεκριμένη απειλή.

Όταν ένα από τα στοιχεία των πληροφοριακών συστημάτων αντιμετωπίζει απειλή τότε και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια απειλή. Με την CRAMM ο αναλυτής δε χρειάζεται να υπολογίζει ο ίδιος τις συσχετίσεις και αλληλεπιδράσεις.

Το CRAMM-εργαλείο ζητά από τους αναλυτές να συσχετίσουν τα Αγαθά με κατηγορίες απειλών από την παραπάνω κατάσταση. Έτσι, το εργαλείο προβαίνει σε συμπεράσματα με βάση το μοντέλο του συστήματος. Για παράδειγμα, αν μία απειλή (π.χ. πυρκαγιά) συσχετισθεί με μία τοποθεσία, τότε το εργαλείο συμπεραίνει ότι η απειλή αυτή αφορά το σύνολο των αγαθών που βρίσκονται στη συγκεκριμένη τοποθεσία.

Στάδιο 2, Βήμα 2: Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)

Για κάθε συνδυασμό απειλής-αγαθού εκτιμάται το μέγεθος της απειλής και η σοβαρότητα των αδυναμιών που μπορεί να οδηγήσουν στην πραγματοποίηση της απειλής. Η CRAMM υπολογίζει το επίπεδο της απειλής με βάση απαντήσεις σε ερωτηματολόγια των απειλών. Η εκτίμηση της απειλής γίνεται σε κλίμακα από 1-5 (very low, low, medium, high, very high). Ο αναλυτής μπορεί να παρέμβει και να τροποποιήσει τις τιμές που δίνει η CRAMM, αν το κρίνει σκόπιμο. Αντίστοιχα, για τις αδυναμίες συμπληρώνονται ερωτηματολόγια αδυναμιών και υπολογίζεται η σοβαρότητα της αδυναμίας σε κλίμακα 1-3 (low, medium, high). Οι απαντήσεις που θα δοθούν στα ερωτηματολόγια προκύπτουν από τα στοιχεία που συλλέγουν οι αναλυτές από τους χρήστες του συστήματος (συνεντεύξεις, στατιστικά κλπ).

Το εργαλείο της CRAMM παρέχει ερωτηματολόγια για κάθε συνδυασμό απειλής-αγαθού. Οι απαντήσεις σ' αυτά εισάγονται στο λογισμικό της CRAMM και υπολογίζεται το επίπεδο των απειλών και των αδυναμιών. Επίσης, παρέχεται η δυνατότητα στους αναλυτές να αλλάξουν τις τιμές που υπολογίστηκαν αυτοματοποιημένα. Επιπλέον, προκύπτει μία αναφορά για την εκτίμηση των απειλών-αδυναμιών ώστε να αξιολογηθούν τα αποτελέσματα αυτής της διαδικασίας.

Στάδιο 2, Βήμα 3: Υπολογισμός επικινδυνότητας για κάθε συνδυασμό Αγαθό-Απειλή-Αδυναμία

Η CRAMM υπολογίζει για κάθε συνδυασμό **Αγαθό-Απειλή-Αδυναμία** το βαθμό επικινδυνότητας. Δεν υπολογίζεται, δηλαδή, απλώς ένας βαθμός επικινδυνότητας για όλο το πληροφοριακό σύστημα, αλλά αποτιμάται η επικινδυνότητα για κάθε συνδυασμό Αγαθό-Απειλή-Αδυναμία. Για το σκοπό αυτό, χρησιμοποιούνται τόσο τα αποτελέσματα της εκτίμησης απειλών και αδυναμιών, όσο και το μοντέλο των πληροφοριακών συστημάτων. Έτσι, ο βαθμός επικινδυνότητας λαμβάνει υπόψη και τη συσχέτιση και τις εξαρτήσεις μεταξύ των στοιχείων των πληροφοριακών συστημάτων. Ο υπολογισμός του βαθμού επικινδυνότητας ακολουθεί μία κλίμακα 1-7 και γίνεται αυτόματα για κάθε συνδυασμό Αγαθό-Απειλή-Αδυναμία. Ο αναλυτής έχει τη δυνατότητα να παρέμβει και να αλλάξει κάποιες τιμές αν το θεωρεί σκόπιμο.

Στάδιο 2, Βήμα 4: Επικύρωση του βαθμού επικινδυνότητας

Η ομάδα μελέτης μπορεί να χρησιμοποιήσει τις αναφορές που παράγει το λογισμικό της CRAMM και το εργαλείο back-track για να εξετάσει συνολικά το βαθμό επικινδυνότητας. Σε περίπτωση που κριθεί ότι χρειάζεται να γίνουν κάποιες αλλαγές, τότε οι αναλυτές έχουν τη δυνατότητα είτε να αλλάξουν τις τιμές της επικινδυνότητας είτε να αλλάξουν τις τιμές που έχουν προκύψει από την εκτίμηση των απειλών και αδυναμιών και να υπολογίσουν εκ νέου την επικινδυνότητα.

3.6.3 Στάδιο 3: Διαχείριση επικινδυνότητας (Risk management)

Στηριζόμενοι στα αποτελέσματα της ανάλυσης επικινδυνότητας (Στάδιο 2), η μέθοδος CRAMM παράγει ένα σχέδιο ασφάλειας για το τα πληροφοριακά συστήματα. Αυτό αποτελείται από μία σειρά αντιμέτρων τα οποία κρίνονται απαραίτητα για την αντιμετώπιση και διαχείριση της επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν. Το σχέδιο ασφάλειας περιλαμβάνει και μία σειρά επιλογών και εναλλακτικών λύσεων, ώστε να παρέχεται ευελιξία στην εφαρμογή του.

Για συστήματα τα οποία έχουν αναπτυχθεί και λειτουργούν ήδη, το προτεινόμενο σχέδιο ασφάλειας μπορεί να συγκριθεί με τα υπάρχοντα αντίμετρα. Η τελική επιλογή των αντιμέτρων που θα εφαρμοστούν λαμβάνει υπόψη και το κόστος που έχουν τα αντίμετρα για τον οργανισμό. Τα βήματα του τρίτου σταδίου περιλαμβάνουν:

- Τον προσδιορισμό των προτεινόμενων αντιμέτρων.
- Τον σχεδιασμό του σχεδίου ασφάλειας.

Στάδιο 3, Βήμα 1: Προσδιορισμός των προτεινόμενων αντιμέτρων

Η CRAMM περιλαμβάνει μια ευρεία βάση αντιμέτρων, γνωστή ως βιβλιοθήκη αντιμέτρων. Τα αντίμετρα αυτά είναι τεχνικά, διοικητικά και οργανωτικά. Το λογισμικό της CRAMM μπορεί να επιλέξει αυτόματα μία κατάσταση προτεινόμενων αντιμέτρων με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας. Τα αντίμετρα χωρίζονται σε ομάδες, ανάλογα με το είδος των απειλών που καλούνται να αντιμετωπίσουν και ανάλογα με το είδος των αγαθών που καλούνται να προστατέψουν.

Η βάση των αντιμέτρων περιλαμβάνει τόσο τις εναλλακτικές λύσεις, δηλαδή ποιο αντίμετρο μπορεί να χρησιμοποιηθεί εναλλακτικά άλλου, καθώς και επιλογές υλοποίησής τους. Μεταξύ των προτεινόμενων αντίμετρων πρέπει να γίνουν συγκεκριμένες επιλογές. Οι επιλογές αυτές βασίζονται σε πολύ σημαντικό βαθμό στην εμπειρία των αναλυτών. Η CRAMM βοηθά ώστε οι επιλογές να ακολουθούν μία δομημένη προσέγγιση και να αιτιολογούνται επαρκώς. Τα κριτήρια που λαμβάνονται υπόψη στην τελική επιλογή περιλαμβάνουν τα εξής:

- Την επίδραση που θα έχουν τα αντίμετρα στη λειτουργία του οργανισμού.
- Τον υπάρχοντα προϋπολογισμό για την ασφάλεια των πληροφοριακών συστημάτων.
- Το κόστος εγκατάστασης και λειτουργίας των αντιμέτρων.
- Την άποψη της διοίκησης και τους στόχους της.
- Ενδεχόμενες ενδείξεις ότι οι απειλές θα αυξηθούν στο μέλλον.

Ακολούθως τα προτεινόμενα αντίμετρα συγκρίνονται με τα υπάρχοντα. Το λογισμικό της CRAMM περιέχει μία βάση με περισσότερα από 2.500 αντίμετρα, ενταγμένα σε ομάδες και ιεραρχημένα ανάλογα με το επίπεδο ασφάλειας που προσφέρουν. Το CRAMM εργαλείο επιλέγει αυτόματα τα αντίμετρα σύμφωνα με τα αποτελέσματα της ανάλυσης επικινδυνότητας. Η κατάσταση-απόφαση για ένα αντίμετρο μπορεί να είναι:

- Εγκατεστημένο (**installed**)
- Προς υλοποίηση (**to be installed**)
- Υπό υλοποίηση (**implementing recommendation**)
- Προτεινόμενο για υλοποίηση (**implemented recommendation**)
- Έχει καλυφθεί ήδη (**already covered**)
- Αναλαμβάνεται η επικινδυνότητα (**accept level of risk**)
- Υπό συζήτηση (**under discussion**)
- Μη εφαρμόσιμο (**not applicable**)

<u>Στάδιο 3, Βήμα 2: Σχεδιασμός του Σχεδίου Ασφάλειας</u>

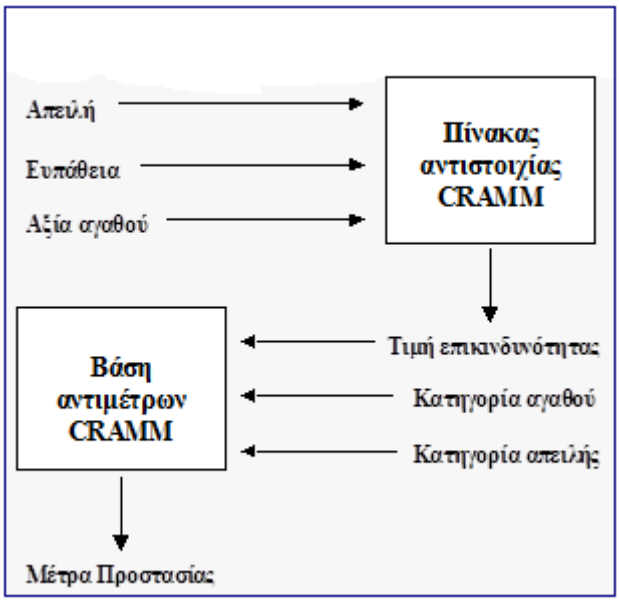
Σχεδιάζεται το σχέδιο ασφάλειας που περιλαμβάνει:

- Το σχέδιο πολιτικής ασφάλειας
- Τους ρόλους και τις υποχρεώσεις του κάθε ρόλου
- Τα συμπληρωματικά έργα που απαιτούνται για την υλοποίηση της ασφάλειας.

Το προϊόν του τρίτου σταδίου είναι το **Σχέδιο Ασφάλειας**.

3.6.4 Εξαγωγή μέτρων προστασίας από το εργαλείο της CRAMM

Στο παρακάτω διάγραμμα (Πίνακας 2) παρουσιάζεται η μέθοδος με την οποία το εργαλείο της CRAMM παράγει τον κατάλογο με τα προτεινόμενα μέτρα προστασίας.



Πίνακας 2 Παραγωγή Καταλόγου με τα προτεινόμενα μέτρα προστασίας

ΚΕΦΑΛΑΙΟ 4

4.1 Εφαρμογή της Μεθόδου CRAMM

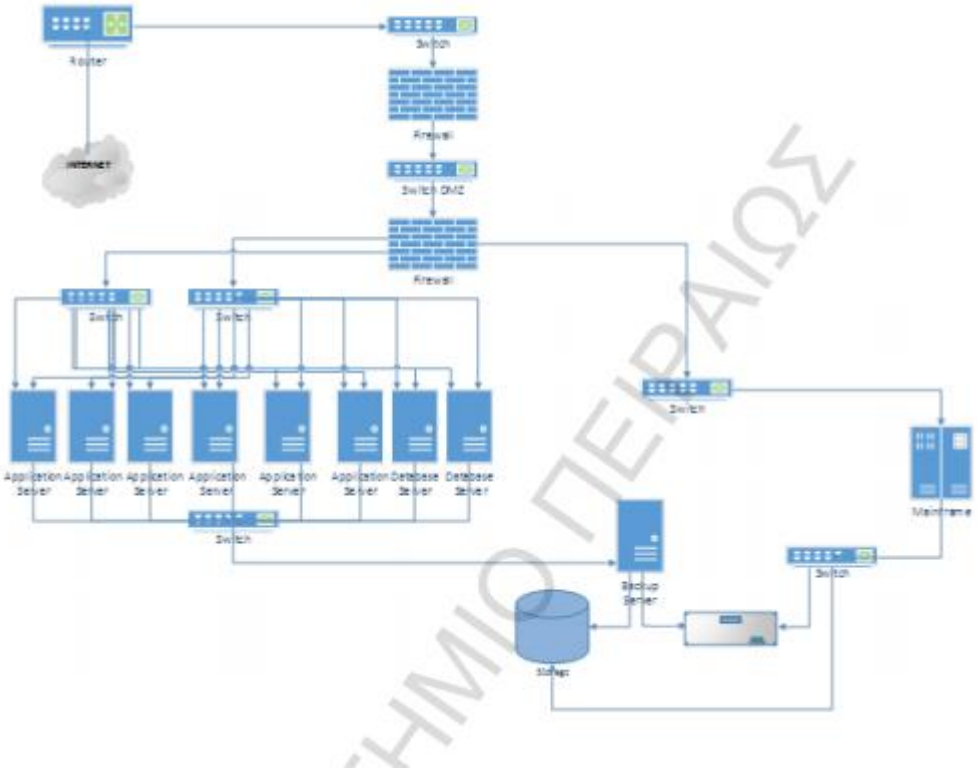
Για την συλλογή των απαραίτητων στοιχείων του Π.Σ. υπήρξε ένας κύκλος συνεντεύξεων με τα αρμόδια άτομα της Κεντρικής Υπηρεσίας Υπολογιστών και Επικοινωνιών (CCTA) το 1987 , έτσι ώστε να υπάρχει κατανόηση του Πληροφοριακού Συστήματος., συνεπώς και τα περιουσιακά στοιχεία του και να καθοριστεί το εύρος της μελέτης. Εξαιτίας του μεγάλου μεγέθους του Π.Σ. έχουν επιλεγεί μόνο συγκεκριμένα συστήματα για μελέτη. Σε αυτό το στάδιο γίνεται καταγραφή του υλικού, του λογισμικού και των εγκαταστάσεων της εταιρείας. (Χαλβατζή 2014)

4.1.1 Πληροφοριακό Σύστημα

Υλικός Εξοπλισμός (Hardware)

Το αρχικό και πιο σημαντικό βήμα είναι να καθορίσουμε τον υλικό εξοπλισμό του Π.Σ., δηλαδή τους υπολογιστές, το δίκτυο, τα μέσα αποθήκευσης κ.τ.λ. Η φυσική αρχιτεκτονική του δικτύου απεικονίζεται στην Εικόνα 2. (Χαλβατζή 2014)

- Mainframe της IBM Z10, λειτουργικό σύστημα z/OS (zero downtime).
- Δύο Εξυπηρετητές Βάσεων Δεδομένων (Database servers) DELL PowerEdge R 900 Redhat Enterprise Linux 4.6 64 bit, σε διάταξη active-active.
- Τέσσερεις Εξυπηρετητές εφαρμογών (Application Servers) DELL PowerEdge 2950 Redhat Enterprise Linux 4.6 64 bit, σε διάταξη active-active.
- Ένας Εξυπηρετητής Εφαρμογών (Application server) Windows 2008 R2.
- Δύο συστήματα ασφαλείας Microsoft’s Threat management Gateway (TMG), που προσφέρουν firewall.
- Ένα σύστημα ασφαλείας Check Point το οποίο χρησιμοποιείται ως Proxy και ως URL filtering.
- Δύο μεταγωγείς (switches) Cisco 3750.
- Πέντε μεταγωγείς (switches) Dell Power Connect 2708, εκ των οποίων οι τρεις λειτουργούν και ως δρομολογητές.
- Δύο συσκευές λήψης αντιγράφων ασφάλειας, NetBackup 7.5 της εταιρείας Symantec.
- Τρείς μονάδες αδιάλειπτης παροχής ισχύος (UPS) Chloride 70-Net, μέγιστης υποστηριζόμενης ισχύς 50-60 kVA.
- Μία γεννήτρια πετρελαίου Sunlight μοντέλο SIS-160KVA SOUNDPROUFED 1500/G.



Εικόνα 2 Αρχιτεκτονική Δικτύου (Χαλβατζή 2014)

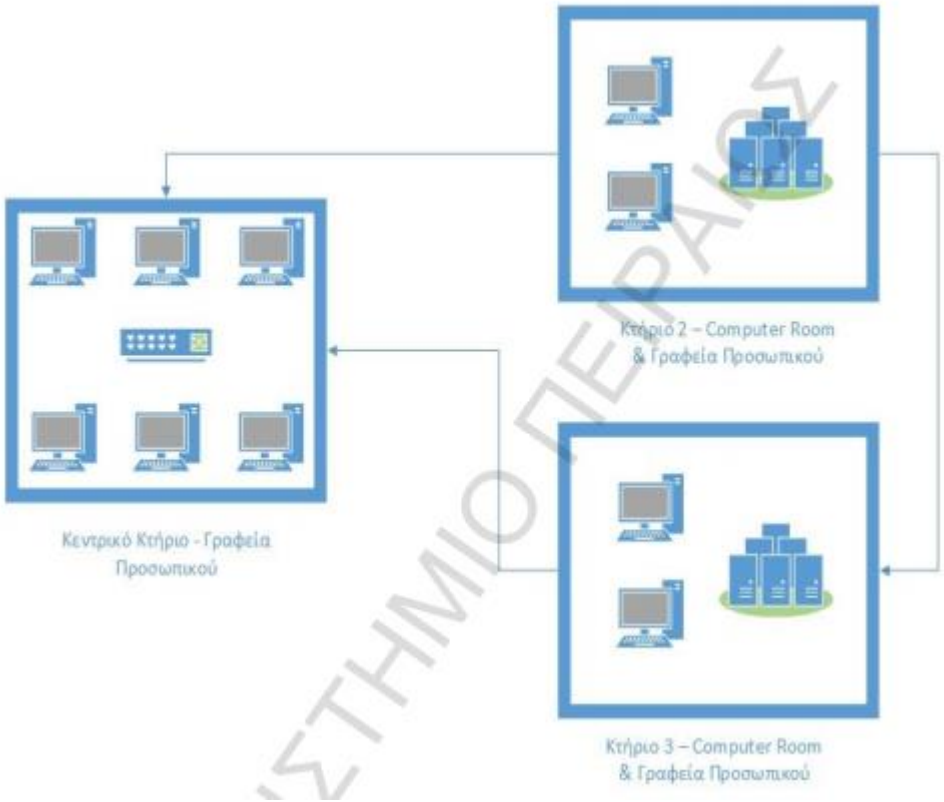
Κτηριακές Εγκαταστάσεις

Οι τοποθεσίες που περιλαμβάνονται στη μελέτη απεικονίζονται στην Εικόνα 3. Στη μελέτη έχουν συμπεριληφθεί (Χαλβατζή 2014):

- το κεντρικό κτήριο της εταιρείας, στο οποίο υπάρχουν μόνο γραφεία προσωπικού,
- το δεύτερο κτήριο, στο οποίο υπάρχει ένα computer room και κάποια γραφεία προσωπικού και
- το τρίτο κτήριο της εταιρείας, όπου στεγάζεται το δεύτερο computer room με εφεδρικά συστήματα (disaster site) και γραφεία προσωπικού.

Επίσης, υπάρχουν και κάποια επιπλέον κτήρια που δεν έχουν συμπεριληφθεί στη μελέτη καθώς είναι ίδια με το κεντρικό κτήριο, οπότε δεν κρίθηκε αναγκαία η περιγραφή τους. Ο καθορισμός των κτηριακών εγκαταστάσεων απαιτείται καθώς στην παρούσα μελέτη λαμβάνονται υπόψη και οι κίνδυνοι

από φυσικές και περιβαλλοντικές καταστροφές.



Εικόνα 3 Κτηριακές Εγκαταστάσεις (Χαλβατζή 2014)

Λογισμικό – Εφαρμογές

Το Π.Σ. που μελετάται αποτελείται από αρκετές εφαρμογές, αλλά στην παρούσα μελέτη αποφασίστηκε να συμπεριληφθούν οι ακόλουθες τέσσερις πιο σημαντικές (Χαλβατζή 2014):

- Εφαρμογή του Συστήματος Πελατών,
- Εφαρμογή του Συστήματος Οικονομικής και Λογιστικής Διαχείρισης,
- Εφαρμογή του Συστήματος Διαχείρισης Εγγράφων και Πρωτοκόλλου,
- Εφαρμογή του Συστήματος Διαχείρισης Προσωπικού.

1. Σύστημα Πελατών

Το σύστημα πελατών θεωρείται το πιο κρίσιμο σύστημα της εταιρείας. Η εφαρμογή του συστήματος πελατών έχει δημιουργηθεί ειδικά για τη συγκεκριμένη εταιρεία και σκοπός της είναι η υποστήριξη των λειτουργικών απαιτήσεων της Διεύθυνσης Πωλήσεων. Συγκεκριμένα, η εφαρμογή περιλαμβάνει τα εξής (Χαλβατζή 2014):

- Διαχείριση πελατών,

- Διαχείριση μετρητών,
- Πληρωμή και παρακολούθηση πληρωμών (λογαριασμών),
- Τιμολόγηση και έκδοση λογαριασμού,
- Παρακολούθηση διακοπών-αποκοπών,
- Παρακολούθηση ενδείξεων,
- Λογιστική παρακολούθηση,
- Έκδοση αναφορών και στατιστικών,
- Είσπραξη εισφορών για θυγατρικές εταιρείες.

2. Σύστημα Οικονομικής και Λογιστικής Διαχείρισης

Σκοπός του συστήματος είναι να υποστηρίξει το Οικονομικό και Λογιστικό τμήμα της εταιρείας, έτσι ώστε να καλύπτονται οι λειτουργικές του απαιτήσεις όσον αφορά τα ακόλουθα (Χαλβατζή 2014):

- Κατάρτιση και εκτέλεση του προϋπολογισμού της εταιρείας,
- Αξιοποίηση όλων των δυνατοτήτων για τη δημιουργία και απόκτηση εσόδων,
- Βεβαίωση των επιβαλλόμενων προστίμων, τελών, δικαιωμάτων και εισφορών,
- Διαχείριση και εκτέλεση προμηθειών,
- Καταγραφή της περιουσίας της εταιρείας,
- Λογιστική και ταμειακή διαχείριση της εταιρείας,
- Τήρηση και συμφωνία των τραπεζικών λογαριασμών,
- Τήρηση του διπλογραφικού συστήματος,
- Διαχείριση αποθηκών και παγίων.

Οι παραπάνω λειτουργικές απαιτήσεις που διαθέτει το σύστημα Οικονομικής και Λογιστικής διαχείρισης καλύπτονται μέσω των ακόλουθων εφαρμογών (Χαλβατζή 2014):

- Γενική – Αναλυτική Λογιστική
- Διαχείριση Προϋπολογισμού
- Διαχείριση Κεφαλαίων

- Διαχείριση Εισπράξεων / Πληρωμών
- Διαχείριση Προμηθειών / Αποθήκης
- Διαχείριση Πάγιων Στοιχείων
- Τήρηση Λογιστικών Βιβλίων και Καταστάσεων
- Λογιστική Διαχείριση Έργων.

3. Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου

Σκοπός του συστήματος Διαχείρισης Εγγράφων και Πρωτοκόλλου είναι η υποστήριξη των λειτουργικών απαιτήσεων της γραμματείας του Μηχανογραφικού Κέντρου της εταιρείας. Το ίδιο σύστημα χρησιμοποιείται από όλες τις γραμματείες της εταιρείας. Μέσω της εφαρμογής γίνεται πρωτοκόλληση εισερχόμενων και εξερχόμενων εγγράφων, έτσι ώστε να εξασφαλίζεται η ορθή απόδοση μοναδιαίου αριθμού πρωτοκόλλου στα έγγραφα και ακολουθεί δρομολόγηση αυτών σε συγκεκριμένους αποδέκτες ή σε ομάδες αποδεκτών. Επιπλέον, γίνεται έλεγχος για διπλές αριθμήσεις και διπλές καταχωρήσεις εγγράφων. (Χαλβατζή 2014)

4. Σύστημα Διαχείρισης Προσωπικού

Σκοπός του συστήματος Διαχείρισης Προσωπικού είναι η υποστήριξη των λειτουργικών απαιτήσεων του τμήματος Προσωπικού της εταιρείας. Το τμήμα αυτό είναι υπεύθυνο για την αποτελεσματική διεκπεραίωση όλων των θεμάτων του προσωπικού και της μισθοδοσίας του. Η εφαρμογή αυτή έχει δημιουργηθεί ειδικά για τις ανάγκες τις εταιρείας και αφορά τις ακόλουθες λειτουργίες:

- Μηχανογραφική τήρηση των προσωπικών μητρώων και έκδοση πιστοποιητικών υπηρεσιακών μεταβολών των υπαλλήλων.
- Μηχανογραφική τήρηση αρχείων διορισμού, πρόσληψης, μονιμοποίησης, μετακίνησης, προαγωγής, λύσης υπαλληλικής σχέσης και συνταξιοδότησης προσωπικού.
- Μηχανογραφική τήρηση σύμβασης προσωπικού, κρατήσεις, ταμεία, φορολογικά στοιχεία, προϋπηρεσία, άδειες, συντάξεις.
- Διαχείριση κατάταξης των υπαλλήλων σε μισθολογική κλίμακα και διαχείριση μισθοδοσίας προσωπικού. Εκκαθάριση αποδοχών (τακτικές, επιδόματα, ασθενείας, υπερωρίες, αποζημίωσης, αναδρομικών). (Χαλβατζή 2014)

Δεδομένα

Για να μπορέσει η CRAMM να επεξεργαστεί τα δεδομένα που συμπεριλαμβάνονται στη μελέτη, είναι απαραίτητη η ταξινόμησή τους στις εξής κατηγορίες:

- Οικονομικά (Financial)
- Προσωπικά (Personal)
- Επιχειρησιακά Ευαίσθητα (Commercially Sensitive)
- Σχετικά με την ασφάλεια (Safety Related) και
- Όλα τα υπόλοιπα (Other Data Types)

Τα δεδομένα που τυγχάνουν επεξεργασίας από τις εφαρμογές έχουν καταταγεί σε ομάδες όπως φαίνονται στον Πίνακα 3.

Πίνακας 3 Ταξινόμηση Δεδομένων (www.unipi.gr)

Εφαρμογές	Ομάδες Δεδομένων	Κατηγοριοποίηση Δεδομένων
Σύστημα Πελατών	Οικονομικά Δεδομένα (Data Financial)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα iv. Άλλο τύπο δεδομένων (π.χ. Μετρήσεις πελατών)
Σύστημα Οικονομικής & Λογιστικής Διαχείρησης	Οικονομικά Δεδομένα 2 (Data Financial 2)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα iv. Άλλο τύπο δεδομένων (π.χ. Δεδομένα διαχείρισης αποθήκης)
Σύστημα Διαχείρισης Εγγράφων και Πρωτοκόλλου	Δεδομένα Διαχείρισης Πληροφοριών (Data Management Information)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα
Σύστημα Διαχείρισης Προσωπικού	Δεδομένα Μισθοδοσίας (Data Payroll)	i. Οικονομικά ii. Προσωπικά iii. Επιχειρησιακά Ευαίσθητα

Παρόλο που το σύστημα Οικονομικής και Λογιστικής Διαχείρισης και το Σύστημα Πελατών διαχειρίζονται οικονομικά δεδομένα, η κατηγοριοποίηση πρέπει να γίνει διαφορετικά καθώς περιλαμβάνουν διαφορετικά δεδομένα και χρήζουν διαφορετικού επιπέδου ασφάλειας, οπότε θα πρέπει να δημιουργηθούν δύο ομάδες δεδομένων. (Χαλβατζή 2014)

4.1.2 Αποτίμηση των Περιουσιακών Στοιχείων του Πληροφοριακού Συστήματος

Σε αυτό το σημείο γίνεται η αποτίμηση των δεδομένων, με βάση τις επιπτώσεις της απώλειας της διαθεσιμότητας, της ακεραιότητας και της εμπιστευτικότητάς τους. Ακολουθεί η αποτίμηση του λογισμικού με τον ίδιο τρόπο και η αποτίμηση του υλικού με βάση το κόστος αντικατάστασης. Για την αποτίμηση δεν λαμβάνονται υπόψη τα υφιστάμενα μέτρα ασφάλειας, αλλά ούτε και η πιθανότητα εκδήλωσης μιας απειλής. Αυτό που λαμβάνεται υπόψη είναι η επίπτωση που θα έχει για την εταιρεία η πραγματοποίηση μιας απειλής.

Η μέθοδος CRAMM περιέχει κάποιους πίνακες αποτίμησης με βάση τους οποίους γίνεται η αξιολόγηση ακολουθώντας μία αριθμητική κλίμακα 1-10. Στην περίπτωση όπου οι πιθανές επιπτώσεις ενός περιουσιακού στοιχείου εντάσσονται σε παραπάνω από μία κατηγορίες, τότε λαμβάνεται υπόψη η κατηγορία με το μεγαλύτερο βαθμό. Στους πίνακες που ακολουθούν εμφανίζονται τα αποτελέσματα αυτού του σταδίου για τις τέσσερις ομάδες δεδομένων που περιγράφηκαν προηγουμένως. Οι περιπτώσεις που μελετήθηκαν θεωρούνται οι πιο σημαντικές κατά τη γνώμη των αρμόδιων στελεχών της εταιρείας. (Χαλβατζή 2014)

4.1.2.1 Αποτίμηση Δεδομένων 1η Ομάδα – Οικονομικά Δεδομένα

Η πρώτη ομάδα αφορά στα δεδομένα που τυγχάνουν επεξεργασίας από το Σύστημα Πελατών. Τα δεδομένα αυτά περιλαμβάνουν κυρίως οικονομικά στοιχεία, προσωπικά στοιχεία πελατών, δεδομένα λογαριασμών και τιμολογίων, επιταγές προμηθευτών κ.ά. Η απώλεια της διαθεσιμότητας των δεδομένων αυτών έχει ως αποτέλεσμα σοβαρή οικονομική απώλεια για την εταιρεία. Πιθανόν να υπάρξουν σοβαρές κυρώσεις, καθώς δεν θα είναι εφικτή η είσπραξη εισφορών για τις θυγατρικές εταιρείες και επιπλέον προκύπτει παύση εισροής εσόδων.

Η απώλεια της ακεραιότητας των δεδομένων μπορεί να επηρεάσει τα οικονομικά και εμπορικά συμφέροντα της εταιρείας. Ειδικότερα, σε περίπτωση ολικής καταστροφής παύει η κύρια λειτουργία της εταιρείας, επηρεάζοντας έτσι και άλλες εταιρείες που εξαρτώνται από τις παρεχόμενες υπηρεσίες του συστήματος πελατών (π.χ. θυγατρικές). Στις περιπτώσεις ύπαρξης λαθών εκτιμάται ότι θα υπάρξει οικονομική απώλεια λαμβάνοντας υπόψη περιπτώσεις λαθών σε λογαριασμούς και σε εισπράξεις τελών για θυγατρικές εταιρείες. Τέλος, σε περιπτώσεις εκτεταμένη ύπαρξη λαθών ή/και σκόπιμη αλλοίωση των δεδομένων, όπου μπορεί να υπάρξουν αλλαγές σε μετρήσεις, εξοφλητικά τιμολόγια κ.τ.λ., έχει ως αποτέλεσμα οικονομική απώλεια για την εταιρεία. Η απώλεια της εμπιστευτικότητας αμαυρώνει τη φήμη της εταιρείας, γεγονός το οποίο συνεπάγεται και την πιθανή πτώση της μετοχής. (Χαλβατζή 2014)

4.1.2.2 2η Ομάδα – Οικονομικά Δεδομένα 2

Η δεύτερη ομάδα περιλαμβανει τα δεδομένα του σύστηματος Οικονομικής και Λογιστικής Διαχείρισης. Στο σύστημα αυτό περιλαμβάνονται προσωπικά δεδομένα, συμβάσεις προμηθευτών, δάνεια, επιταγές, δεδομένα διαχείρισης αποθηκών κ.ά. Η απώλεια της διαθεσιμότητας των δεδομένων είναι ένα μείζον θέμα και μπορεί να προκαλέσει από οικονομική απώλεια μέχρι και αδυναμία τηρήσης των νομικών και κανονιστικών απαιτήσεων, διότι είναι αδύνατη η αποπλήρωμη δανείων και επιταγών προς τρίτους και επιπλέον μπορεί να υπάρξουν μηνύσεις εις βάρος της εταιρείας. Η απώλεια της ακεραιότητας των δεδομένων σε περίπτωση ολικής καταστροφής συνεπάγεται τη μη ολοκλήρωση των οικονομικών υποχρεώσεων της εταιρείας προς τρίτους και τη μη ολοκλήρωση κρίσιμων εργασιών που απαιτούνται, όπως προμήθειες, διαγωνισμοί κ.τ.λ., επηρεάζοντας την ομαλή λειτουργία της εταιρείας.

Η απώλεια της εμπιστευτικότητας επηρεάζει την καλή εικόνα της εταιρείας, καθώς περιλαμβάνονται επιχειρησιακά ευαίσθητα δεδομένα, τα οποία δεν πρέπει να είναι διαθέσιμα στο ευρύ κοινό. Η ύπαρξη

λαθών και η σκόπιμη αλλοίωση δεν έχουν αποτιμηθεί, καθώς γίνεται επικύρωση της ορθότητας των δεδομένων με βάσει τα χειρόγραφα πριν την τελική υποβολή. (Χαλβατζή 2014)

4.1.2.3 3η Ομάδα - Δεδομένα Διαχείρισης Πληροφοριών

Η τρίτη ομάδα αφορά στα εισερχόμενα και εξερχόμενα έγγραφα της εταιρείας, τα οποία πρωτοκολλούνται από τις γραμματείες και δρομολογούνται κατάλληλα. Η απώλεια της διαθεσιμότητας των δεδομένων δεν έχει σημαντική επίπτωση για την εταιρεία, καθώς η διαδικασία μπορεί να επιτελεστεί με χειρόγραφο τρόπο μέχρι την αποκατάσταση της ομαλής λειτουργίας.

Η απώλεια της ακεραιότητας των δεδομένων σε περίπτωση ολικής καταστροφής θα επιφέρει οικονομική απώλεια, η οποία προκύπτει από το κόστος επαναφοράς του συστήματος και επανεισαγωγής των χειρόγραφων δεδομένων. Η ύπαρξη λαθών στα δεδομένα πρωτοκόλλου δεν αποτιμάται, διότι τα δεδομένα φυλάσσονται και σε χειρόγραφη μορφή και πριν την επικύρωσή τους επιβεβαιώνεται η ορθότητά τους. Η απώλεια της εμπιστευτικότητας, λαμβάνοντας υπόψη την αποκάλυψη των δεδομένων σε προσωπικό της εταιρείας, επηρεάζει τη φήμη της αλλά καθώς τα δεδομένα δεν είναι εμπιστευτικά η επίπτωση θα είναι πολύ μικρή. Η αποκάλυψη των δεδομένων σε τρίτους έχει σημαντική επίπτωση, διότι μπορεί να οδηγήσει σε δυσφήμιση της εταιρείας. (Χαλβατζή 2014)

4.1.3 Εκτίμηση Επικινδυνότητας

Ο βαθμός επικινδυνότητας είναι συνάρτηση τριών παραγόντων: της επίπτωσης, της αξίας των περιουσιακών στοιχείων και του επιπέδου των αδυναμιών:

Πιθανότητα = Απειλή x Αδυναμία

Επικινδυνότητα = Πιθανότητα x Επίπτωση

Για να γίνει η αποτίμηση των απειλών που αντιμετωπίζει το Π.Σ. έχουν δοθεί από τα αρμόδια στελέχη της εταιρείας απαντήσεις στα ερωτηματολόγια που παράγει η CRAMM. Επιπλέον, έχουν πραγματοποιηθεί επιτόπιοι έλεγχοι για τον εντοπισμό των αδυναμιών του Π.Σ. Η πιθανότητα πραγματοποίησης των απειλών αξιολογείται στην κλίμακα 1-5 (πολύ χαμηλή, χαμηλή, μέτρια, υψηλή, πολύ υψηλή) και η αξιολόγηση του επιπέδου ευπάθειας για κάθε συνδυασμό απειλής – περιουσιακού στοιχείου αξιολογείται στην κλίμακα 1-3 (χαμηλή, μέτρια, υψηλή). Η συσχέτιση των απειλών με τα περιουσιακά στοιχεία ή τις ομάδες αυτών μπορεί να γίνει είτε με συσχετισμό μιας απειλής σε ένα περιουσιακό στοιχείο ή σε μία ομάδα περιουσιακών στοιχείων, είτε με το συσχετισμό ενός περιουσιακού στοιχείου σε μία ή περισσότερες απειλές. Στην παρούσα μελέτη η συσχέτιση έχει πραγματοποιηθεί συσχετίζοντας κάθε απειλή με ένα ή περισσότερα περιουσιακά στοιχεία. (Χαλβατζή 2014)

4.1.4 Αποτελέσματα Αποτίμησης

Στον πίνακα που ακολουθεί παρουσιάζονται τα αποτελέσματα της αποτίμησης των σημαντικότερων απειλών που αντιμετωπίζει το Π.Σ (Χαλβατζή 2014)

Απειλή	Περιουσιακό Στοιχείο	Πιθανότητα Απειλής	Επίπεδο Αδυναμίας
Πλαστοπροσωπία από Εσωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Πελατών	Πολύ Υψηλή	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Υψηλή	Υψηλή
Πλαστοπροσωπία από Παρόχους Υπηρεσιών	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Πελατών	Πολύ Χαμηλή	Υψηλή
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Πολύ Χαμηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Προσωπικού	Πολύ Χαμηλή	Μέτρια
Πλαστοπροσωπία από Εξωτερικούς Χρήστες	Λογισμικό του συστήματος Λογιστικής & Οικονομικής Διαχείρισης	Υψηλή	Χαμηλή
	Λογισμικό του συστήματος Πελατών	Υψηλή	Μέτρια
	Λογισμικό του συστήματος Διαχείρισης Εγγράφων & Πρωτοκόλλου	Μέτρια	Χαμηλή

Πίνακας 4: Αποτίμιση (www.unipi.gr)

4.1.5 Αντίμετρα

Στα παραπάνω αποτελέσματα δεν έχουν ληφθεί υπόψη τα ήδη εγκατεστημένα μέτρα προστασίας (π.χ. disaster site). Έτσι, σε αυτό το σημείο έρχεται ο υπολογισμός των αντιμέτρων - μέτρων προστασίας που είναι και το τρίτο βήμα της μεθοδολογίας.

Η CRAMM περιλαμβάνει μία δομημένη βάση από τεχνικά, οργανωτικά και διοικητικά μέτρα προστασίας, γνωστή και ως βιβλιοθήκη μέτρων προστασίας. Μέσω του λογισμικού της CRAMM μπορεί να γίνει η αυτόματη επιλογή μιας λίστας προτεινόμενων αντιμέτρων, με βάση τα αποτελέσματα της ανάλυσης κινδύνου. Τα προτεινόμενα μέτρα προστασίας συγκρίνονται με τα υπάρχοντα και είναι πάντα προτιμότερο να παραμένει κάποιο από τα υπάρχοντα παρά να αντικαθίσταται από κάποιο ισοδύναμό του. (Χαλβατζή 2014)

Ένα μέτρο προστασίας μπορεί να βρίσκεται σε μία από τις ακόλουθες καταστάσεις:

- Εγκατεστημένο,
- Προς εγκατάσταση,
- Προς υλοποίηση,
- Προτεινόμενο προς υλοποίηση,
- Έχει ήδη καλυφθεί (από κάποιο άλλο μέτρο),
- Αποδεκτός εναπομένων βαθμός κινδύνου (το μέτρο δεν εγκαθίσταται),
- Υπό συζήτηση,
- Μη εφαρμόσιμο.

ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα

Οι λιμένες αποτελούν το σημαντικότερο κρίκο στην αλυσίδα των θαλάσσιων μεταφορών. Καθώς η ναυτιλία ως κλάδος της οικονομίας παρουσιάζει έντονα παγκοσμιοποιημένο χαρακτήρα η ασφάλεια των λιμένων συνιστά πρωταρχικό παράγοντα για την απρόσκοπτη λειτουργία τους. Έτσι ο τομέας της ασφάλειας των λιμένων έχει τεθεί υπό τη σκέπη της διεθνούς κοινότητας καθώς το πλοίο, ως μεταφορικό μέσο, κινείται μεταξύ λιμένων διαφορετικών κρατών και ηπείρων.

Από τη μελέτη της νομοθεσίας προκύπτει ότι η διεθνής κοινότητα έχει ασχοληθεί επισταμένως με την ασφάλεια των λιμένων που αναφέρεται σε θέματα ανθρωπογενούς προέλευσης. Ειδικότερα έχει δώσει έμφαση σε θέματα εργασιακά, ενδεχομένως υπό την πίεση της διεθνοποίησης του συνδικαλιστικού κινήματος όπως αυτό εκφράζεται από τη Διεθνή Οργάνωση Εργασίας. Επίσης μετά την τρομοκρατική ενέργεια της 11ης Σεπτεμβρίου 2001 στις ΗΠΑ η διεθνής κοινότητα εστίασε το ενδιαφέρον της και στην ασφάλεια των λιμένων από έκνομες ενέργειες θεσπίζοντας και θέτοντας σε εφαρμογή Ειδικό Κώδικα.

Παρατηρείται όμως ένα έλλειμμα σχετικά με τη θέσπιση κανόνων για την πρόληψη και μετριασμό των απειλών φυσικής προέλευσης. Βέβαια στη διεθνής νομοθεσία γίνεται αναφορά σε φυσικές απειλές με γενικό χαρακτήρα. Δεν υπάρχει όμως ειδική εστίαση στις φυσικές καταστροφές σε λιμένες και λιμενικές εγκαταστάσεις. Απαιτείται λοιπόν η ενεργοποίηση των φορέων για την διερεύνηση της επίδρασης των φυσικών φαινομένων στη λειτουργία των λιμένων και μάλιστα εξειδικευμένα ανάλογα με τη γεωγραφική περιοχή και τη λειτουργικότητα του λιμένα.

Βιβλιογραφία

1. “Bow-tie Modeling in Effective Safety Risk Control”, Lisa Shi Senior Consultant, 5 June 2009, Technical Seminar for HKIE and HKARMS, LLOYD’S REGISTER RAIL
2. “Bowtie Pro Methodology”, Enterprise business Centre, Admiral Court, Poynerbook road, Aberdeen, UK, www.bowtiepro.com
3. “Decision Analysis Tools for Risk Management of Industrial Ports and Harbors”, Dr/ Greg Parnell, Professor at Department of Systems Engineering, United States Military Academy at West Point.
4. “Port Hazard and Risk Management system (HARMS)”, BMT ISIS Ltd/ (www.bmtharms.co.uk)
5. “Port Risk Management”, GAO Report to Congressional committees, GAO-07-412.
6. “PortSec. Port Operations Modeling for Security Risk Management and Resource Allocation”/ March 17-2009, Michael Orosz, Ph.D. USC.
7. “Practical HSE risk Management – An Introduction to the Bow-Tie Method”/ (Internation conference for Achieveing Health & Safety Best Practise in Construction, Dubai, UAE, 26 February 2007) Gareth Book, Risktec Solution Ltd.
8. “Security and Risk-based Models in Shipping and Ports. review and Critical Analysis”/ Khalid Bichou, Centre for Transportation Studies, Imperial College London, United Kingdom. (Discussion Paper No. 2008-20, December 2008)
9. “Seismic Risk Management for Container Ports”, Glenn J/ Rix and Stuart D/ Werner/ www.neesgc.gatech.edu, (Seismic risk Management for Port systems)
10. “Structuring an Effective Ports Insurance Programme”/ (David Wardle, Marsh Pty Ltd, Presentation At Pacific Countries Ports Conference, September 2010). www.marsh.com.au
11. “The Risk Management Function” AAPA Administration Seminar July, 2005, Cindi Heffernan, CPCU
12. Best Management Practice 3 - Piracy off the coast of Somalia and Arabian Sea area.
13. Clemen, R.T., Winkler, R.L. 1999. Combining Probability Distributions from Experts in Risk Analysis, Risk Analysis, 19(2), 187–203
14. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. Available at: http://eur-lex.europa.eu
15. Derivatives and Risk Management in shipping, Καβουσάνος Βιζβίκης, Witherby publishing 1st Edition

16. DNV (2006) Risk management/Assessment course in the shipping industry

17. DNV Course (2009) – Maritime Labor Convention 2006

18. Epsilon Odessa Training Center : Risk Assessment & Incident Investigation Course 2009

19. Europa (Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης), 2002. Θαλάσσια ασφάλεια : Ευρωπαϊκός Οργανισμός για την ασφάλεια στη θάλασσα . Δικτυακός τόπος : http://europa.eu/legislation_summaries/institutional_affairs/ institutions_bodies_and_agencies/l24245_el.htm

20. European Commission, Communication from the Commission to the Council and the European Parliament, COM (2007) 62. Improving quality and productivity at work: Community strategy 2007-2010 on health and safety at work. Available at: http://eur-lex.europa.eu

21. European Commission, Communication from the Commission to the Council and the European Parliament, COM (2007) 62. Improving quality and productivity at work: Community strategy 2007-2012 on health and safety at work. Available at: http://eur-lex.europa.eu

22. European Commission, Guidance on risk assessment at work, Luxembourg, 1996, p. 35. Available at: http://osha.europa.eu/en/topics/riskassessment/guidance.pdf

23. European Commission. EU legislation on Maritime Security. [online] Δικτυακός τόπος: http://ec.europa.eu/transport/modes/maritime/security/doc/ legislation_maritime_security.pdf

24. European Maritime Safety Agency (EMSA). Maritime Security Overview. Δικτυακός τόπος : http://emsa.europa.eu/implementation-tasks/visits-and- inspections/maritime-security.html

25. European Union Agency for Network and Information Security (enisa), 2011. Maritime Cyber Security Workshop in Brussels Δικτυακός τόπος: https://www.enisa.europa.eu/media/news-items/cyber-security-in-the-maritime- sector-workshop-in-brussels

26. Executive Session on Maritime Risk Management, Malmö (Sweden), 9 October 2000

27. HSE (2001) "Reducing Risk, Protecting People :HSE's decision-making process", Health & Safety Commission, 2001 Why Risk Management in Shipping? Speech by Mr. W.A. O'Neil, Secretary-General of IMO

28. ILO – Accident prevention on board and at shore (2006) Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work. Available at: http://eur-lex.europa.eu

29. International Maritime Organization. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). Δικτυακός τόπος : http://www.imo.org/About/Conventions/ListOfConventions/Pages/International- Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for- Seafarers-(STCW).aspx

30. International Maritime Organization. International Convention on Maritime Search and Rescue (SAR). Δικτυακός τόπος: http://www.imo.org/About/ Conventions/ListOfConventions/Pages/International-Convention-on-Maritime- Search-and-Rescue-(SAR).aspx

31. Ιωάννης Καλογερόπουλος , " Ανάλυση Επικινδυνότητας του Πληροφοριακού Συστήματος Ασφαλιστικής Εταιρίας Πιστώσεων με τη χρήση του Ebios" Δικτυακός τόπος : http://pages.cs.aueb.gr/courses/epl131/files/CSS_notes.pdf

32. Linking Risk assessment of marine operations to safety management in ports. Dr. Vladimir M. Trbojevic, EQE International Ltd, ABS Consulting, ABS House. MTS conference 2001.

33. Mathiensen T.C (1997) "Cost Benefit Analysis of Existing Bulk Carriers", DNV Paper Series No 97-P008.

34. Millenia Maritime Inc (2010) Risk Assessment Procedure

35. N.Nikitakos 'Communications security using spread spectrum' (in Greek) p. 249 - 260, in "Information Security' Greek Computer Society , 1995

36. N.Nikitakos 'Defense Shipbuilding Industry- Present situation – future prospects' Ministry of Defense, Athens 2003

37. N.Nikitakos « Maritime Communications » (in Greek) , Ministry of Educations, Secondary Technical Schools, Maritime sector, Sept. 2001.

38. N.Nikitakos «Elements of Electricity and Electronics» (in Greek), Ministry of Educations, Secondary Technical Schools, Maritime sector, Sept. 2001.

39. Paris MoU. A short history of the Paris MoU on PSC. Δικτυακός τόπος: https://www.parismou.org/about-us/history

40. Sun Enterprises Ltd (2009) Risk Management Plan SMSystem

41. Ευρωπαικος οργανισμος για την ασφαλεια και υγεια στην εργασια Δικτυακός τόπος : https://osha.europa.eu/el/topics/riskassessment/index_html/ carry_out

42. Χαλβατζή , "Συγκριτική Μελέτη Ανάλυσης Επικινδυνότητας "

43. Εφημερίδα της Κυβερνήσεως , Τεύχος Πρώτο , Αρ . Φύλλου 281. ΝΟΜΟΣ ΥΠ ' ΑΡΙΘ . 3622. Ενίσχυση της ασφάλειας πλοίων , λιμενικών εγκαταστάσεων και λιμένων και άλλες διατάξεις . 20 Δεκεμβρίου 2007

44. Προεδρικό διάταγμα 70/1990(φεκ 31/Α/14-3-90) «Ασφάλεια και Υγιεινή»

45. Σ . Κάτσικας , "Ο ΔΕΚΑΛΟΓΟΣ ...για θέματα Ασφάλειας Πληροφοριακών Συστημάτων και Προστασίας Προσωπικών Δεδομένων στο Ηλεκτρονικό Επιχειρείν " Δικτυακός τόπος : http://www.hcg.gr/node/65

46. ILO (1991). Prevention of major industrial accidents, ILO code of practice.

47. ILO (2005). Safety and health in ports. ILO code of practice, International Labour Office Geneva 3. ILO-IMO (2004). Security in ports. ILO and IMO code of practice. Geneva, International Labour Office/London, International Maritime Organization.

48. ILO-OSH 2001 (2001). Guidelines on Occupational Safety and Health Management Systems,

49. ΥΕΝ (2006). Νομοθετήματα για την ασφάλεια και υγιεινή της εργασίας, 13/02/2006, στο http://egov.yen.gr/media/28248/par_ygieinis.pdf.

50. Γουλιέλμος, Α – Σαμπράκος, Ε. (2002). Ακτοπλοΐα και Ναυτιλία μικρών αποστάσεων, εκδ. Σταμούλη.

51. Μυλωνόπουλος, Δ. (2004). Ναυτιλία. Έννοιες-Τομείς-Δομές, εκδ. Σταμούλης.

52. Παντελόγλου, Γρ. (2004). «Η ενηλικίωση της επαγγελματικής κατάρτισης στη Γαλλία. Νέοι μηχανισμοί αναγνώρισης των γνώσεων των ικανοτήτων, των δεξιοτήτων και των κεκτημένων της πείρας». Επιθεώρηση Εργασιακών Σχέσεων, τεύχος 34, σελ. 37-59.

53. Παρδάλη, Α. (2001). Η Λιμενική Βιομηχανία, εκδ. Σταμούλη.

54. ΥΕΝ/ΕΥΜΑΠΛ (2003). εγκύκλιος με αρ. 09/03 της 14/08/2003 «Υλοποίηση νέων απαιτήσεων Κεφ. XI-2 της Δ.Σ. SOLAS 74 και του ISPS Code για τις Λιμενικές εγκαταστάσεις»

55. Ν. 1568/85 «Υγιεινή και ασφάλεια των εργαζομένων» (ΦΕΚ 117/Α/18-10-85)

56. Ν. 2874/2000 «Προώθηση της απασχόλησης και άλλες διατάξεις» (ΦΕΚ 286/Α/29-12-00) λειτουργούν είτε συμπληρωματικά είτε τροποποιητικά ως προς αυτό (ΥΕΝ, 2006).

57. Π.Δ. 159/1999 «Τροποποίηση του Π.Δ. 17/96 και του Π.Δ. 70α/88 "Προστασία των εργαζομένων που εκτίθενται σε αμίαντο κατά την εργασία"» (ΦΕΚ 157/Α/3-8-1999)

58. Π.Δ. 17/96 «Μέτρα για τη βελτίωση της ασφάλειας και της υγείας των εργαζομένων κατά την εργασία σε συμμόρφωση με τις οδηγίες 89/391/ΕΟΚ και 91/383/ΕΟΚ». (ΦΕΚ 11/Α/18-1-96)

59. Π.Δ. 294/1988 «Ελάχιστος χρόνος απασχόλησης τεχνικού ασφαλείας και γιατρού εργασίας, επίπεδο γνώσεως και ειδικότητα τεχνικού ασφάλειας για τις επιχειρήσεις, εκμεταλλεύσεις και εργασίες του άρθρου 1 παρ. 1 του ν. 1568/1985 "Υγιεινή και ασφάλεια των εργαζομένων"» (ΦΕΚ 138/Α/21-6-1988).

60. Χαλβατζή, Ε. Ι. (2014). Συγκριτική μελέτη ανάλυσης επικινδυνότητας (Master's thesis). Πανεπιστήμο Πειριαώς