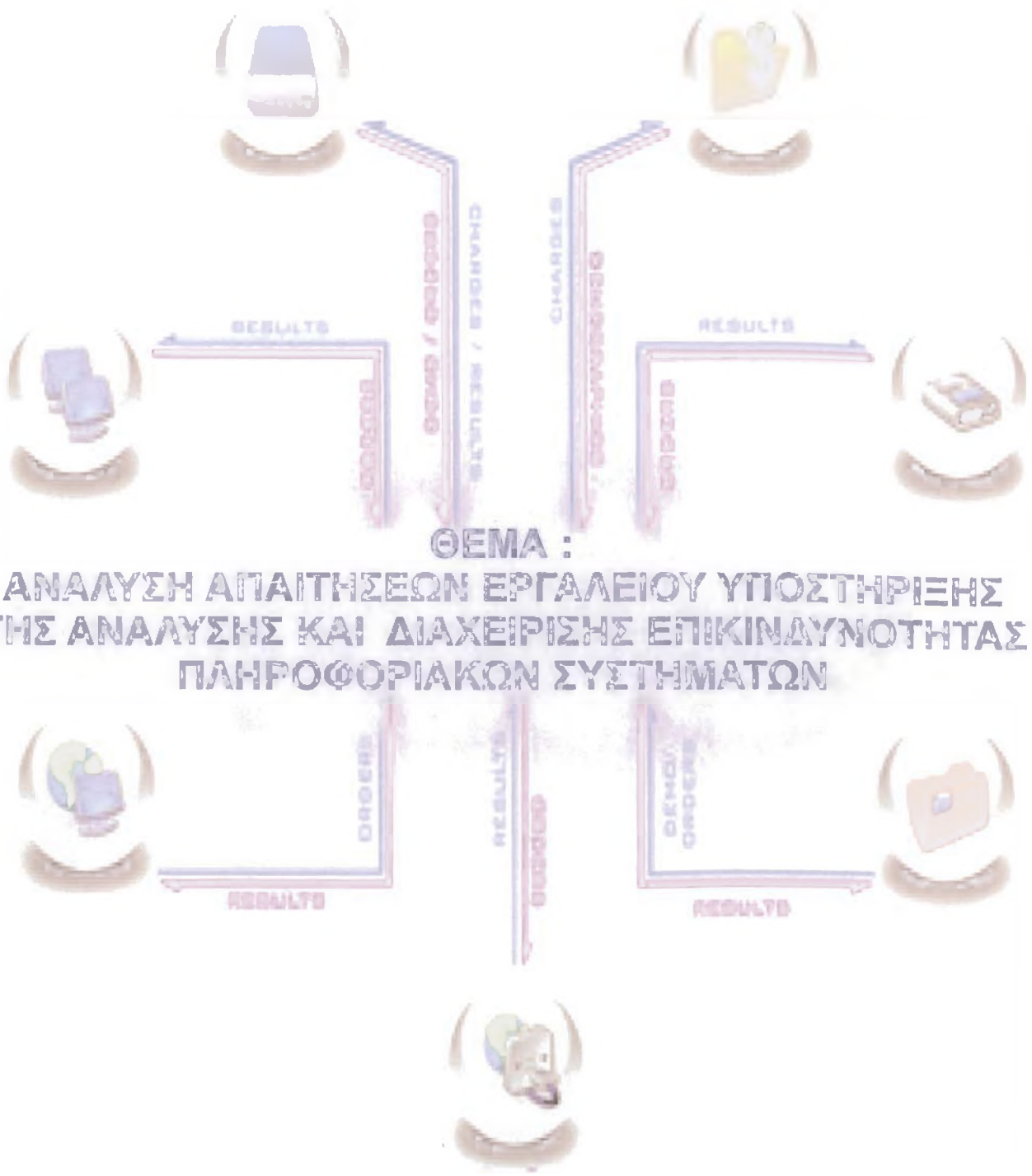
Α.Τ.Ε.Ι. ΜΕΣΟΛΟΓΓΙΟΥ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗ
ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ



ΘΕΜΑ :
ΑΝΑΛΥΣΗ ΑΠΑΙΤΗΣΕΩΝ ΕΡΓΑΛΕΙΟΥ ΥΠΟΣΤΗΡΙΞΗΣ ΤΗΣ ΑΝΑΛΥΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : Χ. ΦΕΙΔΑΣ

ΦΟΙΤΗΤΗΣ : ΚΑΣΚΟΥΤΑ ΔΗΜΗΤΡΑ
ΑΜ : 8632

ΜΕΣΟΛΟΓΓΙ 2006

ΠΡΟΛΟΓΟΣ ΚΑΙ ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα εργασία έχει σαν αντικείμενο την «Ανάλυση των Απαιτήσεων για την Ανάπτυξη ενός Εργαλείου Υποστήριξης της Ανάλυσης και της Διαχείρισης της Επικινδυνότητας Πληροφοριακών Συστημάτων» και υπεύθυνος καθηγητής είναι ο κ. Φειδάς.

Η εργασία αυτή δεν θα μπορούσε να αναπτυχθεί χωρίς την συμμετοχή του κ. Φείδα, ο οποίος ανταποκρίθηκε με προθυμία και διέθεσε τον πολύτιμο χρόνο του χωρίς δεύτερη σκέψη.

Ευχαριστώ επίσης τον κ. Μανωλόπουλο , αναλυτή συστημάτων πληροφορικής εμπορίου και βιομηχανίας, ο οποίος με βοήθησε σημαντικά στην εκπόνηση αυτής της εργασίας, με τις πολύτιμες γνώσεις του πάνω στο χώρο των Πληροφοριακών Συστημάτων.

Ένα μεγάλο ευχαριστώ σε όλους εκείνους τους ανθρώπους που ήταν δίπλα μου κατά την διάρκεια των σποδών μου επηρεάζοντας με είτε θετικά είτε αρνητικά. Ο καθένας από αυτούς συνέβαλε με διαφορετικό τρόπο ώστε η εργασία αυτή να παραδοθεί.

Ξεχωριστά από όλους θα ήθελα να ευχαριστήσω την οικογένεια μου. Ήταν πάντοτε δίπλα μου και με υποστήριζε σε όλη τη διάρκεια των σπουδών μου και της ζωής μου γενικότερα. Χωρίς τη βοήθεια της η εργασία αυτή δεν θα ολοκληρωνόταν.

Σε όλους τους ανθρώπους που νοιάζομαι και αγαπώ..

Δήμητρα Κασκούτα

Σεπτέμβριος 2006

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Με την ραγδαία ανάπτυξη και διείσδυση της πληροφορικής σε όλους τους τομείς της κοινωνικοοικονομικής δραστηριότητας, η εξάρτηση των εταιρειών και των οργανισμών από τα Πληροφοριακά τους Συστήματα εντείνεται διαρκώς, με αποτέλεσμα η απώλεια των υπηρεσιών Πληροφορικής σαν συνέπεια κάποιας καταστροφής να είναι ένα πολύ μεγάλο πρόβλημα με άμεσες επιπτώσεις στη δυνατότητα συνέχισης της λειτουργίας της επιχείρησης ή του οργανισμού.

Έτσι λοιπόν είναι καθημερινό φαινόμενο οι παραβιάσεις ασφαλείας. Ιστοσελίδες παραβιάζονται, προσωπικά δεδομένα υποκλέπτονται, συστήματα τίθενται εκτός λειτουργίας προκαλώντας αναστάτωση και ζημιές. Τα αποτελέσματα ερευνών σχετικών με την ασφάλεια είναι ανησυχητικά.

Επίσης μέσα από την Παγκόσμια Έρευνα Ασφάλειας Πληροφοριών που πραγματοποιείται κάθε χρόνο με την συμμετοχή περισσότερων από 35 χωρών και 4825 επιχειρήσεων προκύπτει το συμπέρασμα ότι υπάρχει αύξηση στα συμπτώματα παραβιάσεων /παρακάμψεων των μέτρων ασφαλείας σε συνδυασμό με την εμφάνιση νέων πληροφοριακών κινδύνων / απειλών. Παρόλο που το 83% των ερωτηθέντων επιχειρήσεων θεωρεί την ασφάλεια πληροφοριών και κατ' επέκταση των Πληροφοριακών Συστημάτων, σημαντική , το

Έτσι κυριότερη αιτία της μη επαρκούς αντιμετώπισης των ζητημάτων ασφαλείας θεωρείται η **μη επαρκής αντίληψη κατανόηση του προβλήματος από πλευράς εργαζομένων**. Δευτερεύουσες αιτίες, που προέκυψαν από την έρευνα, αποτελούν **η έλλειψη σχετικής υποδομής εργαλείων αποτροπής** και η **μη επαρκής αντίληψη/ κατανόηση του προβλήματος** από πλευράς διοίκησης.

Για την προστασία των υπηρεσιών Πληροφορικής από τέτοιες απώλειες θα πρέπει οι εταιρείες να υιοθετήσουν μεθόδους ανάλυσης και διαχείρισης της επικινδυνότητας των Πληροφοριακών Συστημάτων.

Σήμερα είναι διαθέσιμες περισσότερες από 100 μέθοδοι ανάλυσης και διαχείρισης της επικινδυνότητας Πληροφοριακών Συστημάτων, πολλές από τις οποίες υποστηρίζονται από εργαλεία. Μια σειρά όμως επιχειρημάτων δίνουν μια εικόνα για την έντονη ανάγκη ανάπτυξης ενός εργαλείου που να υποστηρίζει την ανάλυση και τη διαχείριση της επικινδυνότητας των Πληροφοριακών Συστημάτων. Ορισμένες από αυτές είναι:

- Δεν υπάρχει διαθέσιμο ένα εργαλείο το οποίο να είναι προσαρμοσμένο στα ιδιαίτερα χαρακτηριστικά της ελληνικής πραγματικότητας και να αντιμετωπίζει τα ξεχωριστά γνωρίσματα της κουλτούρα των Ελλήνων.

- Δεν υπάρχει ένα κοινά αποδεκτό σύνολο κριτηρίων αξιολόγησης για τις μεθόδους.

- Δεν υπάρχει διαθέσιμος πλήρης κατάλογος με τα ιδιαίτερα χαρακτηριστικά όλων των μεθόδων, ενώ κάποιες από αυτές δεν διατίθενται στην ελεύθερη αγορά γεγονός που καθιστά την αξιολόγηση τους εξαιρετικά δύσκολη.

- Πέρα από αυτή την διαπίστωση κρίνεται πως έχει αποκρυσταλλωθεί από ένα σύνολο έμπειρων, στη διαχείριση της επικινδυνότητας, χρηστών ένα κρίσιμο σύνολο χαρακτηριστικών τα οποία θα ήταν δυνατό να αποτελέσουν τη βάση για την ανάπτυξη μιας γενικής εφαρμογής – σε αντιδιαστολή με ένα προσανατολισμένο σε ένα συγκεκριμένο επιχειρηματικό κλάδο ή σε ένα συγκεκριμένο λειτουργικό σύστημα- ευέλικτου και εύχρηστου εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας Π.Σ. που θα στηρίζεται σε μια αποτελεσματική και αποδοτική μέθοδο ανάλυσης και διαχείρισης της επικινδυνότητας.

Στα πλαίσια μιας στρατηγικής για την αντιμετώπιση της ανάπτυξης του εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας Πληροφοριακών Συστημάτων θα πρέπει να χρησιμοποιηθεί μια μεθοδολογία που να αντιμετωπίζει την ανάπτυξη πακέτων λογισμικού. Για το λόγο αυτό με βάση μια σειρά συλλογισμών κρίνεται πως **η δομημένη προσέγγιση** ταιριάζει πιο αποτελεσματικά στο συγκεκριμένο έργο, καθώς αντιμετωπίζει μια σειρά από ιδιαιτερότητες που παρουσιάζονται για την ολοκλήρωση του.

Σχετικά με τον κύκλο ζωής του συγκεκριμένου πακέτου – εργαλείου θα πρέπει να εξεταστούν μια σειρά από προτεινόμενους από την τεχνολογία λογισμικού κύκλους ζωής και να επιλεγεί αυτός που κρίνεται ότι ταιριάζει στη συγκεκριμένη ανάπτυξη, ο οποίος προκύπτει ότι είναι ο παραδοσιακός κύκλος ζωής λογισμικού. Προχωρώντας πιο ειδικά προσδιορίζεται και το συγκεκριμένο σημείο του κύκλου ζωής στο οποίο αφορά η εργασία που είναι η φάση της διερευνητικής μελέτης στα πλαίσια της ανάλυσης των απαιτήσεων λογισμικού.

Ορισμένα από τα σημεία που εξετάζονται αφορούν το είδος χρήσης του εργαλείου, τις λεπτομέρειες της ίδιας της μεθόδου ανάλυση και διαχείρισης της επικινδυνότητας, το κόστος, την ευκολία χρήσης του, τους χρόνους διάρκειας της διαδικασίας και επανάληψης της διαδικασίας ανάλυσης και διαχείρισης της επικινδυνότητας, τα χαρακτηριστικά των ερωτηματολογίων και εκθέσεων που θα παράγει το εργαλείο, το είδος της εκπαίδευσης που θα απαιτείται για αυτό, το πώς θα γίνεται το ταίριασμα του σε μια επιχείρηση ή έναν οργανισμό, ειδικές απαιτήσεις υλικού και λογισμικού, απαιτήσεις ασφαλείας για το εργαλείο, διάφορα χαρακτηριστικά των αντίμετρων που θα περιλαμβάνει το εργαλείο, στοιχεία σχετικά με την κάλυψη περιουσιακών αγαθών και την κάλυψη απειλών και αδυναμιών, τις δυνατότητες ενοποίησης με άλλα εργαλεία και άλλα.

Τελικά προσδιορίστηκαν απαιτήσεις που αφορούν την βασική λειτουργία του εργαλείου μέσα από πέντε γενικές φάσεις – βήματα: **Φάση 1η** :Ορισμός του προβλήματος, Ορισμός του συστήματος, Προσδιορισμός των ορίων του συστήματος, Διαγραμματικές τεχνικές ανάλυσης και μοντελοποίησης, **Φάση 2η**: Ανάλυση της επικινδυνότητας , Αποτίμηση των περιουσιακών αγαθών του οργανισμού, Προσδιορισμός και αποτίμηση των απειλών και των αδυναμιών, υπολογισμός της συνολικής επικινδυνότητας, **Φάση 3η** : Υλοποίηση, **Φάση 4η**: Παρακολούθηση και **Φάση 5η**: Αναθεώρηση.

Άλλες γενικές απαιτήσεις είναι η εφαρμογή σε κάθε στάδιο του κύκλου ζωής της ανάπτυξης λογισμικού, προσαρμογή στην ελληνική γλώσσα/ δεδομένα/ κουλτούρα, εφαρμογή σε μεγάλου μεγέθους οργανισμούς, εφαρμογή σε διάφορους επιχειρηματικούς κλάδους ή τύπους επιχειρήσεων και οργανισμών, ευθυγράμμιση ως προς την ελληνική και ευρωπαϊκή νομοθεσία, αλληλεξαρτήσεις των διαφορετικών συστημάτων, ύπαρξη διαφόρων επιπέδων λεπτομέρειας μιας ανάλυσης, εφαρμογή της μεθόδου γρήγορα και αποτελεσματικά, δυνατότητα ορισμού ενός αποδεκτού επιπέδου επικινδυνότητας, υπόδειξη του που βρίσκονται τα σημαντικότερα προβλήματα, ενσωμάτωση της επιχειρηματικής επικινδυνότητας και ενσωμάτωση γενικών απειλών και αδυναμιών.

Σχετικά με τα αντίμετρα απαιτείται η πρόταση ειδικών και λεπτομερών αντίμετρων, οικονομικώς αποδοτικών αντίμετρων, ισορροπημένου συνόλου από αντίμετρα, μέτρων που να βοηθούν στην αποδοχή των υπολοίπων αντίμετρων. Ακόμα απαιτείται από τη μέθοδο να λαμβάνει υπόψη τις πιθανές αρνητικές επιπτώσεις από την υιοθέτηση αντίμετρων, να κάνει σύνδεση αντίμετρων με δηλώσεις πολιτικών ασφαλείας, να υπάρχει η δυνατότητα δήλωσης του τύπου σχέσης ανάμεσα σε δηλώσεις πολιτικής ασφαλείας.

Άλλες γενικές απαιτήσεις αφορούν την πρόταση από το εργαλείο δυνητικού χρόνου επανάληψης της Ανάλυσης της Επικινδυνότητας, δυνατότητα πειραματισμού με διαφορετικά σενάρια, δυνατότητα ιχνηλάτησης, δυνατότητα επαλήθευσης των αποτελεσμάτων μέσα από την επανάληψη, διαχείριση της διαδικασίας ανάλυσης και διαχείρισης της επικινδυνότητας, δυνατότητα αλλαγής των δεδομένων, ευκολία προσαρμογής στις αλλαγές της τεχνολογίας, φιλικότητα προς τον χρήστη και ευχρηστία, εξαγωγή των δεδομένων του εργαλείου.

Σε σχέση με τα ερωτηματολόγια και τις εκθέσεις που θα παράγει το εργαλείο απαιτούνται εκθέσεις για τη διοίκηση και εκθέσεις τεχνικές , δυνατότητα φιλτραρίσματος στις εκθέσεις, δυνατότητα επεξεργασίας των εκθέσεων, ερωτηματολόγια με μορφή φόρμας, προσεκτική διατύπωση των ερωτήσεων των ερωτηματολογίων, παρουσίαση συνοδευτικών στις ερωτήσεις αναφορών πληροφόρηση, ομαδοποίηση των ερωτήσεων με βάση την κατηγορία χρηστών συστήματος, δυναμικό «ξεδίπλωμα» των ερωτήσεων και ερωτηματολόγιο με ένα ελάχιστο σύνολο ερωτήσεων.

Όσον αφορά τις απαιτήσεις από το υλικό και το λογισμικό, το βασικό λειτουργικό σύστημα είναι τα Windows, εναλλακτικό λειτουργικό σύστημα είναι το UNIX και θα μπορεί να λειτουργεί το εργαλείο ακόμα και στο περιβάλλον ενός φορητού προσωπικού υπολογιστή.

Σχετικά με τις απαιτήσεις ασφαλείας αναφέρεται ότι τα δεδομένα θα πρέπει να προστατεύονται, να γίνεται έλεγχος της διαδικασίας αλλαγών στη βάση δεδομένων και να υπάρχει σύστημα ελέγχου προσπέλασης.

Για όλους αυτούς τους λόγους η παρούσα εργασία έχει ως στόχο την πραγματοποίηση μιας διερευνητικής μελέτης στα πλαίσια της ανάλυσης απαιτήσεων για την

Στο **1° κεφάλαιο** παρουσιάζεται μια σειρά από ορισμούς κάποιων εννοιών οι οποίες χρησιμοποιούνται μέσα στην εργασία.

Στο **2° Κεφάλαιο** αναλύεται η φιλοσοφία που το εργαλείο ακολουθεί. Πρώτα δίνεται ένας ορισμός για το εργαλείο αυτό και τα συμπεράσματα που απορρέουν του ορισμού αυτού. Έτσι οριοθετείται ο χώρος και το πεδίο δράσης αυτού, Κατόπιν επιλέγεται η μεθοδολογία που το εργαλείο ακολουθεί αφού προηγηθεί μια κριτική των υπαρχόντων μεθοδολογιών. Η μεθοδολογία που το εργαλείο θα υλοποιεί αναλύεται και παρουσιάζονται τα σημεία αυτής που σχετίζονται απόλυτα με το συγκεκριμένο εργαλείο. Η μεθοδολογία που επιλέχθηκε αποτελεί συνδυασμό τριών προσεγγίσεων:

a) Της Μεθοδολογίας Ευμετάβλητων Συστημάτων (SSM) που ακολουθεί το Paradigm II,
b) Της μοντελοποίησης οργανισμών και επιχειρήσεων (business modeling) και
c) Της ανάλυσης της επικινδυνότητας που ακολουθεί το Paradigm I.

Στο **3° Κεφάλαιο** παρουσιάζονται κάποιες σκέψεις σχετικά με την ανάλυση και την διαχείριση της επικινδυνότητας όπως τις διάφορες δυσχέρειες και τα πλεονεκτήματα που παρουσιάζει η διαχείριση της επικινδυνότητας , γενικά για τα εργαλεία που υποστηρίζουν την ανάλυση και τη διαχείριση της επικινδυνότητας, τα πλεονεκτήματα και τους περιορισμούς που παρουσιάζουν καθώς και μια κριτική γύρω από αυτά.

Στο **4° Κεφάλαιο** γίνεται περιγραφή της στρατηγικής αντιμετώπισης του θέματος, όσο αφορά τις υπάρχουσες προσεγγίσεις για την ανάπτυξη πακέτων λογισμικού, όπως η δομημένη προσέγγιση, η αντικειμενοστρεφής προσέγγιση και η τεχνικής κατασκευής προτύπου και παρατίθενται συμπεράσματα που προκύπτουν σχετικά με αυτές. Στη συνέχεια περιγράφεται ο κύκλος ζωής του εργαλείου που θα αναπτυχθεί.

Στο **5° Κεφάλαιο** πραγματοποιείται η ανάλυση των απαιτήσεων. Για την υλοποίηση της χρησιμοποιήθηκε το μοντέλου του κύκλου ζωής του λογισμικού του IEEE. Η επιλογή αυτού του μοντέλου έχει να κάνει με το γεγονός ότι χρησιμοποιήθηκε ευρέως και αντιπροσωπεύει τη δομημένη προσέγγιση. Όπως έχει προαναφερθεί το εργαλείο αυτό πρόκειται να παραχθεί σε διάφορα στάδια , έτσι η πρακτική του διαίρει και βασίλευε με τον τεμαχισμό των εργασιών που αποτελεί κύριο χαρακτηριστικό της δομημένης προσέγγισης μπορεί μέσω του μοντέλου αυτού να εφαρμοστεί πλήρως. Η ανάλυση γίνεται με χρήση ΔΡΔ , λεξικού δεδομένων και ακολουθώντας τις οδηγίες για τη σύνταξη ενός ΕΠΑΛ. Μέσα στο έγγραφο αυτό περιγράφονται οι λειτουργικές απαιτήσεις, οι απαιτήσεις εξωτερικών διεπαφών , οι απαιτήσεις επίδοσης και οι περιορισμοί σχεδίασης.

Το **6° Κεφάλαιο** αποτελεί το πρώτο βήμα για την υλοποίηση της σχεδίασης. Αυτή θα πραγματοποιηθεί ακολουθώντας της οδηγίες για τη σύνταξη ενός ΕΠΑΛ. Στην παρούσα εργασία περιγράφεται μόνο η αποσύνθεση του συστήματος Λογισμικού, η οποία αποτυπώνει τη διαίρεση του συστήματος Λογισμικού σε

οντότητες σχεδίου. Για την αναπαράσταση χρησιμοποιούνται Διαγράμματα Δομής που παρουσιάζουν την ιεραρχία των μονάδων του συστήματος.

Στο **7ο Κεφάλαιο** παρουσιάζονται τα κριτήρια επικύρωσης ή αποδοχής του τελικού προϊόντος, Στο σημείο αυτό προσδιορίζονται τα κριτήρια που αφορούν τον έλεγχο του λογισμικού (ενοτήτων, συνένωσης, αποδοχής) καθώς και αυτά που αφορούν την τεκμηρίωση του, με αναφορές και στα διάφορα υπάρχοντα πρότυπα τα οποία είναι δυνατό να χρησιμοποιηθούν.

Στο **8ο Κεφάλαιο** γίνεται μια εκτίμηση του χρονοδιαγράμματος των εργασιών που ακολουθούν και θίγονται κάποια θέματα που αφορούν την διαχείριση του έργου.

Στο **9ο Κεφάλαιο** παρουσιάζονται λύσεις χρηματοδότησης για την δημιουργία του εργαλείο αυτού.

Το **10ο Κεφάλαιο** αποτελεί το πρώτο βήμα για την υλοποίηση της σχεδίασης. Στην παρούσα εργασία περιγράφεται μόνο η αποσύνθεση του Συστήματος Λογισμικού, η οποί αποτυπώνει τη διαίρεση του Συστήματος Λογισμικού σε οντότητες σχεδίου. Για την αναπαράσταση χρησιμοποιούνται διαγράμματα Δομής που παρουσιάζουν την ιεραρχία των μονάδων του συστήματος.

ΚΕΦΑΛΑΙΟ 1

ΟΡΙΣΜΟΙ ΚΑΙ ΚΥΡΙΕΣ ΕΝΝΟΙΕΣ

1.1. Πληροφοριακό Σύστημα

Είναι κοινός τόπος ότι η τεχνολογία των υπολογιστών είναι σήμερα καθοριστική για τη σωστή και αποδοτική διαχείριση κάθε μορφής οργανισμού ή επιχείρησης. Οι εφαρμογές των υπολογιστών και της πληροφορικής γενικότερα καλύπτουν κάθε τομέα της ανθρώπινης δραστηριότητας.

Η ύπαρξη και μόνο, όμως, ενός υπολογιστή όσο ισχυρός και αν είναι, δεν αρκεί για να λύσει τα προβλήματα μιας επιχείρησης. Χρειάζεται να δημιουργηθούν τα κατάλληλα συστήματα που θα παραλαμβάνουν κάθε φορά τα δεδομένα και θα τα μετατρέπουν σε πληροφορίες με βάση συγκεκριμένες προδιαγραφές. Στην περίπτωση αυτή αναφερόμαστε σε πληροφοριακά συστήματα (information systems) που δημιουργούνται από ειδικούς επαγγελματίες της πληροφορικής (αναλυτές συστημάτων) με βάση τις απαιτήσεις που καθορίζουν οι χρήστες (users).

Ένα πληροφοριακό σύστημα αποτελεί κάτι μη απτό. Είναι ένα ιδεατό κατασκεύασμα το οποίο δημιουργείται για να αντιπροσωπεύει μια φυσική οντότητα η οποία υπάρχει μέσα σε μια επιχείρηση ή σε ένα οργανισμό. Η οντότητα αυτή αποτελεί βασικότατο δομικό συστατικό της επιχείρησης ή του οργανισμού και επηρεάζει σημαντικά τη λειτουργία τους.

Ένα πληροφοριακό σύστημα ακολουθεί σχεδόν πάντα μια συγκεκριμένη πορεία:δημιουργείται, αναπτύσσεται, εξελίσσεται και τελικά αποσύρεται. Η ύπαρξη του οριοθετείται τη χρονική στιγμή που η επιχείρηση ή ο οργανισμός παίρνει την απόφαση για τη δημιουργία του. Στη συνέχεια ακολουθεί μια περίοδος κατά την οποία προσδιορίζονται οι βασικές απαιτήσεις των λειτουργιών του και σχεδιάζονται οι λειτουργίες που ικανοποιούν τις απαιτήσεις αυτές. Από εκεί και πέρα ξεκινάει μια μεγάλη χρονική περίοδος κατά την οποία πραγματοποιείται η ανάπτυξη του και η διαρκής εξέλιξη του ώστε να είναι σε θέση να ικανοποιεί διαρκώς τις ανάγκες της επιχείρησης ή του οργανισμού στον οποίο ανήκει. Φυσικά κάποια στιγμή έρχεται η ώρα που πρέπει να αποσυρθεί όταν η επιχείρηση ότι είναι πια ξεπερασμένο, αναποτελεσματικό και μη αποδοτικό. Η πορεία ενός πληροφοριακού συστήματος από τη στιγμή του καθορισμού του προβλήματος που πρέπει να επιλύσει μέχρι τη λειτουργία του, τη συντήρηση του και τέλος την απόσυρση του είναι **γνωστός ως Κύκλος Ζωής του Πληροφοριακού Συστήματος.**

Ένα πληροφοριακό σύστημα αποτελείται από τρεις αλληλοεξαρτώμενες παραμέτρους:

- **Τεχνική (Υλικό και Λογισμικό)**
- **Οργανωτική (Διαδικασίες)**
- **Κοινωνική (Ανθρώπινες Σχέσεις)**

Ο Ρόλος ενός Πληροφοριακού Συστήματος

Σε μια επιχείρηση ένα Πληροφοριακό Σύστημα αποτελεί το συστατικό που συνδέει το φυσικό σύστημα παραγωγής με το σύστημα λήψης αποφάσεων. Βασική λειτουργία του είναι ο μετασχηματισμός των δεδομένων που υπάρχουν στο φυσικό σύστημα παραγωγής σε πληροφορίες (δεδομένα) που απαιτούν οι δραστηριότητες του συστήματος λήψης αποφάσεων. Όμως και αντίστροφα διαβιβάζει δεδομένα που παράγει το σύστημα διοίκησης σε κατάλληλες πληροφορίες (δεδομένα) για το φυσικό σύστημα παραγωγής.

Εκτός από τις παραπάνω βασικές λειτουργίες ένα πληροφοριακό σύστημα πρέπει να προσφέρει και επιπλέον δυνατότητες για:

- ⇨ Συνεχή εξέλιξη για την ικανοποίηση νέων ή αυξανόμενων αναγκών
- ⇨ Βοήθεια στις διαδικασίες ελέγχου και διοίκησης της επιχείρησης ή του οργανισμού
- ⇨ Βοήθεια στον προγραμματισμό και τη δημιουργία της στρατηγικής ανάπτυξης της επιχείρησης ή του οργανισμού
- ⇨ Συνεισφορά στη δημιουργία αλλαγών ώστε η επιχείρηση να είναι σε θέση να προσαρμόζεται συνεχώς στο περιβάλλον του – ένα ολοκληρωμένο πληροφοριακό σύστημα πρέπει να είναι ευέλικτο και προσαρμόσιμο ώστε να ανταποκρίνεται στις αλλαγές και τις διαφορετικές απαιτήσεις διαφόρων ομάδων χρηστών.
- ⇨ Εκπαίδευση και μάθηση.

Ολοκληρωμένος Ορισμός του Πληροφοριακού Συστήματος

Ένα Πληροφοριακό Σύστημα αποτελεί ένα οργανωμένο σύνολο που αποτελείται από τα εξής πέντε αλληλοεπιδρώντα στοιχεία:

- **Άνθρωποι**
- **Διαδικασίες**
- **Δεδομένα**
- **Λογισμικό**
- **Υλικός Εξοπλισμός**

Επομένως ένα πληροφοριακό σύστημα είναι σύστημα το οποίο είναι σε θέση να:

- Προσδιορίζει κατά τρόπο αποδοτικό και αποτελεσματικό ,τις πραγματικές ανάγκες των ανθρώπων που το χρησιμοποιούν και
- Να επεξεργάζεται όλες τις απαραίτητες πληροφορίες ώστε να ικανοποιούνται οι ανάγκες αυτές.

Πιο συγκεκριμένα ένα Πληροφοριακό Σύστημα ως σύστημα επεξεργασίας πληροφοριών, φροντίζει για τη συνεχή ικανοποίηση των μεταβαλλόμενων και αυξανόμενων αναγκών των χρηστών. Αυτό επιτυγχάνεται κυρίως με:

- Τον όσο το δυνατόν πιο αποτελεσματικό τρόπο ανάκτησης, αποθήκευσης, επεξεργασίας, παρουσίασης και διάδοσης των πληροφοριών.
- Την παροχή των απαραίτητων μέσων και του κατάλληλου περιβάλλοντος μάθησης στους εμπλεκόμενους χρήστες ώστε να βελτιωθεί η αποτελεσματικότητα της διαδικασίας λήψης αποφάσεων.
- Την υποστήριξη των διαδικασιών λειτουργίας, ελέγχου και στρατηγικού σχεδιασμού της επιχείρησης ή του οργανισμού.

Παραδοσιακός Κύκλος Ζωής ενός Πληροφοριακού Συστήματος

Οι περισσότεροι ερευνητές αποδέχονται ότι ο παραδοσιακός κύκλος ζωής ενός Π.Σ. αποτελείται από τις ακόλουθες επτά φάσεις:

1. **Διερευνητική μελέτη**
2. **Μελέτη Σκοπιμότητας**
3. **Ανάλυση απαιτήσεων**
4. **Σχεδιασμός του Συστήματος**
5. **Υλοποίηση – Κωδικοποίηση**
6. **Εγκατάσταση**
7. **Λειτουργία – Συντήρηση**

Οι φάσεις αυτές πρέπει να βρίσκονται διατεταγμένες σειριακά, δηλαδή η ολοκλήρωση κάθε φάσης να οδηγεί πάντα στην αμέσως επόμενη της. Αυτό προϋποθέτει ότι τα αποτελέσματα κάθε φάσης θα οδηγούν κατά τρόπο αναμφισβήτητο στην επόμενη, δηλαδή το προϊόν που παράγει κάθε φάση θα γίνεται δεκτό όπως είναι χωρίς να υπάρχει η περίπτωση αλλαγής του αργότερα. Μόνο σε αυτή την περίπτωση είναι δυνατόν να παγιωθεί η σειρά εκτέλεσης των διαφόρων φάσεων.

1.2. Επικινδυνότητα και Συναφείς έννοιες

Η έννοια της επικινδυνότητας είναι στενά συνδεδεμένη με τις ενέργειες που πραγματοποιούμε. Η Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (CCTA) ορίζει ως επικινδυνότητα την πιθανότητα να συμβούν ανεπιθύμητα επακόλουθα – συνέπειες. Ο βαθμός της επικινδυνότητας μπορεί να είναι τόσο μεγάλος ώστε να παρεμποδίζεται η επίτευξη διάφορων στόχων. Στα πλαίσια μιας επιχείρησης ή ενός οργανισμού θα πρέπει να υπάρχει η κατάλληλη προετοιμασία ώστε να είναι δυνατό να αντιμετωπιστούν μια σειρά πιθανών καταστάσεων που θα μπορούσαν να προκαλέσουν ζημιά στον οργανισμό η οποία μπορεί να αποτιμάται χρηματικά ή όχι (φήμη). Στην προσπάθεια να μειωθεί η υπάρχουσα επικινδυνότητα θα πρέπει να:

- Αναγνωρισθεί η επικινδυνότητα
- Να είναι δυνατή η αναγνώριση και αποτίμηση των κινδύνων που απειλούν τις δραστηριότητες.
- Να γίνει διαχείριση των κινδύνων ώστε να είναι δυνατή η επίτευξη των στόχων.

Καθώς ένα μεγάλο μέρος των λειτουργιών ενός οργανισμού στηρίζονται στη χρήση πληροφοριακών συστημάτων, η επιτυχία του οργανισμού είναι δυνατό να εξαρτάται από την επιτυχημένη διαχείριση της επικινδυνότητας των Πληροφοριακών Συστημάτων από ομάδες εμπειρογνωμόνων σε θέματα ασφαλείας Πληροφοριακών Συστημάτων. Έτσι η δημιουργία ενός ασφαλούς Πληροφοριακού Συστήματος προϋποθέτει την μείωση της επικινδυνότητας αυτού.

Η ανάλυση της επικινδυνότητας (risk analysis) προερχόμενη από το χώρο των οικονομικών και διοικητικών επιστημών αποτελεί μια συστηματική διαδικασία κατά την οποία γίνεται προσδιορισμός και εκτίμηση της συνολικής επικινδυνότητας ενός Πληροφοριακού Συστήματος δηλαδή, προσδιορίζονται τα αγαθά του συστήματος , οι αδυναμίες, και οι απειλές που αυτά αντιμετωπίζουν καθώς και οι επιπτώσεις που έχουν οι τελευταίες στα αγαθά. Για κάθε μια απειλή αναφέρονται τα πιθανά μέσα προστασίας ή αντίμετρα μαζί με τα κόστη αυτών, ενώ η τελευταία φάση περιλαμβάνει μια ανάλυση κόστους – οφέλους (cost – benefit analysis).

1.3. Διαχείριση της Επικινδυνότητας

Ένα οποιοδήποτε πληροφοριακό σύστημα αποτελείται από υλικό, λογικό, εξοπλισμό επικοινωνιών, εξοπλισμό περιβαλλοντικού ελέγχου και υλικό τεκμηρίωσης. Επιπλέον διαχειρίζεται, δηλαδή επεξεργάζεται, μεταδίδει και αποθηκεύει πληροφορίες. Όλα τα παραπάνω αποτελούν τα περιουσιακά στοιχεία (assets) του συστήματος , τα οποία πρέπει να προστατευθούν.

Κάθε σύστημα όσο καλά και αν είναι σχεδιασμένο, έχει αναπόφευκτες αδυναμίες. Εξάλλου το σύστημα υπόκειται σε διάφορες απειλές (threats). Μία απειλή εκμεταλλεύεται κάποια ή κάποιες αδυναμίες του συστήματος και οδηγεί σε ένα ή περισσότερα ανεπιθύμητα γεγονότα (impacts) που με τη σειρά τους επιφέρουν συνέπειες (consequences) στο σύστημα και κατ' επέκταση στον οργανισμό ή την επιχείρηση που το χρησιμοποιεί.

Ο στόχος της πολιτικής ασφαλείας του οργανισμού ή της επιχείρησης είναι να ελαχιστοποιεί την πιθανότητα εμφάνισης ανεπιθύμητων γεγονότων (προφανώς μειώνοντας είτε τις αδυναμίες του συστήματος είτε την πιθανότητα επιτυχούς εκμετάλλευσης μιας αδυναμίες από κάποια απειλή, αφού δεν είναι δυνατόν να υπάρξει έλεγχος επί των απειλών) ή τουλάχιστον να ελαχιστοποιήσει τις συνέπειες των ανεπιθύμητων γεγονότων. Για να γίνει αυτό απαιτείται η επιλογή και η υλοποίηση αποτελεσματικών αντιμέτρων.

Η διαχείριση κινδύνων είναι η διαδικασία που:

- Αναπτύσσει ένα αφηρημένο μοντέλο του πραγματικού πληροφοριακού περιβάλλοντος που μελετάται, ορίζοντας έτσι σαφώς τα όρια του. Ένα τέτοιο περιβάλλον μπορεί να αποτελείται από ένα ή περισσότερα πληροφοριακά συστήματα και να εμπεριέχει τόσο ανοικτά διασυνδεδεμένα συστήματα όσο και κλειστά συστήματα.
- Καταγράφει και αποτιμά τα περιουσιακά στοιχεία του συστήματος.
- Εκτιμά πιθανές συνέπειες λόγω της χρήσης της τεχνολογίας των αυτοματοποιημένων πληροφοριακών συστημάτων.
- Αναλύει αδυναμίες του συστήματος που σε συνδυασμό με πιθανές επιθέσεις εναντίον του διαμορφώνουν συνέπειες.
- Υπολογίζει τον βαθμό κινδύνου του συστήματος.
- Επιλέγει και προτείνει αποτελεσματικά με την έννοια της βελτιστοποίησης του λόγου κόστους/ απόδοση, αντίμετρα που ελαττώνουν τον κίνδυνο σε αποδεκτά επίπεδα.
- Παρακολουθεί την υλοποίηση των αντίμετρων καθώς και το βαθμό αποτελεσματικότητας τους, τη συμφωνία τους με διεθνή πρότυπα, την επικαιρότητα τους και την καταλληλότητα τους στο συγκεκριμένο επιχειρησιακό περιβάλλον και προτείνει κατά καιρούς αλλαγές αν αυτό κριθεί απαραίτητο.

Η διαχείριση κινδύνων είναι η τεχνική που χρησιμοποιείται κατά κύριο λόγο από ειδικούς της ασφάλειας πληροφοριακών συστημάτων προκειμένου να διερευνήσουν τη σκοπιμότητα εφαρμογής αντιμέτρων. Ειδικότερα η διαχείριση κινδύνων θεωρείται ως τεχνική που μπορεί να χρησιμοποιηθεί για την αιτιολόγηση της αναγκαιότητας εφαρμογής αντίμετρων προς τη διοίκηση του οργανισμού.Από άλλη – περισσότερο τεχνική – οπτική γωνία η διαχείριση κινδύνων θεωρείται ως ένα εργαλείο για τη σχεδίαση της ασφάλειας πληροφοριακών συστημάτων με χρήση αντιμέτρων που επιλέγονται βάσει στατιστικών μεθόδων.

Η διαχείριση κινδύνων είναι μια συνεχής κυκλική διαδικασία που συνήθως ξεκινά από το πρώτο στάδιο του ορισμού των ορίων ενός πληροφοριακού συστήματος. Τα υπόλοιπα στάδια συμπληρώνουν τη διαδικασία, της οποίας τελικός στόχος είναι το λεγόμενο **«Ασφαλές Υπολογιστικό Περιβάλλον».**

Η διαχείριση κινδύνων είναι ένα πολύ σημαντικό εργαλείο στη σχεδίαση ασφαλών πληροφοριακών συστημάτων, επειδή συστηματικά ταξινομεί και καθοδηγεί τη διαδικασία απόφασης για το ποιο υποσύνολο από το σύνολο των πιθανών αντιμέτρων θα υλοποιηθεί. Είναι λοιπόν απαραίτητη για την υποστήριξη της προσπάθειας ανάπτυξης ασφαλών πληροφοριακών συστημάτων από τη διοίκηση του οργανισμού.

Μεθοδολογίες Διαχείρισης Κινδύνων

Σήμερα υπάρχουν διαθέσιμες πολλές μεθοδολογίες διαχείρισης κινδύνων, οι περισσότερες από αυτές διατίθενται και σε αυτοματοποιημένη μορφή, δηλαδή επιτρέπουν τη χρήση υπολογιστή.

Η επιλογή της πιο κατάλληλης μεθόδου για το συγκεκριμένο περιβάλλον και οι ανάγκες μιας επιχείρησης ή ενός οργανισμού είναι πολύ σημαντική αλλά και καθόλου εύκολη. Οι παράγοντες που δυσκολεύουν μια τέτοια επιλογή είναι οι εξής:

1) Δεν υπάρχει διαθέσιμος πλήρης κατάλογος όλων των διαθέσιμων μεθοδολογιών, με τα ιδιαίτερα χαρακτηριστικά τους.
2) Δεν υπάρχει κοινά αποδεκτό σύνολο κριτηρίων αξιολόγησης για τις μεθοδολογίες.
3) Κάποιες μεθοδολογίες καλύπτουν τμήματα μόνον της όλης διαδικασίας διαχείρισης κινδύνων
4) Οι μεθοδολογίες διαφέρουν πολύ στο επίπεδο ανάλυσης που χρησιμοποιούν. Κάποιες χρησιμοποιούν υψηλού επιπέδου περιγραφές του πληροφοριακού συστήματος που μελετούν ενώ κάποιες άλλες απαιτούν λεπτομερειακές περιγραφές.
5) Κάποιες μέθοδοι δεν διατίθενται στην ελεύθερη αγορά, γεγονός που κάνει την αξιολόγηση τους πολύ δύσκολη, αν όχι αδύνατη.

1.4. Ο Κύκλος Ζωής της Ασφάλειας Πληροφοριών σε έναν Οργανισμό

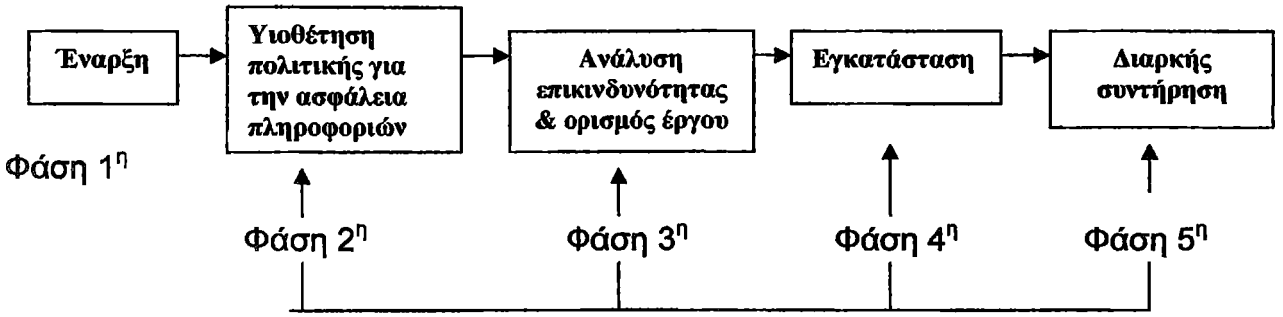
Το πρόβλημα της ασφάλειας των πληροφοριών αφορά στην προστασία της **ακεραιότητας / ορθότητας (integrity)** των βάσεων δεδομένων και αρχείων (βάση γνώσης) στα οποία είναι καταχωρημένες οι πληροφορίες. Οι χρήστες ενός πληροφοριακού συστήματος έχουν την δυνατότητα να ανακτούν πληροφορίες και να τις τροποποιούν. Προκειμένου να προστατευθεί το περιεχόμενο των αρχείων το σύστημα ελέγχει το **βαθμό εξουσιοδότησης (authorization)** του κάθε χρήστη.

Μερικοί χρήστες είναι εξουσιοδοτημένοι για ανάγνωση μόνο **(read – only)** , άλλοι για ανάγνωση και γράψιμο **(read and write)** και αυτά για κάποιο τμήμα ή όλη τη βάση γνώσης. Με αυτόν τον τρόπο το πληροφοριακό σύστημα προστατεύεται από λάθη (μη ηθελημένα ή σκόπιμα). Για να γίνει αυτό ο κάθε χρήστης είναι δηλωμένος στο σύστημα με την ταυτότητα του (π.χ. **κωδικός χειριστή- user ID**) και για να κάνει μια δοσοληψία θα πρέπει να δώσει στο σύστημα κάποιο συνθηματικό **κωδικό εισαγωγής (password)** που αν δεν είναι ακριβώς εκείνο που έχει προκαθοριστεί δεν θα μπορέσει να έχει προσπέλαση στα δεδομένα.

Ο σκοπός ύπαρξης μιας μεθοδολογίας για την ασφάλεια πληροφοριών δημιουργεί πολλαπλούς στόχους , ενώ προκύπτει από προβλήματα όπως τα ακόλουθα:

- Οι περισσότερες επιχειρήσεις έχουν υλοποιήσει τμηματικά την ασφάλεια των πληροφοριών με αποτέλεσμα να εμφανίζεται υψηλό ποσοστό αποτυχίας.
- Η πλειοψηφία των οργανισμών χειρίζεται την ασφάλεια των πληροφοριών είτε από μια τεχνολογική οπτική γωνία ή από την πλευρά των εφαρμογών, έχοντας ως κατάληξη ένα χαλαρά ολοκληρωμένο περιβάλλον.
- Η επιδίωξη παραδοσιακών τυπικών δομών διοίκησης έχουν αρνητική επίδραση στην υλοποίηση της ασφάλειας πληροφοριών.
- Η έλλειψη δέσμευσης από τη διοίκηση συμπεριλαμβανομένης της ανώτερης μέσης και γενικής.

Έχοντας κατά νου τις συνηθισμένες δομημένες προσεγγίσεις σχετικά με τον κύκλο ζωής ανάπτυξης λογισμικού, αναπτύχθηκαν οι κύριες φάσης μιας μεθοδολογίας για την εισαγωγή, υλοποίηση και συντήρηση της ασφάλειας των πληροφοριών όπως αυτή παρουσιάζεται παρακάτω.

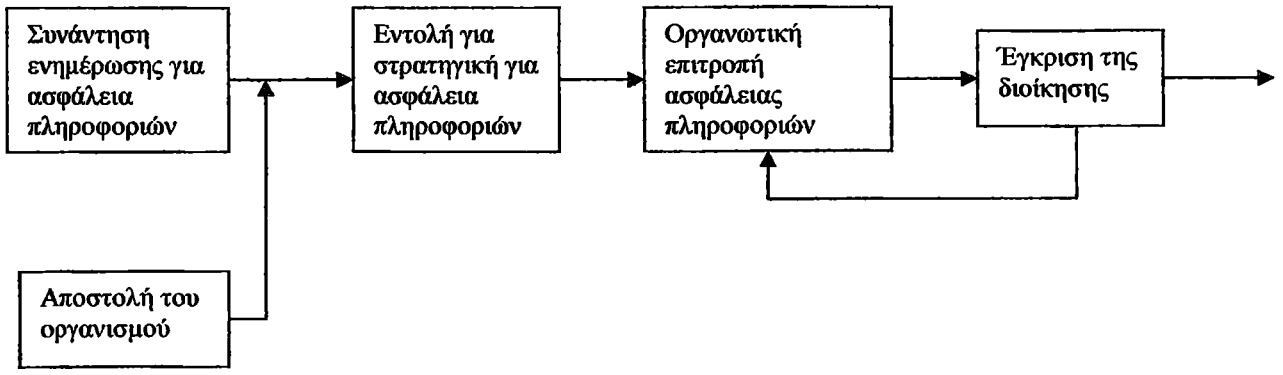


Σχήμα 1.1:Παρουσίαση μια μεθοδολογίας για την ασφάλεια πληροφοριών

Η μεθοδολογία αποτελείται από πέντε φάσεις :

Φάση 1η :Έναρξη

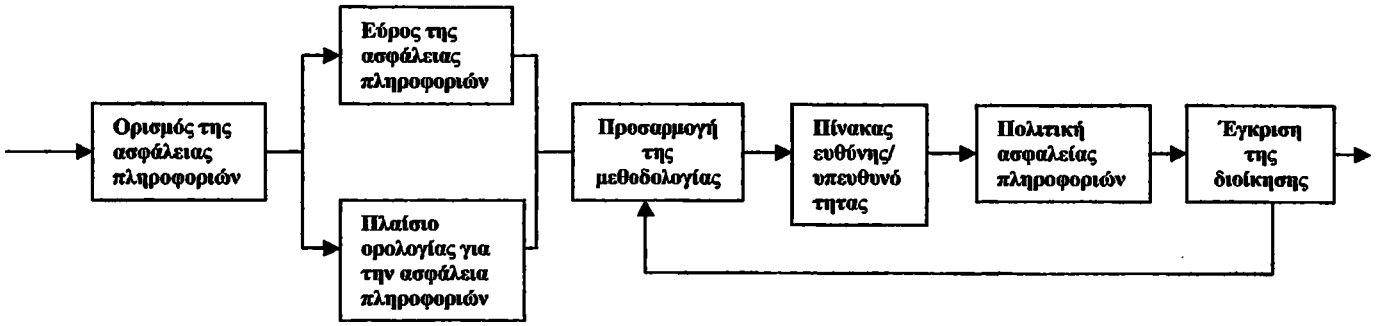
Η φάση αυτή σχετίζεται με τον οργανισμό. Στο σημείο αυτό πρέπει να αναπτυχθεί η ενημερότητα της ανώτερης διοίκηση γύρω από θέματα ασφαλείας πληροφοριών, ώστε να επιτευχθεί η υποστήριξη της αποκτώντας παράλληλα μια νέα στάση και προσέγγιση προς στρατηγικά σημαντικά αγαθά της τεχνολογίας πληροφοριών. Επίσης κρίνεται ότι θα πρέπει να ορισθεί μια ειδική ομάδα ανθρώπων η οποία θα έχει ως αντικείμενο την προστασία αυτών των αγαθών εισάγοντας νέες τεχνικές.



Σχήμα 1.2:Φάση 1η: Έναρξη

Φάση 2η :Υιοθέτηση πολιτικής για ασφάλεια πληροφοριών

Η ανώτερη διοίκηση θα πρέπει να υιοθετήσει μια πολιτική για την ασφάλεια, η οποία είναι η βάση για την ανάπτυξη κατάλληλου πλαισίου για τη διαχείριση της ασφάλειας πληροφοριών. Η πολιτική αυτή θα καλύπτει τις ανάγκες όλων των τμημάτων του οργανισμού που θα χρειάζονται την ασφάλεια πληροφοριών.



Σχήμα 1.3: Φάση 2η: Υιοθέτηση πολιτικής ασφαλείας υπολογιστών

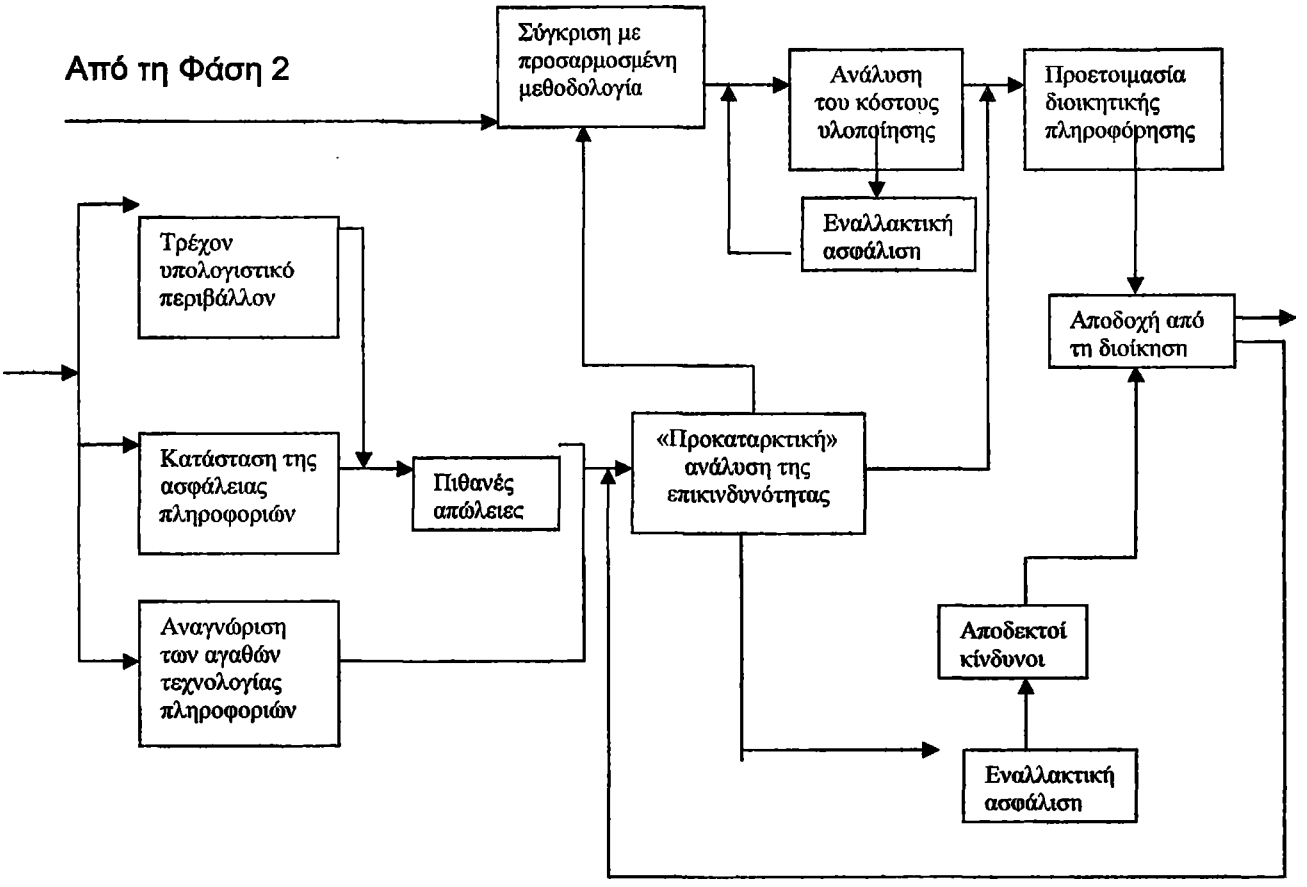
Φάση 3η :Ανάλυση της Επικινδυνότητας και ορισμός έργου (project definition)

Αν επιλεγούν τα κατάλληλα μέτρα προστασίας, το άμεσο και έμμεσο κόστος που σχετίζεται μα αυτά θα πρέπει να είναι λιγότερο από το κόστος των ζημιών τα οποία υποτίθεται ότι θα αποτρέψουν. Η αναγνώριση των ζημιών και των μέτρων προστασίας αποτελούν σημαντικά δεδομένα εισόδου για την ανάπτυξη ενός πλάνου εργασίας για την σωστότερη διαχείριση ενός έργου ασφαλείας πληροφοριών.

Προτού προσδιοριστεί η τρωτότητα ενός συστήματος σε σχέση με πιθανούς κινδύνους είναι απαραίτητο να γίνει αντιληπτό ότι η πληροφορία είναι ένα πολύτιμο περιουσιακό στοιχείο. Η αναγνώριση αυτών των κινδύνων θα ξεκινήσει από τη διατύπωση ενός γενικού και ευρύ ορισμού του προβλήματος και την ανάλυση της επικινδυνότητας. ***Η σύγκριση του κόστος των προβλημάτων και του κόστους των λύσεων δεν είναι δυνατή χωρίς την ποσοτικοποίηση του προβλήματος σε χρήμα.*** Θα πρέπει να εντοπιστούν οι λύσεις σε προφανή προβλήματα με σχετικά χαμηλό κόστος επίλυσης.

Μετά την ανάλυση της επικινδυνότητας το επόμενο βήμα οδηγεί στο να προσδιοριστεί ποιοι κίνδυνοι είναι αποδεκτοί και αν μπορούν να καλυφθούν με ασφάλιση (insurance). Για τους μη αποδεκτούς κινδύνους θα πρέπει να επιλεγεί ένα σύνολο από μέτρα προστασίας τα οποία τους ελαχιστοποιούν έχοντας ταυτόχρονα το μικρότερο δυνατό κόστος.

Η προετοιμασία της επαρκούς πληροφόρησης η οποία θα δοθεί στη διοίκηση για έγκριση της εγκατάστασης των επιλεγμένων μέτρων προστασίας, θα πρέπει να σχεδιαστεί με προσοχή και να περιλαμβάνει τεκμηριωμένους «αποδεκτούς κινδύνους» και πιθανή, εναλλακτική ασφάλιση καθώς και μια πλήρη έκθεση της ανάλυσης κόστους/ οφέλους /παραγωγικότητας (cost/ benefit/ productivity) του προβλήματος και των προτεινόμενων μέτρων προστασίας.



Σχήμα 1.4: Φάση 3η: Ανάλυση επικινδυνότητας και ορισμός του έργου(προβλήματος)

Όσο υλοποιούνται μέτρα προστασίας , οι απώλειες μειώνονται, ενώ το κόστος των μέτρων αυξάνεται. Το άθροισμα των απωλειών και του κόστους των μέτρων παρουσιάζει κάποιο ελάχιστο σημείο . Ο στόχος είναι να επιλεγεί αυτό το σημείο, στο οποίο οι ζημιές και το κόστος των αντιμέτρων να κινούνται κοντά σε αυτό αλλά όχι στα δεξιά του ελάχιστου. Αυτό το σημείο καμπής θα αναπαριστά τον οικονομικά αποδοτικά βαθμό έντασης της ασφάλειας.

Υπάρχει ακόμα ένας ακόμα σημαντικός παράγοντας ο οποίος εμφανίζεται σχετικός με το επίπεδο ασφαλείας: όσο δυναμώνει η «ένταση» ασφαλείας θα πρέπει να εφαρμοστούν στους πόρους(ανθρώπους, δεδομένα κτλ) διάφορα εντεινόμενα μέτρα 'ώστε να αποκτηθεί ένα αυξανόμενο επίπεδο ασφαλείας. Ο παράγοντας αυτός ονομάζεται **παραγωγικότητα (productivity)** π.χ. η ενσωμάτωση στην κανονική λειτουργία των προγραμμάτων, μέτρων λογικής πρόσβασης και ελέγχων λογικής του προγράμματος. **Η εύρεση του σημείου ισορροπίας ανάμεσα στην**

παραγωγικότητα και τα μέτρα προστασίας είναι κρίσιμη για την επιτυχία οποιουδήποτε υπολογιστικού περιβάλλοντος τελικού χρήστη (end – user computing environment). Η σχέση αυτή είναι δυνατόν να απεικονιστεί ως εξής:

$$\textbf{Παραγωγικότητα} = \frac{1}{\text{Επίπεδο προστασίας}}$$

Φάση 4η: Εγκατάσταση

Η φάση αυτή καλύπτει όλες τις τεχνολογικές πλευρές της ασφάλειας πληροφοριών. Όπως τη φυσική και λογική πρόσβαση, την κρυπτογραφία, το πλάνο ανάκαμψης μετά από καταστροφή κ.α.

Φάση 5η: Διαρκής Συντήρηση

Η ανάπτυξη συστημάτων ελέγχου μέσα σε συστήματα εφαρμογών (application systems) θα πρέπει να ορισθεί παράλληλα με τις διαρκείς διαδικασίες συντήρησης, όπως ελεγκτικές υπηρεσίες, την εκπαίδευση και αναθεώρηση των μέτρων προστασίας, συμπεριλαμβανομένης και της πολιτικής ασφαλείας.

1.5 Χρήστες του Εργαλείου

Οι χρήστες του εργαλείου υποστήριξης της ανάλυσης και της διαχείρισης της επικινδυνότητας Πληροφοριακών Συστημάτων θα είναι χρήστες ειδικού σε θέματα ασφαλείας πληροφοριών, οι οποίοι θα κάνουν χρήση αυτού:

1) Εσωτερικά στο πληροφοριακό σύστημα ενός οργανισμού (όπως θα έκανε ένας υπεύθυνος ασφαλείας πληροφοριών) ή
2) Εξωτερικά στον οργανισμό (όπως σύμβουλοι σε θέματα ασφαλείας και διαχείρισης της επικινδυνότητας) αλλά και
3) Εσωτερικά και εξωτερικά στα πλαίσια του κύκλου ζωής ενός πληροφοριακού συστήματος.

Τα μοντέλα ανάλυσης και διαχείρισης της επικινδυνότητας, οι μέθοδοι και τα πακέτα λογισμικού αποτελούν σημαντικά εργαλεία για τον σχεδιασμό της ασφάλειας ενός πληροφοριακού συστήματος αλλά το να λάβει κάποιος τις σωστές απαντήσεις στα σχετικά ζητήματα εξαρτάται από την εμπειρία του ειδικού. Συχνά απαιτείται να λαμβάνονται αποφάσεις άλλοτε με βάση αδιάσειστα στοιχεία και άλλοτε με στήριγμα γενικές αρχές ενώ σε άλλες περιπτώσεις θα πρέπει να γίνονται καινοτομίες και να

χρησιμοποιείται η διαίσθηση που θα βασίζεται σε μια μεγάλη ποικιλία από σχετικές εμπειρίες. Η εμπειρογνωμοσύνη η οποία εμπεριέχει ένα αποδοτικό και αποτελεσματικό μείγμα όλων αυτών των απόψεων δεν χάνει τη δύναμη της με την υιοθέτηση μιας γενικής μεθόδου ανάλυσης και διαχείρισης της επικινδυνότητας. Αλλά χρησιμοποιείται με πιο αποτελεσματικό τρόπο.

ΚΕΦΑΛΑΙΟ 2

Η ΦΙΛΟΣΟΦΙΑ ΤΟΥ ΕΡΓΑΛΕΙΟΥ

Όπως είναι γνωστό, ένα εργαλείο βοηθά στην υλοποίηση μιας μεθοδολογίας της οποίας την φιλοσοφία ακολουθεί. Πέρα από την φιλοσοφία του, πρέπει να προσδιοριστεί και σε ποιους στοχεύει- αποσκοπεί η δημιουργία του εργαλείου αυτού. Στις επόμενες σελίδες αναλύονται τα παραπάνω θέματα.

2.1 Ορισμός του εργαλείου

Το εργαλείο αυτό υποστηρίζει την ανάλυση και την διαχείριση της επικινδυνότητας των πληροφοριακών συστημάτων. Έτσι κρίνεται απαραίτητη η οριοθέτηση του χώρου δράσης αυτού για δύο λόγους:

1) Καθότι το εργαλείο θα παραχθεί μέσα από επιστημονική προσπάθεια, υπάρχει προβληματισμός στο που στοχεύει το εργαλείο αυτό να εφαρμοστεί.
2) Επειδή το πληροφοριακό σύστημα εξυπηρετεί κάποιον οργανισμό και «κάποιος» το χρησιμοποιεί πρέπει να προσδιοριστεί ο χρήστης του εργαλείου αυτού.

Έτσι ανάλογα με το χρήστη και το σκοπό χρήσης αλλάζει και η χρησιμότητα του εργαλείου αυτού. Το εργαλείο αυτό θα υποστηρίζει την ανάλυση και την διαχείριση της επικινδυνότητας των πληροφοριακών συστημάτων (που από **εδώ και πέρα θα χρησιμοποιείται η λέξη εργαλείο), πρέπει να οριστεί επακριβώς ώστε να είμαστε σε θέση να καταγράψουμε τις απαιτήσεις αυτού.**

Έτσι έχουμε:

> ***Το εργαλείο αυτό σχεδιάζεται για τον αναλυτή. Υποστηρίζει την ανάλυση της επικινδυνότητας του πληροφοριακού συστήματος προς εξέταση και διαχειρίζεται την επικινδυνότητα στον οργανισμό – του ελλαδικού χώρου πάντοτε - του οποίου το πληροφοριακό σύστημα εξετάζεται, τα οποία προήλθαν από το εργαλείο και φιλτραρίστηκαν από τον αναλυτή.***

Από τον ορισμό αυτόν προκύπτουν κάποια συμπεράσματα που θα αναλυθούν στην επόμενη ενότητα.

2.2 Συμπεράσματα

Ο ορισμός του εργαλείου που προαναφέρθηκε παραπέμπει στα εξής συμπεράσματα:

- Το εργαλείο αυτό δεν προορίζεται προς πώληση σε εταιρείες - οργανισμούς. Το εκπαιδευτικό ίδρυμα (μέσω της σχετικής επιστημονική ομάδας)θα το χρησιμοποιεί αναλαμβάνοντας την εκπόνηση σχετικών έργων. Επίσης το εργαλείο θα χρησιμοποιείται και από συμβουλευτικές εταιρείες (consultant houses) για την πραγματοποίηση της ανάλυσης σε εταιρείες / πελατών αυτών.

- Ο αναλυτής που θα χρησιμοποιήσει το εργαλείο αυτό πρέπει να είναι γνώστης θεμάτων σχετικά με την ασφάλεια. Δηλαδή πρέπει να έχει εμπειρία σχετική με την ανάλυση των πληροφοριακών συστημάτων, την ανάλυση της επικινδυνότητας αλλά και με τεχνικά θέματα και θέματα διαχείρισης έργων Πληροφορικής. Οι συμβουλευτικού οίκοι είναι σε θέση να έχουν τέτοιους αναλυτές (λόγω αυξημένων προσόντων ζήτησης ή και προϋπηρεσίας -εμπειρίας που διαθέτουν σε τέτοια έργα).

- Τα συμπεράσματα που θα προκύπτουν από τα έργα θα φιλτράρονται (με τη σχετική εχεμύθεια) ώστε δυναμικά το εργαλείο αυτό να τροποποιείται και να προσαρμόζεται στις αλλαγές που πραγματοποιούνται στον ελληνικό χώρο και στις ΤΠΕ.

- Το εργαλείο αυτό προορίζεται για τον ελληνικό χώρο, οπότε πρέπει να λαμβάνεται υπόψη η ιδιαιτερότητα του Έλληνα (ιδίως η κουλτούρα του). Επίσης πρέπει η σχετική νομοθεσία να εφαρμόζεται (ν.2472/1997 αρθ. 10 παρ. 3 και οδ. 95/46/EC αρ. 17 παρ. 2) ενώ οι οθόνες , τα ερωτηματολόγια, οι εκθέσεις (reports) και γενικά κάθε διεπαφή του πρέπει να είναι στην ελληνική γλώσσα.

- Η χρηματική αξία των επιπτώσεων και αντίμετρων πρέπει να εκφράζεται σε EURO και προαιρετικά ίσως και σε δολάρια.

Εκτός από τα προαναφερθέντα συμπεράσματα που προκύπτουν (ή και υπονοούνται) από τον ορισμό, αναδύονται και κάποια άλλα θέματα σχετικά με το εργαλείο αυτό. Συγκεκριμένα:

- Η χρήση του εργαλείου από εξειδικευμένα άτομα, περιορίζει την ανάγκη για ένα εργαλείο εύκολο στη χρήση και φιλικό προς τον χρήστη. Βέβαια δεν πρέπει το εργαλείο αυτό να είναι δύσκολο στη χρήση και δυσνόητο αλλά δεν πρέπει να τίθεται ανάγκης να προσφέρει λεπτομερέστατη βοήθεια.

- Το εργαλείο υποστηρίζει τη διαχείριση της επικινδυνότητας μέχρι του βαθμού πρότασης των κατάλληλων και αποδεκτών από την διοίκηση του προς εξέταση οργανισμού, αντίμετρων. Δεν θεωρείται η επιστημονική ομάδα ή η συμβουλευτική εταιρεία υπεύθυνη για τη διαχείριση της επικινδυνότητας αλλά ο οργανισμός για τις αποφάσεις τις οποίες έλαβε και τον τρόπο υλοποίησης αυτών.

Κατ' επέκταση η επιστημονική ομάδα αγνοεί ανάλυση και σχέδιο ασφάλειας που προϋπήρχε στον οργανισμό του οποίου την ανάλυση αναλαμβάνει να διεκπεραιώσει. Η ανάλυση θα πραγματοποιηθεί εξαρχής λαμβάνοντας υπόψη μόνο τα τωρινά δεδομένα και τις τρέχουσες συνθήκες χρησιμοποιώντας τα προηγούμενα για εμπλουτισμό της βάσης γνώσης.

Πέρα από τα συμπεράσματα αυτά πρέπει να επισημανθεί ότι κάθε εργαλείο ακολουθεί - υλοποιεί κάποια μεθοδολογία. Στην επόμενη ενότητα περιγράφεται η μεθοδολογία που το εργαλείο αυτό υλοποιεί.

2.3 Η Μεθοδολογία του Εργαλείου

Πριν την περιγραφή της μεθοδολογίας που το εργαλείο ακολουθεί κρίνεται σκόπιμη μια κριτική των υπαρχόντων εργαλείων και μεθόδων ανάλυση και διαχείρισης της επικινδυνότητας.

2.3.1. Τα Πλεονεκτήματα της Ανάλυσης και Διαχείρισης της Επικινδυνότητας

Όπως αναφέρει ο Baskerville , η ανάλυση και η διαχείριση της επικινδυνότητας αποτελεί ένα σημαντικό εργαλείο επικοινωνίας μεταξύ του αναλυτή και της διοίκησης. Μέσω της ανάλυσης κόστους / οφέλους (cost/benefit analysis)αιτιολογείται στην ανώτερη διοίκηση η επιλογή των συγκεκριμένων αντιμέτρων και η διοίκηση ευαισθητοποιείται σε θέματα ασφαλείας.

Πέρα όμως από εργαλείο επικοινωνίας έρχεται και σε σύμπνοια με τις απαιτήσεις της ελληνικής και ευρωπαϊκής νομοθεσίας (ν.2472/1997 αρθ. 10 παρ. 3 και οδ. 95/46/EC αρ. 17 παρ. 2). Σύμφωνα με τον νόμο και την οδηγία αυτή , τα πληροφοριακά συστήματα τα οποία επεξεργάζονται προσωπικά δεδομένα, απαιτούνται να λαμβάνουν μέτρα προστασίας, έτσι ώστε, έτσι ώστε « να εξασφαλίζεται ένα επίπεδο ασφαλείας ανάλογο προς του κινδύνους που συνεπάγεται η επεξεργασίας και η φύση των δεδομένων»(Νόμος της Αναλογικότητας).

Τέλος θεωρείται ευέλικτη ώστε να μπορέσει να ενταχθεί σε διάφορα επιστημονικά πλαίσια και να μπορεί να εφαρμοστεί αυτούσια αλλά και σε συνδυασμό με άλλες μεθοδολογίες. Πέρα όμως από τα προαναφερόμενα πλεονεκτήματα η ανάλυση και διαχείριση της επικινδυνότητας παρουσιάζει και μειονεκτήματα.

2.3.2. Τα Μειονεκτήματα της Ανάλυσης και Διαχείρισης της Επικινδυνότητας

Η μέθοδος αυτή , στηριζόμενη στις προαναφερθέντες αναφορές, αγνοεί την «κοινωνική πραγματικότητα» των πληροφοριακών συστημάτων και μεγιστοποιεί την επιρροή των «ειδικών» τεχνοκρατών. Επίσης δημιουργεί ένα απλουστευμένο μοντέλο των πληροφοριακών συστημάτων , αγνοώντας τις αλληλεπιδράσεις των συνιστωσών αυτού και τα ιδιαίτερα χαρακτηριστικά του οργανισμού στο οποίο ανήκει το πληροφοριακό σύστημα.

Η ανάλυση και η διαχείριση της επικινδυνότητας μπορεί να στηρίζεται στην θεωρία των πιθανοτήτων και της στατιστικής αλλά παρουσιάζει μεγάλη υποκειμενικότητα. Συγκεκριμένα ο εκάστοτε αναλυτής στις εκτιμήσεις του για την αξία των αγαθών και την αποτίμηση των απειλών και των αδυναμιών εισάγει υποκειμενικότητα σχετική με την πείρα που διαθέτει.

Επίσης οι στατιστικές μέθοδοι που χρησιμοποιούνται έχουν τύχει αρνητικής κριτικής από διάφορους ερευνητές για την απλότητα τους. Όλα όμως τα πλεονεκτήματα και τα μειονεκτήματα που παρουσιάζουν τα εργαλεία ανάλυσης και διαχείρισης της επικινδυνότητας οφείλονται στις μεθοδολογίες που ακολουθούν.

2.3.3 Κριτική των Μεθοδολογιών των Εργαλείων

Όπως αναφέρει ο Baskerville σε άλλη επιστημονική του αναφορά , οι μέθοδοι Ασφάλειας Πληροφοριακών Συστημάτων (στις οποίες εντάσσεται και η ανάλυση και διαχείριση της επικινδυνότητας που τα εργαλεία υλοποιούν) μπορούν να χωριστούν σε τρεις γενιές. Πρέπει να τονίσουμε ότι η χρήση της λέξης μεθοδολογία δεν είναι απόλυτα δόκιμη. Αυτό έχει να κάνει με το διαφορετικό εννοιολογικό πλαίσιο που χρησιμοποιούν οι συγγραφείς ,δηλαδή άλλες δεν είναι μεθοδολογίες, ενώ αυτές που θεωρούνται ως τέτοιες δεν ακολουθούν πλήρως τον προαναφερόμενο ορισμό.

Κατάταξη των Μεθόδων Βάσει Χαρακτηριστικών

ς οδων	Πρωταρχικα στοιχεια	Μεθοδοι Αναπτυξης Συστηματος & Τυπικα Εργαλεια	Μεθοδοι Αναπτυξης Ασφαλειας & Τυπικα Εργαλεια	Σκοπός	Μεσα	Προκληση	Δικλονικές υποθεσεις	Εργασιες
οδοι klist	Απεικόνιση των περιορισμένων λύσεων	Τεχνικές λύσεις και διαδικασίες του προμηθευτή	Checklist Ασφάλειας και ανάλυση επικινδυνότητας	Επιλογή συστατικών στοιχείων	Έρευνα διαθέσιμων στοιχείων	Απεικόνιση της λύσης στο πρόβλημα	Καθολικές λύσεις	Krauss 1972 Courtney 1977 Browne 1979
ολογικές ινιστικές δοι	Κατανεμημένη και πολύπλοκη λύση αντίστοιχή των λειτουργικών απαιτήσεων	Top-down engineering, rapid prototyping, system & logic flowcharts	CRAMM, BDSS,πίνακες ανάλυσης έκθεσης και σημείων ελέγχων, ερωτηματολόγια Η/Υ	Καταμερισμός της λύσης	Επίλυση κάθε λειτουργικής απαίτησης	Οργάνωση και ολοκλήρωση ενός σύνθετου συνόλου στοιχείων	Ιδανικές παραμετροποιημένες λύσεις	Parker 1981 Fisher 1984
οδοι κού σχηματισ	Υψηλός σε αφαιρετικό επίπεδο σχεδιασμός και έκφρασης του προβλήματος και του χώρου επίλυσης	Δομημένη ανάλυση, μοντελοποίηση δεδομένων, τεχνολογία πληροφοριών, διαγράμματα οντοτήτων συσχετίσεων &ροής δεδομένων, ευμετάβλητα συστήματα.	Σχεδιασμός λογικών ελέγχων, διαγράμματα ροής δεδομένων	Πρόβλημα και λύση σε αφαιρετικό επίπεδο	Μοντελοποίηση των απαραίτητων στοιχείων του προβλήματος	Επιλογή των σωστών στοιχείων για το μοντέλο	Σχεδιασμός σε αφαιρετικό επίπεδο	Baskerville 1988

Οι μεθοδολογίες της τρίτης γενιάς είναι οι πρόσφατες και σε αυτές μπορούν να προστεθούν και το «Πλαίσιο μεθοδολογίας για τον κύκλο ζωής της ασφάλειας των υπολογιστών στον οργανισμό», Το «Πλαίσιο IBAG για ασφάλεια τεχνολογιών πληροφορίας σε εμπορικό κλάδο» και η «Μεθοδολογία ανάπτυξης ασφαλών συστημάτων εφαρμογών (application systems)». Οι μεθοδολογίες αυτές όπως και της δεύτερης γενιάς ακολουθούν μια μηχανιστική αντίληψη, με εκτέλεση προκαθορισμένων βημάτων. Τα βήματα αυτά θα μπορούσαν χαρακτηριστικά να περιγραφούν ως εξής:

1) Προσδιορισμός και αποτίμηση περιουσιακών στοιχείων του συστήματος.
2) Προσδιορισμός και αποτίμηση απειλών
3) Ανάλυση της Επικινδυνότητας
4) Ιεράρχηση μέτρων προστασίας προς εφαρμογή
5) Υλοποίηση μέτρων και διαρκής συντήρηση (διαχείριση επικινδυνότητας)

Οι προαναφερθείσες μεθοδολογίες ακολουθούν μια κοινή αντίληψη, **Παράδειγμα(Paradigm)** όπως χαρακτηριστικά αναφέρει ο Kuhn,Παράδειγμα είναι

το σύνολο των πεποιθήσεων, των αναγνωρισμένων αξιών και τεχνικών, που ασπάζονται τα μέλη μιας δεδομένης ομάδας επιστημόνων και που τους παρέχει για ένα χρονικό διάστημα πρότυπα προβλημάτων και λύσεων τους. Έτσι οι παραπάνω μεθοδολογίες στηρίζονται στο **Παράδειγμα Ι** ακολουθούν δηλαδή τις εξής παραδοχές:

- Η πραγματικότητα ,όπως την αντιλαμβανόμαστε, είναι [illegible], δηλαδή αποτελείται από συστήματα.
- Η μεθοδολογία που χρησιμοποιούμε για να την διερευνήσουμε είναι [illegible].

Δεν υπάρχει μια αυστηρή διατύπωση με μια συγκεκριμένη σειρά βημάτων, ενώ περιορίζεται περισσότερο στην εξέταση υπαρχόντων συστημάτων. Έτσι είναι περισσότερο στατικά και δύσκαμπτα με περιορισμένη ευελιξία, ενώ ο αναλυτής παίζει το ρόλο του λύτη του προβλήματος που εξαρχής είναι γνωστό ότι υπάρχει και έχει καθοριστεί. Ο αναλυτής παίζει το ρόλο της αυθεντίας «αντικειμενικοποιώντας»την υποκειμενικότητα (μέσω της χρήσης της στατιστικής) που είναι ορατή αφού οι αποτιμήσεις των απειλών και των αγαθών στηρίζονται στην εμπειρία και μόνο του αναλυτή.

Ακόμα παραλείπεται ο ανθρώπινος παράγοντας διότι θεωρείται ως τεχνικό και μόνο ζήτημα με προβλεπόμενη συμπεριφορά. Ακόμα και το μοντέλο του πίνακα του McCumber παρόλο που επιτρέπει την ταυτόχρονη απεικόνιση διαφόρων θεμάτων (ακόμα και την εκπαίδευση του προσωπικού), μελετά το υπάρχον σύστημα στατικά. Δεν πρέπει όμως να αγνοείται το γεγονός ότι κάθε πληροφοριακό σύστημα δημιουργείται από ανθρώπους και λειτουργεί με αυτούς για ικανοποίηση των δικών τους στόχων. Ακόμα δεν είναι δυνατόν να προβλεφθεί πόσο μάλλον να ποσοτικοποιηθεί η ανθρώπινη συμπεριφορά, γεγονός που εναντιώνεται με την ποσοτικοποίηση και την βελτιστοποίηση στις οποίες στηρίζεται η δύσκαμπτη αυτή προσέγγιση.

Βέβαια οι μεθοδολογίες αυτές έχουν και **πλεονεκτήματα:**

- Είναι κατάλληλες για μεγάλα και σύνθετα συστήματα διευκολύνοντας τον έλεγχο της εγκυρότητας των αποτελεσμάτων μέσω της πιστής εφαρμογής της σχετικής μεθόδου.
- Ο έλεγχος του κόστους διευκολύνεται λόγω της δυνατότητας αιτιολόγησης και αποτίμησης κάθε δραστηριότητας στα πλαίσια της μεθόδου.

Αντίθετα με το Παράδειγμα Ι αναπτύχθηκε η εικονική μεθοδολογία (virtual methodology) που ακολουθεί το παράδειγμα ΙΙ, δηλαδή την ευμετάβλητη προσέγγιση. Κατά τον Kuhn στο Paradigm II επικρατούν οι ακόλουθες παραδοχές:

- Η πραγματικότητα, όπως την αντιλαμβανόμαστε είναι **προβληματική**.
- Η μεθοδολογία που χρησιμοποιούμε για την διερεύνηση της είναι συστημική.

Η μόνη μεθοδολογία που έχει αναπτυχθεί και ακολουθεί το Paradigm II είναι της Hitchings, η αποκαλούμενη και εικονική μεθοδολογία (virtual methodology). Η Hitchings θεωρεί ότι η **μεθοδολογία πρέπει να είναι ένα εργαλείο που θα χρησιμοποιείται σαν καταλύτης για την ανάλυση και τη σχεδίαση ενός πληροφοριακού συστήματος.** Το εργαλείο αυτό πρέπει να προσαρμόζεται ώστε να ταιριάζει στον οργανισμό ή το σύστημα που μελετάται, δηλαδή να είναι εικονικό

εργαλείο. Οι φάσεις της εικονικής μεθοδολογίας παρουσιάζονται στο παρακάτω σχήμα.

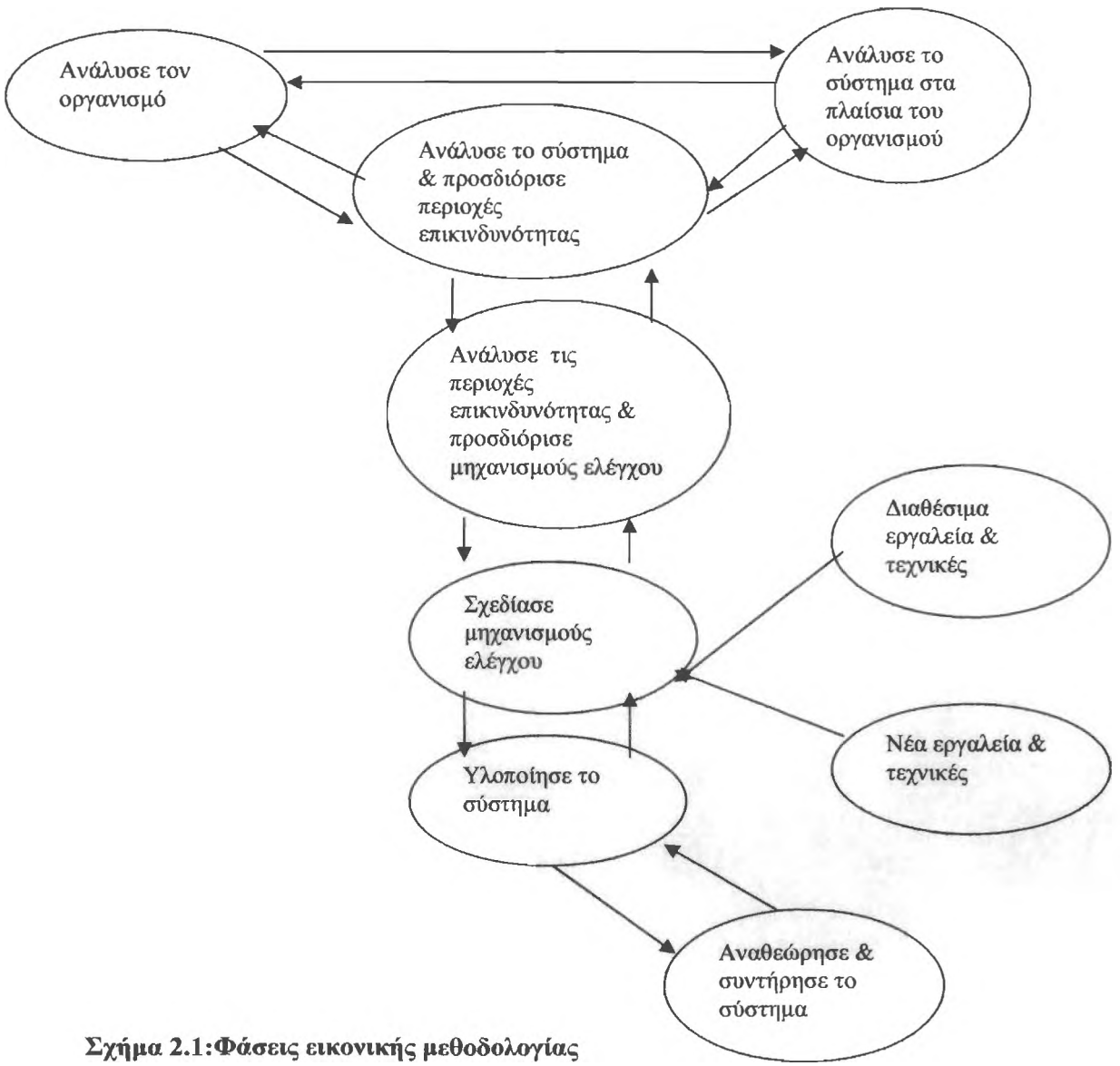
Στα **πλεονεκτήματα της εικονικής μεθοδολογίας** περιλαμβάνονται τα εξής:

- Ο δυναμικός χαρακτήρας της μεθοδολογίας
- Η έμφαση σε θέματα σχετικά με το προσωπικό και η συνεκτίμηση κοινωνικών παραγόντων αλλά και του πλαισίου του οργανισμού στον οποίο το πληροφοριακό σύστημα εντάσσεται.

Αντίστοιχα τα **μειονεκτήματα της** είναι:

- Η αδυναμία αιτιολόγησης του κόστους των αντίμετρων με όρους κόστους – οφέλους
- Η έλλειψη συγκεκριμένων μεθόδων και τεχνικών για την υλοποίηση των φάσεων της μεθοδολογίας αυτής έτσι ώστε να ισχυροποιήσουν την εγκυρότητα της.

Μέσω της παραπάνω κριτικής – παρουσίασης είμαστε σε θέση να παρουσιάσουμε τη μεθοδολογία που το συγκεκριμένο εργαλείο ακολουθεί.



Σχήμα 2.1:Φάσεις εικονικής μεθοδολογίας

2.3.4. Επιλογή της Μεθοδολογίας του Εργαλείου

Όπως προαναφέρθηκε οι μεθοδολογίες που ακολουθούν τα δύο παραδείγματα (paradigms) έχουν ελαττώματα και προτερήματα. Έτσι κρίνεται σκόπιμη μια προσπάθεια συνδυασμού των δύο αυτών προσεγγίσεων (συστηματική και συστημική προσέγγιση).

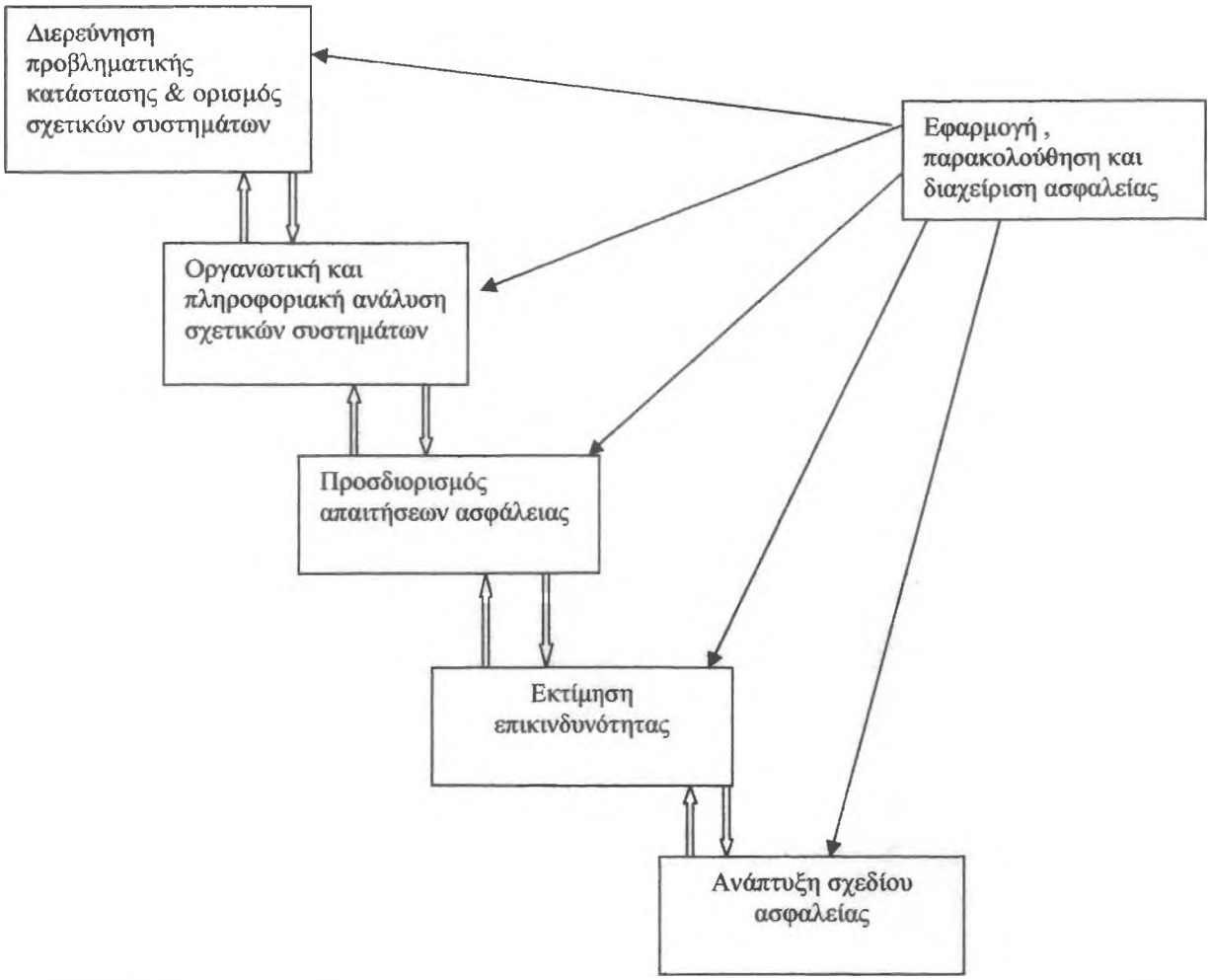
Στην ανάπτυξη ενός πληροφοριακού συστήματος υπάρχει παλινδρόμηση μεταξύ των δύο αυτών παραδειγμάτων. Έτσι ο αναλυτής θα πρέπει πρώτα να εξετάσει το σύστημα outside – in, δηλαδή με όρους εκτός συστήματος (τι βλέπει ο χρήστης), στη συνέχεια θα πρέπει να το εξετάσει inside – out, αφού πρέπει να προσδιορίσει τις ανάγκες των χρηστών.

Μια σχετική μεθοδολογία είναι αυτή που συνδυάζει τρεις δημοφιλείς μεθοδολογικές προσεγγίσεις:

- Τη μεθοδολογία των ευμετάβλητων συστημάτων (SSM – Paradigm II)
- Τη μοντελοποίηση οργανισμών και επιχειρήσεων (business modeling)
- Την ανάλυση της επικινδυνότητας.

Οι φάσεις και τα βήματα της μεθοδολογίας αυτής παρουσιάζονται συνοπτικά στο παρακάτω σχήμα και πίνακα και στη συνέχεια αναλύονται τα βήματα αυτής που σχετίζονται με το συγκεκριμένο εργαλείο. Έτσι δικαιολογείται ταυτόχρονα και ο λόγος επιλογής της συγκεκριμένης μεθοδολογίας.

Σχήμα 2.2: Μεθοδολογίες ανάπτυξης και διαχείρισης ασφάλειας



Φάσεις και Βήματα Μεθοδολογίας Ανάπτυξης και Διαχείρισης Ασφάλειας Πληροφοριακών Συστημάτων

Φάση	Βήματα ανά Φάση
Φάση 1. Διερεύνηση Προβληματικής Κατάστασης και Ορισμός Σχετικών Συστημάτων	**Βήμα 1:**Κατασκευή και ανάλυση πλούσιας εικόνας (rich picture) **Βήμα 2:**Καταγραφή και ανάλυση βασικών ορισμών (root definitions) των υπό εξέταση συστημάτων **Βήμα 3:**Υιοθέτηση ενός βασικού ορισμού και ενός ορισμού ασφαλείας για τα υπό εξέταση συστήματα **Βήμα 5:** Συγκρότηση ομάδων εργασίας **Βήμα 6:** Κατάρτιση του πλάνου και του έργου
Φάση 2. Οργανωτική και Πληροφοριακή Ανάλυση Σχετικών Συστημάτων	**Βήμα 1:**Ανάπτυξη οργανωτικών – επιχειρησια μοντέλων **Βήμα 2:**Ανάπτυξη ερμηνευτικών πληροφορια μοντέλων
Φάση 3. Προσδιορισμός Απαιτήσεων Ασφαλείας	**Βήμα 1:**Προσδιορισμός κύριων αγαθών (assets) ορισμός χαρακτηριστικών ιδιοτήτων ασφαλείας **Βήμα 2:**Ανάλυση επιπτώσεων στον οργανισμό **Βήμα 3:**Αποτίμηση κύριων αγαθών **Βήμα 4:**Προσδιορισμός απαιτήσεων ασφαλείας υποστηρικτικών πόρων **Βήμα 5:**Επικύρωση
Φάση 4. Εκτίμηση επικινδυνότητας	**Βήμα 1:**Εντοπισμός και αποτίμηση απειλών **Βήμα 2:**Εντοπισμός και αποτίμηση αδυναμιών **Βήμα 3:**Εκτίμηση βαθμού επικινδυνότητας **Βήμα 4:**Προσδιορισμός προτεραιοτήτων **Βήμα 5:**Επικύρωση
Φάση 5. Ανάπτυξη Σχεδίου Ασφαλείας	**Βήμα 1:**Προσδιορισμός ρόλων και υπευθυνοτήτων **Βήμα 2:**Ανάπτυξη πολιτικής ασφαλείας **Βήμα 3:**Επιλογή μέτρων προστασίας **Βήμα 4:**Ανάπτυξη στρατηγικού σχεδίου εφαρμογής συνεχούς διαχείρισης επικινδυνότητας
Φάση 6. Εφαρμογή, Παρακολούθηση διαχείριση Ασφαλείας	**Βήμα 1:**Επικύρωση – αποδοχή σχεδίου ασφαλείας **Βήμα 2:**Εφαρμογή σχεδίου ασφάλειας **Βήμα 3:**Συνεχής παρακολούθηση και διαχείριση ασφαλείας **Βήμα 4:**Έλεγχος – επανεκτίμηση- Αναθεώρηση

Σχήμα 2.3: Φάσεις και βήματα μεθοδολογίας ανάπτυξης και διαχείρισης ασφαλείας ΠΣ

Η πρώτη φάση κρίνεται πολύτιμη. Μέσω αυτής είναι δυνατή η εξέταση του οργανισμού στον οποίο εντάσσεται το υπό εξέταση ,κάθε φορά πληροφοριακό σύστημα. Βάσει του ορισμού για το συγκεκριμένο εργαλείο ,όπως αναφέραμε παραπάνω, ενδιαφερόμαστε για τον οργανισμό και την κουλτούρα του.

Η επόμενη φάση μας δίνει την δυνατότητα να μπορέσουμε να δούμε τον οργανισμό και το Πληροφοριακό Σύστημα δυναμικά. Δεν πρέπει να ξεχνάμε το γεγονός ότι η πληροφορία είναι μια από τις συνιστώσες κάθε πληροφοριακού συστήματος και η δυνατότητα αποτύπωσης αυτής στατικά (δομή πληροφορίας) και δυναμικά (κύκλος ζωής πληροφορίας) μας βοηθά στη μελέτη της ασφάλειας του συστήματος καθώς συμβάλουν στον εντοπισμό των σημείων όπου απειλείται η ακεραιότητα και η εγκυρότητα (validity) της πληροφορίας. Επίσης η ανάπτυξη οργανωτικών – επιχειρησιακών μοντέλων βοηθά στην αναγνώριση των σημαντικότερων – κρισιμότερων διαδικασιών (processes) και στην αναδιοργάνωση αυτών, λόγω υλοποίησης των προτεινόμενων αντιμέτρων, της διαχείρισης της επικινδυνότητας και της ανατροφοδότησης (feedback) που επιθυμούμε.

Τα αποτελέσματα της 3^{ης} και της 4^{ης} φάσης συνδυάζονται με το παραγόμενο αποτέλεσμα την αποτίμηση του βαθμού επικινδυνότητας. Τα αποτελέσματα των φάσεων αυτών εξαρτώνται από τα προϊόντα των προηγούμενων φάσεων, ιδιαιτέρως από τη δεύτερη. Οι δύο αυτές φάσεις σε συνδυασμό και με την επόμενη αποτελούν το αντικείμενο αυτής της εργασίας. Οι φάσεις αυτές ακολουθούν το Paradigm I έτσι η προσέγγιση θα είναι δύσκαμπτη με συγκεκριμένα προς υλοποίηση βήματα.

Οι τελευταίες δύο φάσεις σχετίζονται με τη διαχείριση της επικινδυνότητας. Τόσοι η πολιτική ασφαλείας όσο και τα αντίμετρα (προϊόντα πέμπτης φάσης) εντάσσονται στις ενέργειες της διαχείρισης της επικινδυνότητας. Επίσης η εφαρμογή του σχεδίου ασφαλείας και η εξασφάλιση του επιπέδου ασφάλειας του οργανισμού (στόχοι έκτης φάσης) αποτελούν τις ενέργειες για τη συνεχή διατήρηση και παρακολούθηση της επικινδυνότητας.

Σε όλες τις φάσεις της μεθοδολογίας αυτής, υπάρχει επικύρωση από τη διοίκηση ή τους δικαιούχους, Αυτό συσχετίζεται με την παραδοχή ότι τα εργαλεία ανάλυσης και διαχείρισης της επικινδυνότητας αποτελούν το μέσο επικοινωνίας μεταξύ αναλυτή και διοίκηση. Άλλα πλεονεκτήματα χρήσης της μεθοδολογίας αυτής είναι η προσπάθεια της να συγκεράσει διαφορετικά παραδείγματα.

Δεν πρέπει επίσης να λησμονούμε τον ορισμό για το συγκεκριμένο εργαλείο. Δεν πρέπει η κουλτούρα και το πλαίσιο του οργανισμού στον οποίο εντάσσεται το υπό εξέταση Πληροφοριακό σύστημα να αγνοείται. Η προαναφερόμενη μεθοδολογία μπορεί να συνδυάζει στοιχεία σχετικά με τον οργανισμό και το πληροφοριακό σύστημα ως σύστημα ανθρώπινης δραστηριότητας αλλά και στοιχεία τα οποία εμφανίζονται σε κάθε ένα από τα υπάρχοντα εργαλεία ανάλυσης και διαχείρισης της επικινδυνότητας.

Παρόλα αυτά υπάρχουν μειονεκτήματα στη χρήση της μεθοδολογίας αυτής. Το κυριότερο μειονέκτημα είναι το υψηλό κόστος εφαρμογής της .Εντούτοις η μεθοδολογία είναι αρκετά ευέλικτη αφήνοντας περιθώριο για ενσωμάτωση λιγότερο ή περισσότερο δαπανηρών μεθόδων και τεχνικών υλοποίηση των βημάτων της.

ΚΕΦΑΛΑΙΟ 3

ΑΝΑΛΥΣΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

3.1 Οι δυσχέρειες της διαχείρισης της επικινδυνότητας –Γενικές Απόψεις

Τα τελευταία είκοσι χρόνια,τα διοικητικά στελέχη βομβαρδίστηκαν από πληθώρα απόψεων και συμπερασμάτων που σχεδόν ασταμάτητα παράγονται στο διαρκώς αναπτυσσόμενο πεδίο της μηχανοργάνωσης των επιχειρήσεων. Πολυάριθμες μελέτες,συμπεράσματα ερευνών και ολοκληρωμένες θεωρίες προσπαθούν να εξηγήσουν το σύνθετο πρόβλημα της διαχείρισης, ανάλυσης καθώς και του τρόπου αντιμετώπισης της επικινδυνότητας που γεννάται από την χρήση των πληροφοριακών συστημάτων. Προσπαθούν να δώσουν στα διοικητικά και εκτελεστικά στελέχη σαφής και ειδικές οδηγίες για την καλύτερη διαχείριση των συστημάτων αυτών και των δυσχερειών που προκύπτουν κατά την εφαρμογή και χρήση τους στα πλαίσια μιας οργάνωσης που στοχεύει στη μεγιστοποίηση της παραγωγικότητας της επιχείρησης.

Πράγματι,η επίδραση διακεκριμένων επιστημόνων ,όπως οι: , διακρίνεται πολύ έντονα.Η μεγάλη προσφορά και οι υποδείξεις αυτής της ελιτιστικής ομάδας των ερευνητών είχαν έντονη επίδραση στον χώρο των επιχειρήσεων και της βιομηχανίας της πληροφορικής και επηρέασαν καθοριστικά την ανάπτυξη και την εφαρμογή των πληροφοριακών συστημάτων στις επιχειρήσεις.

Γίνεται λοιπόν μια προσπάθεια να παρουσιαστούν συνοπτικά,αλλά με σαφήνεια και ακρίβεια, οι απόψεις που προτείνουν οι πρωτοπόροι αυτοί ερευνητές των πληροφοριακών συστημάτων , σχετικά με την αναγκαιότητα της ανάλυσης και της διαχείρισης της επικινδυνότητας σε μια επιχείρηση ή έναν οργανισμό, υποστηρίζοντας ότι μπορούν να βοηθήσουν άμεσα τα διοικητικά στελέχη να διευθύνουν καλύτερα τις επιχειρήσεις τους, καθώς και ότι αυτές μπορούν να αποβούν χρονοβόρες για την επιχείρηση και για αυτό θα πρέπει να αποφεύγεται να υιοθετούνται από τις επιχειρήσεις.

Ας εξετάσουμέ τώρα μερικές από τις σπουδαιότερες απόψεις που επικρατούν τα τελευταία χρόνια.

Ο **Williams** επιχειρηματολογεί ότι τα αποτελέσματα και η επιτυχία της ανάλυσης της επικινδυνότητας (αναφερόμενος γενικά στην ανάλυση της επικινδυνότητας),μπορεί να είναι τόσο θετικά, όσο θετική είναι και η αντίληψη και η ποσοτικοποίηση τη επικινδυνότητας από την ομάδα των αναλυτών και τονίζει ότι αυτό είναι το σημείο όπου δοκιμάζεται η αξιοπιστία της ανάλυσης της επικινδυνότητας.

Από την άλλη μεριά, σύμφωνα με τον **Bernstein**, το μεγαλύτερο πρόβλημα για την επικινδυνότητα είναι ότι χρειάζεται περισσότερη δημιουργική δουλειά για την

ανάπτυξη εργαλείων πρόβλεψης (predictive tools) και μετρήσεων, τα οποία δε θα στηρίζονται σε μεγάλο βαθμό σε ιστορικά δεδομένα.

Ο **Gilbert** ισχυρίζεται ότι ένα σημαντικό μειονέκτημα είναι ότι δεν υπάρχει μια πρότυπη (standard) μέθοδος ή μια συμφωνημένη προσέγγιση για την πραγματοποίηση της ανάλυσης της επικινδυνότητας, ενώ δεν υπάρχει καμία επιβεβαίωση ότι μια συγκεκριμένη μέθοδος είναι πλήρης ή ακριβής.

Σύμφωνα με τον Gilbert η ανάλυση της επικινδυνότητας σχηματίζει τη βάση για την ανάπτυξη ενός αποδοτικού οικονομικά προγράμματος διαχείρισης της επικινδυνότητας. Η διαχείριση της επικινδυνότητας εξασφαλίζει ότι έγιναν όλα τα λογικά βήματα για να εμποδιστούν καταστάσεις που θα μπορούσαν να εμποδίσουν την επιτυχία της αποστολής του οργανισμού. Γενικά η πραγματοποίηση της ανάλυσης της επικινδυνότητας αυξάνει την ενημερότητα του προσωπικού για δυνατά προβλήματα και ενδυναμώνει το πρόγραμμα της διαχείρισης της επικινδυνότητας.

Στο πνεύμα αυτών και ο **Van de Haar και Von Solms** ,παραδέχονται ότι δεν υπάρχουν διεθνών προδιαγραφών αποδεκτά πρότυπα στον τομέα της ανάλυσης της επικινδυνότητας για τα πληροφορικά συστήματα.

Οι **Anderson και Shain** ,αναφέρουν ότι μια τυπική εφαρμογή της ανάλυσης της επικινδυνότητας αποτελεί μια απαράδεκτα χρονοβόρα διαδικασία, απαιτώντας μεγάλη επένδυση σε ανθρώπινους πόρους. Επιπλέον, οι περισσότερες μέθοδοι ανάλυσης της επικινδυνότητας στηρίζονται ουσιαστικά σε ποιοτικές υποθέσεις (quality guesses) ,από όπου προκύπτουν ποσοτικά αποτελέσματα, τα οποία θα πρέπει να αξιολογηθούν με μεγάλη προσοχή. Τέλος, οι ίδιοι συγγραφείς επισημαίνουν ότι οι μέθοδοι ανάλυσης της επικινδυνότητας δεν προσπαθούν να μοντελοποιήσουν το ανθρώπινο περιβάλλον του συστήματος, παρόλο που είναι γενικά παραδεκτό ότι οι άνθρωποι είναι αυτοί που θέτουν τους μεγαλύτερους κινδύνους. Επομένως υπάρχει το ενδεχόμενο μερικοί οργανισμοί να εμπιστευθούν τυπικές εφαρμογές της ανάλυσης της επικινδυνότητας, οι οποίες μπορούν να έχουν μόνο ανακριβή και υποκειμενικά αποτελέσματα.

Στο ίδιο κλίμα βρίσκονται και οι σχολιασμοί του **Baskerville** ,ο οποίος προσθέτει ότι η ανάλυση της επικινδυνότητας πρέπει να αντιμετωπιστεί κύρια ως εργαλείο επικοινωνίας για την δικαιολόγηση των σχετικών με την ασφάλεια δαπανών στην ανώτατη διοίκηση ενός οργανισμού. Πέρα από αυτό το όφελος, διακρίνει ελάχιστη αξία στα τελικά αποτελέσματα της ανάλυσης της επικινδυνότητας, σημειώνοντας ότι « ,η οποία έχει κοινωνικά και ερευνητικά ψεγάδια.

Επίσης επισημαίνει ότι η υπερβολική εμπιστοσύνη στην ανάλυση της επικινδυνότητας μπορεί να αποδειχθεί μια αυτοαναιρούμενη πρακτική, καθώς είναι δυνατό αν τα αποτελέσματα δεν τύχουν προσεκτικής ερμηνείας. Πέρα από αυτό όμως τονίζει ότι, δεν υπάρχει στην πραγματικότητα κάποια εναλλακτική της ανάλυσης της επικινδυνότητας πρακτική για την αξιολόγηση των κινδύνων που αντιμετωπίζει ένας οργανισμός. Σχολιάζοντας το γεγονός ότι οι τρέχουσες μέθοδοι δεν είναι αμερόληπτες, αναφέρει ότι αυτό μπορεί να είναι στην πραγματικότητα ένα θετικό γεγονός, καθώς ένας επαγγελματίας της ασφάλειας μπορεί εύκολα να αλλάξει τις τιμές εισόδου, μέχρι τα αποτελέσματα να φτάσουν σε

ένα επίπεδο επικινδυνότητας αποδεκτό από αυτόν/ ή , αλλά και σε κόστος αποδεκτό από την διοίκηση. Στο τέλος, το επίπεδο της επικινδυνότητας που θα έχει το πληροφοριακό σύστημα (ή τουλάχιστον κάποια από τα στοιχεία του) θα εξαρτάται μόνο από την εμπειρία και την προσωπική κρίση του επαγγελματία της ασφάλειας. Έτσι η μέθοδος ανάλυσης της επικινδυνότητας χρησιμοποιείται μόνο για να προσδώσει κάποια αξιοπιστία στα προτεινόμενα αντίμετρα.

Η άποψη αυτή έρχεται να επιβεβαιώσει την θέση των Anderson και Shain ότι τα εργαλεία ανάλυσης της επικινδυνότητας συχνά χρησιμοποιούνται επειδή αυτό είναι υποχρεωτικό και όχι επειδή τυγχάνει να είναι ιδιαίτερα επαρκή.

Επιπρόσθετα οι **Angell και Smithson** σημειώνουν και αυτοί το πρόβλημα της μεγάλης υποκειμενικότητας των υπολογισμών που αφήνουν την προσέγγιση ανοιχτή στην πολιτική εκμετάλλευση, ενώ εκτός από αυτό αναφέρουν ότι η ανάλυση της επικινδυνότητας είναι εντελώς ακατάλληλη για τους σχετικά απίθανους κινδύνους οι οποίοι μπορούν να αποδεχθούν μοιραίοι.

Το τελευταίο αυτό σημείο αποτίμησης και κατάταξης της επικινδυνότητας τονίζεται και από **τον Hurst** ,ο οποίος επίσης μιλά για την ανικανότητα από μέρους των μεθόδων, διάκρισης ανάμεσα στα γεγονότα υψηλής συχνότητας – χαμηλής επίπτωσης και στα χαμηλής συχνότητας – υψηλής επίπτωσης, θεωρώντας ότι οι περισσότεροι κίνδυνοι βρίσκονται στο μέσο της κλίμακας της επικινδυνότητας.

Μια γενική κριτική γύρω από την ανάλυση της επικινδυνότητας επιχειρεί ο **Charette** ,ο οποίος διακρίνει έξι κινδύνους στην ανάλυση της επικινδυνότητας ,αποκαλύπτοντας έτσι τις συχνά κρυμμένες σε αυτή δυσκολίες.

1) Για αρχή αν η ανάλυση υπερεκτιμά την επικινδυνότητα, τότε μπορεί να εγείρει ένα υπερβολικό ποσό προσπάθειας μετριασμού της.Το γεγονός αυτό μπορεί να οδηγήσει στην παρακράτηση πόρων από άλλες βασικές προβληματικές περιοχές και στην αποτυχία να τύχει εκμετάλλευσης μια νέα ευκαιρία. Συμμετρικά, προς αυτό ,αν η ανάλυση υποεκτιμήσει την επικινδυνότητα το αποτέλεσμα είναι συχνά η έκπληξη όταν ο κίνδυνος τελικά παρουσιάστηκε. Το γεγονός αυτό μπορεί να οδηγήσει τη διοίκηση σε πανικό αντί να αποδειχθεί μια προενεργητική (proactive) διοίκηση να βρεθεί να αντιδρά σε γεγονότα. Σε κάθε περίπτωση την επόμενη φορά που θα πραγματοποιηθεί η ανάλυση υποχρεωτικά ή όχι ,θα υπάρχει αυξημένος σκεπτικισμός σχετικά με την αναγκαιότητα της ή τις προτάσεις της ανεξάρτητα από την περίσταση.

2) Ένας δεύτερος κίνδυνος που προκύπτει για την ανάλυση της επικινδυνότητας είναι ότι μπορεί να είναι πολύ ακριβής. Σε αυτή την περίπτωση δεν μπορεί κάποιος να δείξει αργότερα την πραγματική αξία της ανάλυσης καθώς από την υπόδειξη της ανάλυσης αποφεύχθηκε ο κίνδυνος.

3) Ένα άλλο σημείο που θα πρέπει να προσεχθεί είναι ότι η ανάλυση της επικινδυνότητας μπορεί να χρησιμοποιηθεί σαν μέσο για την διατήρηση της υπάρχουσας κατάστασης με σκοπό την αποθάρρυνση της καινοτομίας ή της αλλαγής.

4) Ένας τέταρτος σημαντικό κίνδυνος είναι ότι η ανάλυση της επικινδυνότητας συχνά βασίζεται υπερβολικά στην παραγωγή αριθμών, ενώ δεν ασχολείται αρκετά

με την ανάλυση των ανθρώπων και της κοινής λογικής για την ερμηνεία των αποτελεσμάτων.

5) Ένας άλλος παράγοντας για την ανάλυση της επικινδυνότητας είναι ότι η πραγματοποίηση της μπορεί να εμποδίσει την επιτυχία ενός έργου. Ο ένας λόγος για αυτό είναι ότι ευνοεί την κατανάλωση πόρων και ο άλλος είναι ψυχολογικός:Αν η επικινδυνότητα μιας προσπάθειας βρεθεί υψηλή τότε το γεγονός της πραγματοποίησης της ανάλυσης της επικινδυνότητας είναι δυνατόν να στιγματίσει την προσπάθεια ως προβληματική και ως εκ τούτου θα έπρεπε να αποφευχθεί.

6) Η τελευταία δυσκολία για την ανάλυση της επικινδυνότητας είναι ότι δεν υπάρχει έλεγχος ποιότητας για τις ίδιες τις μεθόδους ανάλυσης της επικινδυνότητας. Οι κίνδυνοι είναι μόνο ενδεχόμενα και όχι σίγουρα γεγονότα, επομένως μόνο αρκετά αργότερα μπορεί να εξακριβωθεί η αξία της ανάλυσης της επικινδυνότητας.

Σε μια νεώτερη δημοσίευση του ο **Charette** αναφέρει ότι η διαδικασία διαχείρισης τις επικινδυνότητας «δεν είναι τόσο εύκολη όσο φαίνεται» .Πρώτα από όλα η διαδικασία ανάλυσης υποθέτει ότι οι υποκειμενικές διαδικασίες απόφασης που χρησιμοποιούνται είναι λογικές. Από την άλλη όμως αυτό δεν συμβαίνει σχεδόν ποτέ, υπονοώντας ότι υπάρχει ένα κενό ανάμεσα στη διαδικασία και την πραγματικότητα. Οι αντιλήψεις, οι τάσεις πόλωσης, οι πολιτικές πρακτικές, αλλά και πολλά άλλα στοιχεία που προκύπτουν κάνουν την πραγματική διαδικασία απόφασης να μοιάζει παράλογη ή με έναν περίεργο τρόπο λογική.

Στη συνέχεια, απαιτείται η απόφαση σχετικά με το ποια μέθοδος ανάλυσης θα χρησιμοποιηθεί. Μια προσέγγιση από πάνω προς τα κάτω (top- down) θα έχει μια συμπερασματική αντίληψη της κατάστασης, ανακαλύπτοντας κινδύνους που αντιλαμβάνεται πιο συχνά η διοίκηση. Μια προσέγγιση από κάτω προς τα πάνω (bottom – up) θα προσφέρει μια επαγωγική αντίληψη, ανακαλύπτοντας κινδύνους που είναι περισσότερο εμφανής στους εργαζόμενους. Και οι δύο προσεγγίσεις είναι δυνατόν να χρησιμοποιούν την ίδια μέθοδο διαχείρισης της επικινδυνότητας, αλλά η οπτική γωνία, η σημαντικότητα και οι ενέργειες που απαιτούνται για την αποτροπή των κινδύνων είναι δυνατόν να διαφέρουν εκπληκτικά. Επιπλέον υπάρχει και το πρόβλημα που σχετίζεται με το πώς ο αναλυτής θα πετύχει τη συνεργασία με όλους όσους εμπλέκονται, οι οποίοι βλέπουν τον αναλυτή σαν ένα κατάσκοπο της διοίκησης ή σαν τον άνθρωπο που θα τους κατηγορήσει για κάθε μελλοντική αποτυχία. Η άποψη αυτή ευθυγραμμίζεται με τις απόψεις του CCTA για την διαχείριση της επικινδυνότητας σχετικά με την υπερνίκηση των εμποδίων σε επίπεδο προσωπικό, οργανωσιακό και πολιτιστικό.

Ένα άλλο ζήτημα σύμφωνα με τον Charette είναι το τι τελικά χαρακτηρίζεται ως κίνδυνος και τι ως πρόβλημα. Η διαμάχη ανάμεσα στον κίνδυνο και το πρόβλημα συνδέεται επίσης και με το τι αποφασίζεται να είναι ένα αποδεκτό επίπεδο επικινδυνότητας. Στη συνέχεια υπάρχει το θέμα του λάθους των υπολογισμών. Πως είναι δυνατόν να θέτει κάποιος πιθανότητες και συνέπειες σε κινδύνους που δεν έχουν προηγούμενη εμφάνιση; Για παράδειγμα θα πρέπει να αντιμετωπίζονται οι επιμέρους κίνδυνοι ως ανεξάρτητοι (κάνοντας εύκολα τα μαθηματικά τους) ή ως εξαρτημένοι μεταξύ τους;

Με παρόμοιο τρόπο **οι Kwok και Longley** καταγράφουν τα προβλήματα που αντιμετωπίζουν οι υπεύθυνοι ασφαλείας ανάμεσα στα οποία περιλαμβάνονται η δυσκολία να επιτευχθεί η πλήρης δέσμευση της ανώτερης διοίκησης.

Ο **Frosdick** πρεσβεύει ότι οι μέθοδοι ανάλυσης της επικινδυνότητας είναι ανεπαρκείς. Προτείνει έναν ορισμό της ανάλυσης της επικινδυνότητας, προτείνοντας ο όρος να αναφέρεται στο άθροισμα της αναγνώρισης της επικινδυνότητας (risk identification), την εκτίμηση (estimation) και την αποτίμηση (evaluation). Για κάθε στοιχείο, ο Frosdick σχολιάζει τα θέματα της αποδοτικότητας και εξάγει συμπεράσματα. Για τις τεχνικές αναγνώρισης της επικινδυνότητας αναφέρει ότι στηρίζονται σε μεγάλο βαθμό σε υστερινή πληροφόρηση, η οποία δεν έχει προλάβει ακόμα να γίνει γνωστή και σε καμία περίπτωση δεν μπορεί να προβλέψει τους μελλοντικούς κινδύνους που θα εμφανιστούν. Επιπλέον οι τεχνικές της εκτίμησης της επικινδυνότητας είναι ανεπαρκείς. Η αξιοπιστία των δεδομένων, πάνω στα οποία βασίζονται ποσοτικοποιημένες εκτιμήσεις, τίθεται σε αμφισβήτηση. Οι διαφορετικές εκφράσεις του ποσοτικοποιημένου κινδύνου έχουν επίδραση στον τρόπο με τον οποίο ο κίνδυνος γίνεται ακόλουθα αντιληπτός. Οι ισχυρισμοί των επιστημόνων για ουδέτερη αντικειμενικότητα στην εκτίμηση της επικινδυνότητας δεν μπορούν να στηριχθούν όταν η επικινδυνότητα είναι ένα υποκειμενικό κοινωνικό κατασκεύασμα .Στο ίδιο πνεύμα ο Frosdick καταλήγει ότι οι τεχνικές για την αποτίμηση της επικινδυνότητας οι οποίες δεν αντιμετωπίζουν την επικινδυνότητα ως ένα αθροιστικό κατασκεύασμα (collective construct),αποδεικνύονται ανεπαρκείς.

Όπως καταλήγει ο **Douglas και Wildavsky** , «η αποδεκτή επικινδυνότητα είναι θέμα κρίσης και τη σημερινή εποχή οι κρίσεις διαφέρουν σημαντικά. Ανάμεσα στην ιδιωτική, υποκειμενική αντίληψη και τη δημόσια, φυσική επιστήμη κείται μια κουλτούρα, μια μεσαία περιοχή από κοινά πιστεύω και αξίες. Η παρούσα υποδιαίρεση της ύλης (division of subject) που αγνοεί την κουλτούρα είναι αυθαίρετη και αυτό αναιρούμενη».

Πάνω σε αυτό το σημείο, ο **Rosa** αναφέρει ότι απομένει να γίνει πολύ ακόμα δουλειά μέχρι να γίνει κατανοητή η ανθρώπινη αντίληψη και οι αντιδράσεις σε σχέση μα αναγνωρισμένους κινδύνους. Ίσως, κυρίαρχο, ανάμεσα στα προβλήματα που αντιμετωπίζουν οι ερευνητές σχετικά με την επικινδυνότητα ,είναι ότι αυτή αποτελεί ένα αφηρημένο φαινόμενο, το οποίο μπορούμε να το δούμε είτε αντικειμενικά, σαν μια μετρήσιμη πραγματικότητα (positivism) ή υποκειμενικά σαν μια κοινωνικά κατασκευασμένη ιδέα (cultural relativism).

Η **Shrader – Frachette** επικρίνει αυτές τις ακραίες θέσεις και προτείνει να ακολουθηθεί μια μέση οδός την οποία αποκαλεί «scientific proceduralism».Η δουλειά που έχει γίνει στον τομέα της αντίληψης των κινδύνων, δείχνει πως διαφορετικοί παράγοντες εισέρχονται στην περιοχή λήψης απόφασης για τα άτομα και κατά κάποιο τρόπο εξηγεί το γιατί μπορεί να είναι δύσκολο να οριστεί με αριθμητικούς όρους η έννοια της αποδεκτής επικινδυνότητας (acceptable risk)

Οι **Dhillon και Backhouse** αναφέρουν ότι οι υποκειμενικές αρχές των προσεγγίσεων για την ασφάλεια των περισσοτέρων πληροφοριακών συστημάτων ανάλυσης της επικινδυνότητας και αυτών που βασίζονται σε αποτίμηση (evaluation based),απαριθμούνται ως εξής:

i. Οι οργανισμοί και τα πληροφοριακά συστήματα μελετώνται σε σχέση με αυστηρά όρια,τα οποία τα διαφοροποιούν μεταξύ τους αλλά και από το περιβάλλον.
ii. Τα πληροφοριακά συστήματα αλλά και η διαχείριση της ασφάλειας γίνονται αντιληπτά ως θέματα που έχουν φύση διαδικαστική (processual),κατά συνέπεια επικεντρώνονται στην είσοδο (input),ρυθμοαπόδοση (throughput) ,έξοδο (output),ανατροφοδότησης (feedback mechanisms).
iii. Οι οργανισμοί και τα πληροφοριακά τους συστήματα θεωρούνται ασφαλή, αν ικανοποιούνται οι ανάγκες των μοντέλων (υποσυστημάτων) δηλαδή, έχοντας ασφαλή υποσυστήματα μπορεί να επιτευχθεί η ασφάλεια του οργανισμού).
iv. Τα διαφορετικά μοντέλα (που υποβοηθούν στη προστασία τμημάτων ενός πληροφοριακού συστήματος) είναι αμοιβαία αλληλοεξαρτώμενα (mutually interdependent).
v. Η συνολική ασφάλεια μπορεί να επιτευχθεί αναλύοντας την συμπεριφορά των συνιστωσών ενός συστήματος.

Σύμφωνα με αυτούς τους ερευνητές το μεγαλύτερο μέρος της δουλειάς πάνω σε θέματα ασφαλείας –συγκρινόμενο με το μεγαλύτερο μέρος της έρευνας σε πληροφοριακά συστήματα – στηρίζεται στο διαδικαστικό παράδειγμα (functionalist paradigm), όπως αυτό αναλύεται στο πλαίσιο των Burrell και Morgan (1979).Συνεπώς οι διάφορες όψεις της ασφάλειας των πληροφοριακών συστημάτων αντιμετωπίζονται ως τελευταία σκέψη στο σχεδιασμό του συστήματος, την ανάπτυξη και την υλοποίηση.

Οι **Dhillon και Blackhouse** καταλήγουν ότι είναι πραγματικά χρήσιμο να εξεταστούν όλες οι φιλοσοφικές απόψεις και να γίνουν κατανοητά τα δυνατά σημεία και οι αδυναμίες τους,στην περίπτωση που τα θέματα ασφαλείας θα πρέπει να αντιμετωπιστούν με τρόπο ολιστικό.

Στην ίδια κατεύθυνση ο **White** ευθυγραμμίζεται με την κριτική που γίνεται μέσα από τις αρχές i,ii,v των προηγούμενων ερευνητών. Σύμφωνα με τον White οι περισσότερες προσεγγίσεις βασίζονται **στην αρχή του «διαίρει και βασίλευε».**Η άποψη αυτή παρουσιάζει πολλά πλεονεκτήματα, παρέχει μια αυστηρή δομή που βοηθάει στο να τίθεται σε σειρά η πραγματογνωμοσύνη (collate expertise) σε διαφορετικές πλευρές του προβλήματος, κάνει ρητή τη λογική που ακολουθείται στο συλλογισμό και διευκολύνει την εποικοδομητική κριτική. Παρόλα αυτά η αρχή της υπεραπλούστευσης (reductionist expertise) αποτυγχάνει στο να θεωρήσει ότι τα ατυχήματα και οι αποτυχίες είναι «αναδυόμενες ιδιότητες (emergent principles) » που προκύπτουν από «ολόκληρα συστήματα (whole systems)».Αυτό σημαίνει ότι αποτυγχάνει στο να αντιληφθεί πως οι διαφορετικές πλευρές ενός συστήματος αλληλεπιδρούν και υποτιμά τις περιβαλλοντικές επιπτώσεις.

Επίσης οι **Caelli et al** παραδέχονται ότι τα όρια της ανάλυσης της επικινδυνότητας είναι ασαφή και επιπλέον προσθέτουν ότι μια από τις κύριες αιτίες αποτυχίας της είναι η δυσκολία να οριστούν τα περιουσιακά στοιχεία και να εξασφαλιστεί ότι εξετάστηκαν όλες οι δυνατές απειλές σε ένα συγκεκριμένο περιβάλλον.

Οι **Halliday et al** πιστεύουν ότι οι οργανισμοί που εφαρμόζουν συμβατική ανάλυση και διαχείριση της επικινδυνότητας αντιμετωπίζουν ένα πλήθος δυσκολιών. Το «συμβατικό» αναφέρεται σε αυτές τις μεθόδους που βασίζονται στο παραδοσιακό μοντέλο «περιουσιακό στοιχείο- απειλή-αδυναμία».Σύμφωνα με τους συγγραφείς αυτές οι αναλύσεις της επικινδυνότητας έχουν την τάση να είναι χρονοβόρες. Επίσης εξαιτίας του γεγονότος ότι πολλές από αυτές τις μεθόδους αναπτύχθηκαν αρχικά με στόχο να ικανοποιήσουν τις ανάγκες σε ασφάλεια μεγάλων οργανισμών (στρατιωτικοί, κυβερνητικοί οργανισμοί), είναι δύσκολο να προσαρμοστούν στις ανάγκες μικρότερων οργανισμών χωρίς να υπάρχει κάποια γνώση και πραγματογνωμοσύνη. Αυτή η τελευταία απαίτηση σύμφωνα πάντα με τους συγγραφείς συχνά υποεκτιμάτε. Εναλλακτικά **προτείνουν μια εταιρική προσέγγιση που έχει σημείο εστίασης βασισμένο στην επιχείρηση (business oriented focus),**από την οπτική γωνία της τεχνολογίας πληροφοριών. Η προσέγγιση αυτή επικεντρώνεται στην επαγγελματική εξάρτηση (business dependence) αντί για την αδυναμία των υπολογιστικών συστημάτων. Επιπλέον, οι Halliday προτείνουν τη χρήση **«σεναρίων επικινδυνότητας» (risk scenario)** ώστε να ανακαλυφθούν οι κίνδυνοι.

Στο ίδιο πνεύμα και ο **Sommer** αναφέρει ότι το πλεονέκτημα της αναγνώρισης και δημιουργίας σεναρίων για ζημιά είναι ότι δίνει στα πιθανά θύματα μια περισσότερο λεπτομερή εικόνα των κινδύνων που αντιμετωπίζουν. Επίσης κάνει δυνατή την αφαίρεση πολλών χαμηλής πιθανότητας κινδύνων, έχοντας ως αποτέλεσμα τα αντίμετρα να είναι περισσότερο προσαρμοσμένα σε πραγματικές συνθήκες. Ο Sommer τονίζει τη χρησιμότητα αυτής της ευρετικής (heuristic) μεθόδου σε περιπτώσεις όπως η βιομηχανική κατασκοπία και παρουσιάζει τους περιορισμούς του υπολογιστικού (calculative) και checklist τύπου αναλύσεις της επικινδυνότητας.

Οι **McNamee και Selim** αναφέρουν ότι ο σχεδιασμός του σεναρίου (scenario planning) μπορεί να αποτελεί ένα εργαλείο για καλύτερη, μεγάλης κλίμακας, αποτίμηση της επικινδυνότητας (risk assessment) σε περιόδους σημαντικών αλλαγών. Τα σενάρια έχουν την δυνατότητα να συνδυάζουν ποιοτικά και ποσοτικά δεδομένα με ευφάνταστο τρόπο.

Τέλος ο **McName** υποστήριξε ότι ο σχεδιασμός του σεναρίου έχει μια ειδική χρήση και στη μικρής κλίμακας αποτίμηση της επικινδυνότητας στις περιοχές της απάτης, της διαχείρισης κρίσεων και καταστροφών .Χρησιμοποιώντας σενάρια για εξέταση της επικινδυνότητας λόγω της απάτης για παράδειγμα, ο εσωτερικός ελεγκτής μπορεί να διερευνήσει τις πηγές της απάτης πριν εμφανισθούν και στη συνέχεια, να αλλάξει τα μέτρα ασφαλείας ή το σχεδιασμό του συστήματος ,έτσι ώστε να αλλάξει την πιθανότητα εμφάνισης της απάτης.

3.2 Τα Πλεονεκτήματα της Διαχείρισης της Επικινδυνότητας

Ο **Lemieux** ισχυρίζεται ότι μια μέθοδος διαχείρισης της επικινδυνότητας (όπως η **CRAMM**) μπορεί να προσφέρει πολλά πλεονεκτήματα σε έναν οργανισμό. Η χρήση αυτής της μεθόδου εξασφαλίζει ότι κάποιος μέσα στον οργανισμό θα ασχοληθεί τουλάχιστον με την **αναγνώριση και αποτίμηση (valuation)** μερικών

στοιχείων του πληροφοριακού συστήματος (φυσικά περιουσιακά αγαθά όπως υπολογιστές, πληροφορικά αγαθά) και την αναγνώριση ορισμένων δυνατών απειλών και αδυναμιών. Όλοι οι οργανισμοί που ενδιαφέρονται για την ασφάλεια των πληροφοριών θα απαιτούν αργά ή γρήγορα μια τέτοιου είδους απογραφή και η δυνατότητα να πραγματοποιηθεί με ένα δομημένο τρόπο θεωρείται μια θετική συνεισφορά. Καθώς η μέθοδος υποχρεώνει το χρήστη να αξιολογήσει, τουλάχιστον ποιοτικά, τη σοβαρότητα των αναγνωρισμένων απειλών και αδυναμιών, μπορεί ακόμα να βοηθήσει στο να εστιάσει την ανάπτυξη αντιμέτρων για περισσότερο ευαίσθητα στοιχεία του συστήματος.

Ο **Pfleeger** ισχυρίζεται ότι ένα από τα σημαντικότερα πλεονεκτήματα της ανάλυσης της επικινδυνότητας είναι ότι **βελτιώνει την ενημερότητα (awareness).**Η συζήτηση γύρω από θέματα ασφαλείας μπορεί να ανεβάσει το γενικό επίπεδο του ενδιαφέροντος ανάμεσα στους εργαζομένους ,ενώ επιπλέον, η ανάλυση της επικινδυνότητας μπορεί να δικαιολογεί δαπάνες για την ασφάλεια και να βελτιώνει τη βάση των αποφάσεων.

Στο ίδιο πνεύμα ο **Frosdick** καταλήγει ότι παρόλο που οι μέθοδοι ανάλυσης της επικινδυνότητας παρουσιάζουν πολλούς περιορισμούς, είναι απαραίτητες για να εξασφαλίζουν ότι οι διαδικασίες λήψης αποφάσεων της διαχείρισης της επικινδυνότητας στηρίζονται σε επιστημονική πληροφόρηση.

Οι **Eloff et al** συνοψίζοντας το ρόλο της ανάλυσης της επικινδυνότητας για την ασφάλεια των πληροφοριών, τονίζουν ότι η ανάλυση της επικινδυνότητας **αποτελεί προαπαιτούμενο όχι μόνο για την δημιουργία μιας πολιτικής ασφαλείας πληροφοριών αλλά και τη βήμα προς βήμα εκλέπτυνση μια πολιτικής για την ανάπτυξη ενός πλάνου προστασίας προς υλοποίηση.** Επιπρόσθετα η ανάλυση της επικινδυνότητας είναι δυνατόν να χρησιμοποιηθεί ως μηχανισμός για την επίτευξη της ανάμιξης της ανώτερης διοίκησης στη διαχείριση της επικινδυνότητας. Τέλος αναφέρουν ότι μέσα από την χρήση της ανάλυσης της επικινδυνότητας είναι δυνατόν να αποκτηθεί η απαραίτητη γνώση για την ανάπτυξη ενός οικονομικά αποδοτικού πλάνου ασφαλείας.

3.3 Εργαλεία Υποστήριξης της Ανάλυσης και Διαχείρισης της Επικινδυνότητας

Μέχρι σήμερα έχουν αναπτυχθεί και είναι διαθέσιμες πληθώρα μεθόδων ανάλυσης και διαχείρισης της επικινδυνότητας, οι περισσότερες από τις οποίες έχουν αποτελέσει τη βάση για την ανάπτυξη αντίστοιχων εργαλείων. Η χρήση τέτοιων εργαλείων κρίνεται ιδιαίτερα σημαντική, καθώς χρησιμοποιούνται στις περισσότερες περιπτώσεις για την πραγματοποίηση του υπολογιστικού μέρους μιας μεθόδου και τη διαδοχική εφαρμογή των βημάτων της διαχείρισης της επικινδυνότητας, αποτελώντας στην ουσία ένα σύστημα στήριξης αποφάσεων, το οποίο υποβοηθά σε μεγάλο βαθμό το έργο του χρήστη που προσπαθεί να υπολογίσει τη συνολική επικινδυνότητα ενός συστήματος, προκειμένου στη συνέχεια να λάβει ίσως μέτρα για τον περιορισμό της.

3.4 Πλεονεκτήματα των Εργαλείων

Σε αντιπαραβολή με την μη αυτόματη μέθοδο ανάλυσης της επικινδυνότητας της οποίας η ολοκλήρωση απαιτεί μήνες, ένα εργαλείο αποτιμά τα αδύνατα σημεία ενός συστήματος σε σημαντικά μικρότερο χρόνο. Η ανάλυση είναι δυνατόν να γίνει αρκετά γρήγορα ώστε να εξασφαλιστεί ότι τα αποτελέσματα δεν έχουν απαρχαιωθεί εξαιτίας αλλαγών που έχουν συμβεί στο σύστημα.

Επιπλέον οι αυτοματοποιημένες διαδικασίες –πέρα από την περιοδική επιθεώρηση- **επιτρέπουν την κεντρική διαχείριση και τον έλεγχο της σύνθεσης και της υλοποίησης των έργων αποτίμησης της επικινδυνότητας**. Τα έργα αυτά καταλήγουν σε περισσότερο προτυποποιημένες προσεγγίσεις για την αποτίμηση της θέσης ενός οργανισμού όσον αφορά την ασφάλεια ειδικά σε εκτεταμένα, κατανεμημένα περιβάλλοντα με πολλαπλά υποδίκτυα και φυσικές τοποθεσίες.

Τέλος η ανάλυση και η διαχείριση της επικινδυνότητας η οποία πραγματοποιείται με τη βοήθεια ενός εργαλείου, **είναι δυνατό να αποτελέσει ένα εξαιρετικό βοήθημα σχεδιασμού (planning) της ασφάλειας των πληροφοριακών συστημάτων μια επιχείρησης ή ενός οργανισμού,** επιτρέποντας στο χρήστη να δοκιμάσει πολλά σενάρια **«what – if»**,προσομοιώνοντας τα αποτελέσματα της επιλογής διαφορετικών αντιμέτρων. Κατά συνέπεια θα πρέπει να επιτρέπει στο χρήστη να διαλέξει τα πιο αποτελεσματικά μέσα προστασίας με το μικρότερο κόστος.

3.5 Εδικοί Περιορισμοί των Εργαλείων

Τα εργαλεία ανάλυσης της επικινδυνότητας είναι δυνατόν να προκαλέσουν διάφορα είδη προβλημάτων. Μπορεί **να παρασύρουν κάποιον στο να σκεφτεί ότι οι αριθμοί που λαμβάνει είναι σωστοί,** όταν στην πραγματικότητα αυτοί που παράγονται ως ακριβείς να είναι λανθασμένοι. Επίσης βοηθούν στην **ανάλυση καταστάσεων πριν γίνουν πλήρως κατανοητές**, έτσι δίνουν αυτοπεποίθηση στον αναλυτή χωρίς στην ουσία να αξίζει, κάνοντας τον να φαντάζεται ότι μοντελοποιεί την πραγματικότητα ενώ μοντελοποιεί μια διαστρεβλωμένη εικόνα της πραγματικότητας.

Όσο οι χρήστες αποκτούν εμπειρία σε ένα εργαλείο ανάλυσης της επικινδυνότητας , **υπάρχει ο κίνδυνος να υιοθετήσουν μια μηχανιστική προσέγγιση στην ανάλυση**, εισάγοντας ίσως δεδομένα στα τυφλά και με απερισκεψία.

Έτσι η χρήση αυτοματοποιημένων μεθόδων, μειώνει την ανθρώπινη διαίσθηση και δημιουργικότητα, γεγονός που μπορεί να οδηγήσει στην επιλογή λιγότερο οικονομικών και αποδοτικών αντιμέτρων.

3.6 Κριτική εργαλείων ανάλυσης και διαχείρισης της επικινδυνότητας

Το να προχωρήσει κάποιος στην επιλογή της καταλληλότερης μεθόδου και του σωστού εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας για ένα συγκεκριμένο περιβάλλον και τις ανάγκες μιας επιχείρησης ή ενός οργανισμού, αποτελεί μια πολύ σημαντική κα καθόλου εύκολη υπόθεση. Ανάμεσα στους παράγοντες που δυσχεραίνουν μια τέτοια επιλογή είναι και οι ακόλουθοι:

- Δεν υπάρχει ένα κοινά αποδεκτό σύνολο κριτηρίων αξιολόγησης για τις μεθόδους.
- Κάποιες μέθοδοι καλύπτουν μόνο τμήματα της όλης διαδικασίας της διαχείρισης της επικινδυνότητας.
- Οι μέθοδοι διαφέρουν πολύ στο επίπεδο ανάλυσης με την έννοια ότι κάποιες χρησιμοποιούν υψηλού επιπέδου περιγραφές του πληροφοριακού συστήματος που μελετούν, ενώ κάποιες άλλες απαιτούν λεπτομερειακές περιγραφές.
- Δεν υπάρχει διαθέσιμος πλήρης κατάλογος με τα ιδιαίτερα χαρακτηριστικά όλων των μεθόδων, ενώ κάποιες από αυτές δεν διατίθενται στην ελεύθερη αγορά, γεγονός που καθιστά την αξιολόγηση τους εξαιρετικά δύσκολη.

Αναγνωρίζοντας την ύπαρξη αυτών των δυσκολιών και την σημασία της ανάπτυξης μιας ομογενοποιημένης μεθόδου διαχείρισης της επικινδυνότητας, η Ευρωπαϊκή Επιτροπή ανέθεσε με τη μορφή έργου την καταγραφή και αξιολόγηση των διαθέσιμων μεθόδων και εργαλείων. Με βάση τα αποτελέσματα αυτής της έρευνας (INFOSEC,1992) θα επιχειρηθεί στη συνέχεια μια κριτική παρουσίαση των συμπερασμάτων.

Είδη υπαρχόντων εργαλείων

Είναι δυνατό να διακρίνει κάποιος διάφορες κατηγορίες εργαλείων με βάση την κάλυψη τομέων εφαρμογής που παρέχει το καθένα, το είδος της πλατφόρμας(δηλαδή τον συνδυασμό του υλικού και λογισμικού σε σχέση με το υπολογιστικό σύστημα) στην οποία μπορεί το εργαλείο να εκτελεστεί, καθώς και το βαθμό εμπειρίας που απαιτείται για τη χρήση του, αλλά και την έκταση της κάθε μεθόδου, δηλαδή σε ποιες φάσεις και σε τι είδους συστήματα(υπολογιστικά συστήματα)καθώς και σε ποιου είδους ηλεκτρονικούς υπολογιστές, τοπικά δίκτυα, μητροπολιτικά δίκτυα, δίκτυα φωνής μπορεί να εφαρμοστεί. Πιο αναλυτικά:

- Σε ότι αφορά τον τομέα εφαρμογής τους,τα περισσότερα εργαλεία από αυτά που περιλαμβάνονται στη σχετική έρευνα αναφέρουν ένα ευρύ φάσμα περιοχών χρησιμοποίησης τους, ενώ από τα υπόλοιπα, δύο καλύπτουν λιγότερους τομείς από ότι τα πρώτα(κάποιο υποσύνολο του συνόλου των τομέων και κλάδων), δύο εστιάζονται σε οικονομικούς τομείς(τραπεζικοί ,ασφαλιστικοί, χρηματοοικονομικοί) και δύο δεν αναφέρουν κανένα τομέα.

- Η πλατφόρμα λειτουργίας της πλειοψηφίας των εργαλείων είναι ένας προσωπικός υπολογιστής, ενώ αναφέρεται ένα εργαλείο που λειτουργεί σε περιβάλλον UNIX και ένα ακόμα σε υπολογιστή τεχνολογίας MAC.Επιπρόσθετα κάποια εργαλεία απαιτούν την εγκατάσταση και κάποιου λογισμικού υποστήριξης (βάση δεδομένων, κειμενογράφο κλπ.)

- Συχνά η εμπειρία που έχουν οι χρήστες σε σχέση με θέματα ασφαλείας και ειδικότερα στην ανάλυση και διαχείριση της επικινδυνότητας προκειμένου να χρησιμοποιήσουν ένα εργαλείο, αποτελεί ένα σημαντικό παράγοντα για την επιλογή ενός εργαλείου. Αρκετά από τα διαθέσιμα εργαλεία απαιτούν οι χρήστες να είναι εξειδικευμένοι ή να έχουν λάβει κάποια εκπαίδευση σχετική με το εργαλείο, ενώ ένα ικανό πλήθος αυτών εργαλείων απαιτεί μικρή ή καθόλου εμπειρία των χρηστών.

- Σε σχέση με την έκταση της μεθόδου από την πλευρά των φάσεων ανάπτυξης διαπιστώνεται ότι για τα περισσότερα εργαλεία αναφέρεται ότι μπορούν να χρησιμοποιηθούν στις τέσσερις φάσεις του κύκλου ζωής (προμελέτη, μελέτη ,υλοποίηση, λειτουργία) ενώ τα υπόλοιπα μόνο σε συγκεκριμένες φάσεις. Επιπρόσθετα σε ότι αφορά τα είδη συστημάτων τα οποία καλύπτει η κάθε μέθοδος, η πλειονότητα τους πρεσβεύει ότι μπορεί να χειριστεί όλα τα είδη συστημάτων.

Βήματα της ανάλυσης και της διαχείρισης της επικινδυνότητας όπου βοηθούν τα εργαλεία

Έχοντας υπόψη τα βήματα της διαδικασίας της ανάλυσης και της διαχείρισης της επικινδυνότητας, όπως αυτά περιγράφηκαν σε προηγούμενη παράγραφο, και με βάση τα στοιχεία που συγκεντρώθηκαν στα πλαίσια της έρευνας, διαπιστώνει κάποιος ότι τα διαθέσιμα εργαλεία καλύπτουν κυρίως τα βήματα της ανάλυσης της επικινδυνότητας θεωρώντας ότι έτσι καλύπτεται γενικότερα και η διαχείριση της επικινδυνότητας.

- Η πλειοψηφία των εργαλείων **παρέχουν κάλυψη για τις περισσότερες από τις επιλεγμένες ομάδες περιουσιακών στοιχείων** (υλικό, firmware, επικοινωνίες, περιβάλλον, λογισμικό συστήματος, λογισμικό εφαρμογών, συστήματα διαχείρισης βάσεων δεδομένων, αυτοματισμό γραφείου, δεδομένα – πληροφορίες, διαδικασίες, επιχειρηματικές λειτουργίες, τεκμηρίωση, ανθρώπους ,χρήματα, ακίνητα).

- Η πλειοψηφία των εργαλείων **συνεισφέρει στον εντοπισμό αδυναμιών και απειλών που σχετίζονται με ατυχήματα** (υλικό, αστοχίες, φυσικά ατυχήματα, απώλεια υπηρεσιών),με λάθη (λογικά, σχεδίασης) και με κακόβουλες επιθέσεις όπως κλοπή, απάτη, δολιοφθορά, ιούς,hacking, κατάχρηση πόρων),ενώ οι μέθοδοι που ως επί το πλείστον χρησιμοποιούνται για την μέτρηση τους είναι εξίσου ποιοτικές(αδυναμίες, απειλές) και ποσοτικές και λιγότερο πιθανολογικές.

Ο υπολογισμός της ζημιάς γίνεται στις περισσότερες περιπτώσεις σε σχέση με τις έννοιες της **διαθεσιμότητας, εμπιστευτικότητας** (εσωτερικής, εξωτερικής)**,ακεραιότητας** (τυχαίας, σκόπιμης) και **καταστροφής των αγαθών** και οι **μετρικές** που χρησιμοποιούνται είναι ποιοτικές και ποσοτικές .Επίσης, ποσοτικές και ποιοτικές είναι οι μέθοδοι που χρησιμοποιούνται και για τη μέτρηση της συνολικής επικινδυνότητας ενός συστήματος, ενώ σε ελάχιστες περιπτώσεις αυτή γίνεται και πιθανολογικά.

Τέλος η συντριπτική πλειοψηφία των μεθόδων προχωρά στην **πρόταση αντιμέτρων** (φυσικά, προσωπικά, για το υλικό, για το λογισμικό, τις επικοινωνίες, διαδικασίες, οργανωτικά,Tempest) ενώ τα περισσότερα εργαλεία κάνουν και μια δικαιολόγηση της ασφάλειας που αυτά τα μέτρα ασφαλείας προσπαθούν να παρέχουν.

Κριτική των Εργαλείων

Μελετώντας κάποιος τα στοιχεία της έρευνας είναι δυνατό να οδηγηθεί σε ορισμένες παρατηρήσεις σχετικά με την ανάλυση και την διαχείριση της επικινδυνότητας και πως αυτή προσεγγίζεται από σχετικές μεθόδους και εργαλεία.

Σε μια πρώτη φάση κρίνεται ότι οι περισσότερες μέθοδοι κα κατ' επέκταση τα εργαλεία **δεν καταφέρνουν να επεκταθούν πολύ πιο πέρα από το πλαίσιο και τις ανάγκες ενός συγκεκριμένου τομέα** – αν και προβάλλονται ως εργαλεία γενικής χρήσης- η μελέτη του οποίου συνήθως αποτελεί έναυσμα για την δημιουργία τους.Είναι γεγονός ότι η ανάπτυξη πολλών εργαλείων ξεκινά σχεδόν πάντα από την αδυναμία των προϋπαρχόντων εργαλείων να αντιμετωπίσουν τις ιδιαίτερες ανάγκες που παρουσιάζει η προσπάθεια να προσδιοριστεί η επικινδυνότητα του πληροφοριακού συστήματος μιας επιχείρησης ή ενός οργανισμού. Τη δημιουργία μιας νέας και προσαρμοσμένης μεθόδου και του εργαλείου που την ενσωματώνει, ακολουθούσε η επιθυμία των δημιουργών να εκμεταλλευθούν εμπορικά το προϊόν τους. Και είναι σαφές ότι όσο πιο γενικής χρήσης θα μπορούσε να παρουσιαστεί ότι είναι το εργαλείο, τόσο μεγαλύτερη θα είναι η εμπορευσιμότητα του.

Ένα άλλο χαρακτηριστικό των μεθόδων και των εργαλείων τους είναι ότι εκτός από τι γεγονός ότι δεν γίνεται σοβαρή προσπάθεια αυτά να ανταποκρίνονται με όσο τον δυνατόν καλύτερο τρόπο στον γενικό χαρακτήρα που επιδιώκουν να έχουν (σχετικά με τους τομείς και τους κλάδους των επιχειρήσεων) ,**παρουσιάζουν ελλείψεις και ως προς την προσαρμογή τους στα χαρακτηριστικά διαφόρων αγορών και διαφορετικών τύπων κουλτούρας.**

Επιπλέον τα εργαλεία που έχουν αναπτυχθεί μέχρι αυτή τη στιγμή **δεν φαίνεται να έχουν ως αφετηρία για τη μέθοδο τους κάποιο πρότυπο,** όμως αυτό είναι ως ένα βαθμό αναμενόμενο, εφόσον ο χώρος της ανάλυσης και της διαχείρισης της επικινδυνότητας είναι σχετικά νέος, τα περισσότερα από αυτά αναπτύχθηκαν για να καλύψουν τρέχουσες ανάγκες και συμβαίνει οι πιο αποτελεσματικές μέθοδοι να ξεπηδούν μέσα από αρκετή εμπειρία και ωρίμανση της σχετικής γνώσης. Απόρροια της ανωριμότητας των εργαλείων είναι το γεγονός ότι

ενώ τα περισσότερα εργαλεία αναφέρουν ότι καλύπτουν για παράδειγμα, τη φάση της ανάλυσης των αδυναμιών και απειλών ενός συστήματος, φαίνεται ότι παραλείπουν κάποιες από αυτές που κατ' ελάχιστο θα αναμένονταν να καλύπτονται από όλα τα εργαλεία.

Εξετάζοντας την επιλογή να αναπτυχθούν εργαλεία τα οποία θα ήταν δυνατό να χρησιμοποιηθούν ακόμα και από άπειρους σε σχέση με το αντικείμενο χρήστες, διαπιστώνεται ότι ενδέχεται αυτή (η επιλογή) να αποτελεί **τροχοπέδη στην ανάπτυξη μιας αποτελεσματικής μεθόδου ανάλυσης και διαχείρισης της επικινδυνότητας αλλά και στην αποδοτική εκμετάλλευση των αποτελεσμάτων ενός τέτοιου εργαλείου.** Η έννοια του τελευταίου επιχειρήματος είναι ότι ένα μη ειδικός σε θέματα ασφαλείας ή και ανάλυσης και διαχείρισης της επικινδυνότητας είναι δυνατό να μη μπορεί να αιτιολογήσει με τον καλύτερο τρόπο την αναγκαιότητα εφαρμογής αντιμέτρων (και κατά συνέπεια της σχετικής δαπάνης) προς τη διοίκηση ενός οργανισμού ή μιας επιχείρησης ,ή να προωθήσει μέσα σε αυτή θέματα ασφαλείας. Επιπλέον θεωρείται ότι η αναφορά για την χρησιμοποίηση του εργαλείου από μη ειδικευμένους χρήστες υπαινίσσεται κάποιου είδους ικανότητα του εργαλείου να πραγματοποιεί, σε αντιδιαστολή με το να υποστηρίζει, ανάλυση και διαχείριση της επικινδυνότητας, υπαινιγμός ο οποίος κρίνεται ότι δεν είναι εφικτός στα μέτρα των παρόντων εξελίξεων της τεχνολογίας των πληροφοριών.

Πέρα από τις παρατηρήσεις αυτές, αναφέρεται ότι οι μέθοδοι ανάλυσης και διαχείρισης της επικινδυνότητας χρησιμοποιούν σχετικά απλές **στατιστικές τεχνικές, οι οποίες χαρακτηρίζονται από έλλειψη βάθους και ενδογενή μειονεκτήματα.** Όσον αφορά το σχόλιο ότι είναι απλουστευτικές, αυτό προκύπτει από το ότι στη προσπάθεια να αποφευχθεί η πολυπλοκότητα που συνοδεύει την αυστηρή πιθανή μοντελοποίηση κινδύνων και αβεβαιότητας, η ανάλυση και η διαχείριση της επικινδυνότητας μετατρέπεται σε μέθοδο που προσπαθεί να μαντέψει. παρά να προβλέψει φορμαλιστικά, βάση στατιστικών δεδομένων και παρατηρήσεων. Επιπλέον ο σημαντικότερος λόγος της κριτικής σχετικά με την ισχυριζόμενη έλλειψη βάθους φαίνεται να είναι ,ότι δεν παρέχεται από τις μεθόδους η δυνατότητα ανατροφοδότησης (feedback) των αποτελεσμάτων της προδιαγραφής, της σχεδίασης και της υλοποίησης των αντιμέτρων που προτείνει.

Συμπεράσματα

Συμπερασματικά οι **μέθοδοι** και τα **εργαλεία ανάλυσης και διαχείρισης της επικινδυνότητας έχουν σημαντική συνεισφορά στον τομέα της επικοινωνίας θεμάτων και προβληματισμών που αφορούν την ασφάλεια των πληροφοριακών συστημάτων προς την διοίκηση μιας επιχείρησης ή ενός οργανισμού.** Παρόλα αυτά είναι δύσκολο να παραβλέψει κανείς τις αδυναμίες και την ανωριμότητα που αυτά παρουσιάζουν αν και αυτή είναι δυνατόν να δικαιολογηθεί ως ένα βαθμό, από τη σχετικά μικρή πορεία που έχουν διανύσει μέσα στο χώρο της ασφάλειας των πληροφοριακών συστημάτων. Ωστόσο η πορεία είναι αρκετή ώστε μια ομάδα ανθρώπων να έχει την κατάλληλη εμπειρία και να έχει συγκεντρώσει αρκετό υλικό γύρω από διάφορα θέματα ασφαλείας πληροφοριακών συστημάτων αλλά και ανάλυσης και διαχείρισης της επικινδυνότητας, καθιστώντας δυνατό το να μπορεί να συνεισφέρει στην ανάπτυξη μιας νέας μεθόδου – εργαλείου

της ανάλυσης και της διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων.

ΚΕΦΑΛΑΙΟ 4

ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΣΤΡΑΤΗΓΙΚΗΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥ ΘΕΜΑΤΟΣ

Στα πλαίσια της επιλογής μιας στρατηγικής η οποία θα καταλήγει στην ανάπτυξη ενός εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας ορισμένα από τα χαρακτηριστικά του οποίου περιγράφηκαν σε προηγούμενο κεφάλαιο, εξετάστηκαν οι σημαντικότερες ομάδες μεθοδολογιών οι οποίες εφαρμόζονται για την ανάπτυξη πακέτων λογισμικού. Οι ομάδες αυτές αποτελούνται από μεθοδολογίες που ακολουθούν τη δομημένη προσέγγιση, την αντικειμενοστρεφή και την τεχνική κατασκευής προτύπου (prototyping).

Στη συνέχεια θα περιγράφούν τα βασικά χαρακτηριστικά καθώς και ορισμένα πλεονεκτήματα και μειονεκτήματα κάθε μιας ομάδας, ώστε να προσδιοριστεί τελικά η προσέγγιση η οποία ανταποκρίνεται με τον αποτελεσματικότερο τρόπο στην ανάπτυξη του εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων.

4.1 Δομημένη Προσέγγιση

Αναφερόμενος κάποιος στις μεθοδολογίες της δομημένης προσέγγισης, θα έλεγε ότι αυτές χαρακτηρίζονται από τέσσερις θεμελιώδης αρχές:

a) Την αρχή της αφαίρεσης (abstraction) ,η οποία συνιστά την απλοποίηση των πραγμάτων διατηρώντας αυτά που θεωρούνται περισσότερο σημαντικά και βλέποντας τα μέσα από διαφορετικά επίπεδα σημαντικότητας,

b) Της αυστηρής τυπικότητας (formality) ,που δίνει έμφαση στην αυστηρή βήμα προς βήμα εφαρμογή των διαδικασιών ,

c) Του διαίρει και βασίλευε (divide and conquer) η οποία κάνει αναφορά στην κλασική πρακτική του τεμαχισμού σε μικρότερα πιο προσιτά προβλήματα και

d) Της δημιουργίας μιας ιεραρχικής δομής (hierarchical ordering)

Στην κατηγορία αυτή υπάγονται πάρα πολλές μεθοδολογίες οι πλέον γνωστές εκ των οποίων είναι η SSADM, Yourdon DeMacro,Information Engineering,MERISE,STRADIS κ.α.

Ανάμεσα στα [illegible] των μεθοδολογιών αναφέρονται η αποδοτικότητα τους στο να αποτυπώνονται με σαφή, περιεκτικό, οικονομικά αποδοτικό και πλήρη τρόπο οι απαιτήσεις ενός συστήματος, η ικανοποιητική βοήθεια που είναι δυνατό

να παρέχουν στη συντηρησιμότητα του, η μεγάλη εμπειρία που υπάρχει από την πολύχρονη εφαρμογή τους, ενώ από την άλλη μεριά αναφέρεται ότι είναι αρκετά δύσκολη η εφαρμογή τους σε περιβάλλοντα υψηλής πολυπλοκότητας και συστήματα μεγάλης κλίμακας, ενώ αντιμετωπίζουν το χρήστη όχι τόσο σαν συνεργάτη όσο σαν διάδοχο – εντολέα του έργου ανάπτυξης ενός συστήματος γεγονός που μπορεί να συνεισφέρει στην προβληματική ανάπτυξη του ,ιδιαίτερα αν η ομάδα ανάπτυξης δεν έχει την απαραίτητη εμπειρία για να ξεπεράσει τα εμπόδια που ενδεχομένως θα εμφανιστούν.

4.2 Ανικειμενοστρεφής Προσέγγιση

Οι μεθοδολογίες της αντικειμενοστραφούς προσέγγισης αντιλαμβάνονται τα συστήματα μέσα από την χρήση των εννοιών:

i. Του αντικειμένου, δηλαδή της λογικής οντότητας η οποία συνδυάζει δεδομένα και διαδικασίες,

ii. Των μεθόδων, των πράξεων που εκτελεί ένα αντικείμενο όταν λαμβάνει ένα μήνυμα και των μηνυμάτων που στέλνει ένα αντικείμενο σε ένα άλλο ώστε το τελευταίο να εκτελέσει μια λειτουργία.

Επιπρόσθετα εφαρμόζουν τις ιδιότητες:

1. **Της ενσωμάτωσης (encapsulation)**, εννοώντας τη συγκέντρωση δεδομένων και πράξεων στην ίδια δομή με στόχο την απόκρυψη των εσωτερικών λεπτομερειών της υλοποίησης,
2. **Της τμηματοποίησης (modularity)** η οποία αναφέρεται στον χωρισμό των πολύπλοκων συστημάτων σε ενότητες (modules),
3. **Της αφαίρεσης (abstraction)** και
4. **Του πολυμορφισμού (polymorphism),** της ιδιότητας δηλαδή να στέλνεται το ίδιο μήνυμα σε διαφορετικά αντικείμενα και το καθένα να εκτελεί μια λειτουργία που αντιστοιχεί στην τάξη που ανήκει.

Μέσα από τις διάφορες μεθοδολογίες που έχουν αναπτυχθεί εισάγονται αρκετές ακόμα έννοιες (όπως κλάσεις, όψεις, ιεραρχίες, κληρονομικότητα κτλ), ενώ πρέπει να σημειωθεί ότι οι μεθοδολογίες αυτές θεωρούνται γενικά ότι βρίσκονται σε φάση διαμόρφωσης. Ανάμεσα στις πιο γνωστές από αυτές βρίσκονται η μεθοδολογία του Coad καιYourdon,η Object Modeling Technique (OMT), η OOAD(Object Oriented Analysis and Design) κ.α.

4.3 Τεχνική Κατασκευής Προτύπου

Η τεχνική κατασκευής προτύπου είναι η διαδικασία της γρήγορης ανάπτυξης ενός μοντέλου η οποία γίνεται προσπάθεια να απεικονίζει όσο γίνεται περισσότερο την πραγματικότητα. Μερικά από τα θέματα που διερευνώνται σε σχέση με τη χρήση αυτής της τεχνικής είναι η ανακάλυψη των πραγματικών αναγκών των χρηστών μέσα από την δυνατότητα ανάκλησης των φάσεων, τον πειραματισμό με εναλλακτικούς σχεδιασμούς αλλά και η αποτίμηση της απόδοσης του συστήματος.

Ανάμεσα στα πλεονεκτήματα της τεχνικής δημιουργίας προτύπου αναφέρονται η δημιουργία κινήτρου στους χρήστες με τη συμμετοχή τους στην ανάπτυξη ενός

συστήματος, παρέχοντας έτσι τις πλέον αξιόπιστες πληροφορίες σχετικά με τις απαιτήσεις του και η εξουδετέρωση σε ένα βαθμό της ακαμψίας και της αυστηρότητας του κύκλου ζωής των συστημάτων. Επιπλέον επιτρέπει τον προσδιορισμό και την αξιολόγηση των προδιαγραφών του συστήματος μέσα από την διενέργεια πειραμάτων σε ένα σύστημα με στόχο τη μείωση και τον έλεγχο της αβεβαιότητας του προβλήματος ή της αβεβαιότητας των συνεπειών.

4.4 Συμπεράσματα Σχετικά με τις Μεθόδους Ανάπτυξης ενός Πακέτου Λογισμικού

Οι παραπάνω προσεγγίσεις χρησιμοποιούνται και για την ανάπτυξη πληροφοριακών συστημάτων γενικότερα, αντιμετωπίζοντας η καθεμία το θέμα αυτό μέσα από τις δικές της δυνατότητες και χαρακτηριστικά. Η παρούσα όμως περίπτωση μελέτης αφορά ένα εργαλείο, μια εφαρμογή ή αλλιώς ένα πακέτο λογισμικού. Κατά συνέπεια αυτού του είδους η ανάπτυξη θα πρέπει να αντιμετωπιστεί από μια μεθοδολογία που να τη χειρίζεται με τον πιο αποτελεσματικό και αποδοτικό τρόπο.

Εξετάζοντας κάποιος τις παραπάνω μεθοδολογίες ως προς την καταλληλότητα τους για την ανάπτυξη εργαλείων – πακέτων λογισμικού, καταλήγει ότι δύο από αυτές ανταποκρίνονται καλύτερα στις απαιτήσεις για αυτό το είδος ανάπτυξης (δομημένη προσέγγιση και τεχνική κατασκευής προτύπου). Όσον αφορά την αντικειμενοστρεφή προσέγγιση, θεωρείται ότι δεν έχει αντιμετωπιστεί προς το παρόν με τρόπο ολοκληρωμένο από κάποια μεθοδολογία, παρόλο που φαίνεται ότι στα επόμενα χρόνια θα κυριαρχεί στις μεθοδολογίες ανάπτυξης λογισμικού και πληροφοριακών συστημάτων.

Ανάμεσα στις δύο προσεγγίσεις οι οποίες κρίνεται ότι εμπίπτουν στο πλαίσιο της ανάπτυξης του εργαλείου, σύμφωνα με τη δομημένη προσέγγιση, η ανάπτυξη των συστημάτων **βασίζεται σε μια διαρθρωμένη σε συγκεκριμένα βήματα μεθοδολογία,** ενώ η **τεχνική κατασκευής προτύπου αποτελεί μια διαδικασία γρήγορης ανάπτυξης ενός μοντέλου που απεικονίζει όσο το δυνατόν περισσότερο την πραγματικότητα**, με βάση το οποίο γίνεται σταδιακά η ανάπτυξη ,μέσα από αλλεπάλληλους κύκλους αναμόρφωσης και βελτίωσης τους.

Κατά την διαδικασία που ακολουθείται στη δομημένη προσέγγιση, οι φάσεις πρέπει να είναι **σειριακά διαδοχικές**, δηλαδή μια φάση να οδηγεί στην αμέσως επόμενη (ανάλυση, σχεδιασμός, υλοποίηση, έλεγχος, λειτουργία, συντήρηση). Το γεγονός αυτό προϋποθέτει ότι τα αποτελέσματα της μίας οδηγούν κατά τρόπο αναμφισβήτητο στην άλλη και επίσης ότι το προϊόν που παράγει έχει «παγώσει», δηλαδή έχει γίνει δεκτό και δεν μπορεί να αλλάξει αργότερα. Και παρόλο που είναι δυνατή η ανακύκλωση των φάσεων, μια τέτοια κατάσταση δεν είναι επιθυμητό να συμβαίνει κατά την ανάπτυξη ενός συστήματος.

Η τεχνική κατασκευής προτύπου από την άλλη μεριά, έχει ως βασικό χαρακτηριστικό την ανάπτυξη μέσα από **αλλεπάλληλους κύκλους βελτίωσης των φάσεων.** Με άλλα λόγια δεν επιζητείται η ολοκλήρωση και η παγίωση μιας φάσης,

ώστε να προχωρήσει κάποιος στην επόμενη αλλά η ολοκλήρωση τους επιτυγχάνεται μέσα από τη συνεχή ανακύκλωση τους.

Παρά τα πλεονεκτήματα που παρουσιάζει η τεχνική κατασκευής προτύπου σε σχέση με τη δομημένη προσέγγιση, κρίνεται πως ο παράγοντας **«φορέας ανάπτυξης του εργαλείου ανάλυσης και διαχείρισης της επικινδυνότητας»** είναι αυτός που θα επηρεάσει με καθοριστικό τρόπο τη μέθοδο ανάπτυξης που τελικά θα επιλεγεί. Με την προϋπόθεση ότι πρόκειται για ένα ακαδημαϊκό περιβάλλον και όχι μια εταιρεία που αναπτύσσει εφαρμογές λογισμικού για εμπορικούς σκοπούς, υποδεικνύει ότι προσπάθειες τέτοιες, όπως η ανάπτυξη ενός εργαλείου αρχικά εξετάζονται και προσαρμόζονται στις πρακτικές και τις συνήθειες που διέπουν τον χώρο αυτό. Στα πλαίσια αυτών των πρακτικών, με δεδομένη την προσπάθεια που απαιτείται για την ανάπτυξη του εργαλείου, θεωρείται ότι αυτή θα μπορούσε να πραγματοποιηθεί με τη μορφή εργασιών. Κάθε εργασία είναι δυνατό να διαπραγματεύεται μια από τις φάσεις ανάπτυξης όπως αυτές δίνονται στην δομημένη προσέγγιση.

4.5 Ο Κύκλος Ζωής Ενός Πακέτου Λογισμικού

Ένα πακέτο λογισμικού χαρακτηρίζεται από έναν κύκλο ζωής ο οποίος ορίζεται ως ο χρόνος από τη σύλληψη της ιδέας ανάπτυξης μέχρι την απόσυρση του. Προκειμένου να μπορεί κάποιος να επέμβει με σωστό τρόπο και να χειριστεί αποτελεσματικά τις μεθοδολογίες και τις τεχνικές ανάπτυξης του λογισμικού πρέπει να έχει γνώσει του τρόπου ανάπτυξης, λειτουργίας και απόσυρσης του. Για το λόγο αυτό έχουν προταθεί ορισμένα μοντέλα ανάπτυξης λογισμικού τα οποία περιγράφουν τη ζωή του λογισμικού κατά την διάρκεια ολόκληρου του κύκλου ζωής του. Μερικά από τα μοντέλα κύκλου ζωής που έχουν προταθεί είναι τα ακόλουθα:

Μοντέλο του Καταρράκτη(Waterfall model)

Το μοντέλο αυτό χωρίζει τον κύκλο ζωής του λογισμικού σε οκτώ φάσεις. Η σειρά των φάσεων είναι ακολουθιακή, δηλαδή μια φάση ξεκινά όταν ολοκληρωθεί η προηγούμενη της και κάθε φάση παράγει ένα ενδιάμεσο προϊόν χρήσιμο για την επόμενη φάση. Είναι περισσότερο αποτελεσματικό όταν χρησιμοποιείται σε συνδυασμό με τη μέθοδο «πάγωμα – ορόσημο». Από τα κύρια μειονεκτήματα του μοντέλου είναι ότι μαθαίνουμε τη γνώμη του πελάτη αφού έχει φτάσει η ανάπτυξη της κάθε φάσης στο τέλος της.Τέλος σημειώνεται ότι έχουν αναπτυχθεί πολλές παραλλαγές του μοντέλου ,οι γνωστότερες από τις οποίες είναι:

- Προσαύξηση λειτουργικής ικανότητας
- Το μοντέλο IEEE
- Το μοντέλο V

Μοντέλο Βηματικής Εκλέπτυνσης και Επαναληπτικής Προσαύξησης(stepwise refinement and iterative enhancement)

Το μοντέλο αυτό προσαυξάνει τις προδιαγραφές του συστήματος καθώς προσδιορίζει τις μονάδες πηγαίου κινδύνου.

Οι απαιτήσεις θα διατυπωθούν με τη βοήθεια διαγραμματικών κυρίως τεχνικών και άλλων εργαλείων που υποστηρίζουν την απρόσκοπτη επικοινωνία μεταξύ των εμπλεκομένων φορέων ενώ παράλληλα διαθέτουν και την απαιτούμενη αυστηρότητα για την ακρίβεια της περιγραφής.

Για τον προσδιορισμό των απαιτήσεων ,απαιτείται η χρήση μιας σχετικής μεθοδολογίας από το πλήθος των μεθοδολογιών που υπάρχουν.

ΦΑΣΗ 2:Σχεδιασμός του Συστήματος

Η διαδικασία του σχεδιασμού του συστήματος έπεται της τυποποίησης των αρχικών απαιτήσεων και προδιαγραφών του συστήματος, Ο σκοπός αυτής της φάσης είναι ο προσδιορισμός και η ενσωμάτωση των επιθυμητών χαρακτηριστικών στο νέο σύστημα. Επίσης στη φάση αυτή πραγματοποιείται ο σχεδιασμός των διεπαφών , των χαμηλού επιπέδου δομών, των περιπτώσεων ελέγχου, των δομών δεδομένων, των αλγορίθμων και της αποδοτικότητας.

ΦΑΣΗ 3:Υλοποίηση

Η υλοποίηση ή η κωδικοποίηση είναι η διαδικασία κατά την οποία παράγεται ο κώδικας με βάση δύο ομάδες δεδομένων:

- Στην πρώτη ομάδα περιλαμβάνονται τα ενδιάμεσα προϊόντα των προηγούμενων φάσεων(Απαιτήσεις λογισμικού, Σχέδιο Λογισμικού – αρχιτεκτονικό, λεπτομερές)

- Στην άλλη ομάδα περιλαμβάνονται τα πρότυπα και οι αρχές κωδικοποίησης, οι προτάσεις για την τεχνοτροπία της κωδικοποίησης (το ύφος και η μορφή) και τέλος η ταυτότητα της γλώσσας στην οποία θα γίνει κωδικοποίηση.

Η κωδικοποίηση προϋποθέτει την επιτυχή ολοκλήρωση των προηγούμενων φάσεων του κύκλου ζωής, την κατάλληλη τεκμηρίωση που προέκυψε από τις προηγούμενες φάσεις, την υιοθέτηση από την διοίκηση του έργου προτύπων κωδικοποίησης και οδηγιών που προσδιορίζουν την τεχνοτροπία της κωδικοποίησης και τέλος τον προσδιορισμό της γλώσσας προγραμματισμού η οποία θα πρέπει να αναφέρεται στο πλάνου έργου.

ΦΑΣΗ 4:Αξιολόγηση – Έλεγχος

Αυτή η φάση ελέγχου αφορά τον έλεγχο του εργαλείου τόσο στα επιμέρους μέρη του (ενότητες κώδικα) όσο και στο σύνολο του. Προτού το εργαλείο να είναι διαθέσιμό στην αγορά θα πρέπει να πραγματοποιηθούν μια σειρά από ελέγχους για να διαπιστωθεί κατά πόσο αυτό συμμορφώνεται προς τις απαιτήσεις του λογισμικού. Οι έλεγχοι που πραγματοποιούνται είναι αυτοί που απαιτούνται από το πλάνο ποιότητας. Το εργαλείο δεν μπορεί να διατεθεί στην αγορά αν δεν

ολοκληρωθεί ο έλεγχος φτάνοντας σε επίπεδο ποιότητας που ορίζεται από τις απαιτήσεις.

4.6 Το αντικείμενο της Παρούσας Εργασίας

Η παρούσα εργασία αποτελεί μια διερευνητική μελέτη για τον προσδιορισμό του προβλήματος, ενώ θα επικεντρωθεί στην συλλογή και σύνταξη σε προκαταρκτικό στάδιο κάποιων απαιτήσεων για την ανάπτυξη ενός εργαλείου υποστήριξης της ανάλυσης και της διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων.

Είδη Απαιτήσεων που θα πρέπει να Συλλεχθούν

Οι απαιτήσεις που θα πρέπει να συλλεχθούν θα αφορούν τη λειτουργία του εργαλείου, τους περιορισμούς που τίθονται για την ανάπτυξη του (π.χ. συμμόρφωση προς υπάρχοντα πρότυπα, περιορισμοί για το υλικό/ λογισμικό-αν υπάρχουν.),τις επιδόσεις που θα πρέπει να έχει καθώς και άλλες ειδικές απαιτήσεις για τα σημεία διεπαφής του χρήστη, του υλικού ,του λογισμικού, των επικοινωνιών , την ασφάλεια /προστασία δεδομένων, την διαθεσιμότητα ,τις κοινωνικές απαιτήσεις και του τρόπου λειτουργίας του.

Προέλευση των Απαιτήσεων

Δεδομένου ότι η διαδικασία του προσδιορισμού και ανάλυσης των απαιτήσεων οι οποίες πρέπει να χαρακτηρίζονται από ακρίβεια και πληρότητα, είναι ένα εξαιρετικά δύσκολο έργο, απαιτείται ιδιαίτερη προσοχή κατά την εκτέλεση του. Εξέχουσα σημασία θα πρέπει να δοθεί στις πηγές που θα παρέχουν σχετική πληροφόρηση αλλά και στον τρόπο που αυτή θα τύχει επεξεργασίας από τον αναλυτή. Οι πηγές πληροφόρησης και τα χαρακτηριστικά τους είναι τα ακόλουθα:

- Συνέντευξη με ανθρώπους έμπειρους και ειδικούς σε γενικότερα θέματα ασφάλειας σε θέματα ανάλυσης και διαχείρισης της επικινδυνότητας, ελέγχου ασφάλειας πληροφοριακών συστημάτων οι οποίοι θα είναι δυνητικά οι χρήστες του εργαλείου .Κρίνεται ότι όσο μεγαλύτερη είναι η εμπειρία του ατόμου στην εφαρμογή και χρήση άλλων εργαλείων ανάλυσης και διαχείρισης της επικινδυνότητας στο παρελθόν, τόσο μεγαλύτερη βαρύτητα θα έχουν οι απαντήσεις στον προσδιορισμό των απαιτήσεων.

- Οργάνωση συναντήσεων ανταλλαγής απόψεων (workshops) για θέματα σχετικά με τις μεθοδολογίες ανάλυσης και διαχείρισης της επικινδυνότητας, ανάμεσα σε έμπειρους σε θέματα ασφαλείας χρήστες αναμένοντας να προκύψουν μέσα από την ανταλλαγή απόψεων και το διάλογο χρήσιμα και πιθανά συμπεράσματα.

- Χρησιμοποίηση σε περιβάλλον εργαστηριακό (και αν υπάρξει η ευκαιρία σε πραγματικό) διαθέσιμων εργαλείων ανάλυσης και διαχείρισης της επικινδυνότητας

και παρατήρηση του τρόπου με τον οποίο προσεγγίζουν την ανάλυση και διαχείριση της επικινδυνότητας αλλά και μελέτη των εγχειριδίων χρήσης αυτών των εργαλείων.

ΚΕΦΑΛΑΙΟ 5

ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΕΡΓΑΛΕΙΟΥ

Έχοντας θέσει το πλαίσιο στο οποίο θα κινηθούμε και την μεθοδολογία την οποία θα ακολουθήσουμε, είμαστε σε θέση να συγκεντρώσουμε το κατάλληλο υλικό για την ανάλυση των απαιτήσεων που θα επακολουθήσει.

Δικαιολόγηση των Παρατιθέμενων Απαιτήσεων

- Οι απαιτήσεις που παρατίθενται στη συνέχεια έχουν προκύψει μέσα από μια μεθοδική έρευνα και μελέτη απόψεων ανθρώπων έμπειρων και ειδικών σε θέματα ασφαλείας, οι οποίοι μέσα από τα συγκράματα τους έχουν ασχοληθεί και κατ' επέκταση έχουν χρησιμοποιήσει μεθόδους και εργαλεία ανάλυσης και διαχείρισης της επικινδυνότητας.

- Οι απαιτήσεις συλλέχθηκαν από συγκράματα τα οποία έχουν γραφεί από άτομα που έχουν μεγαλύτερη εμπειρία στο συγκεκριμένο αντικείμενο και συνεπώς κατέχουν μεγάλη βαρύτητα στην ανάλυση και την τελική διατύπωση που επιδιώκουμε να παραθέσουμε σε αυτή την εργασία.Η συλλογή των απαιτήσεων έγινε πολύ προσεκτικά έτσι ώστε αυτές είναι σε θέση να χρησιμοποιηθούν για την ανάπτυξη ενός εργαλείου προσαρμοσμένου στα ελληνικά δεδομένα

5.1 Χαρακτηριστικά εργαλείου προς εξέταση

Παρακάτω παρατίθεται ο πίνακας με τα χαρακτηριστικά και ακολουθεί επεξήγηση για την σημασία του.

1.Χρήση της Ανάλυσης της Επικινδυνότητας
* Πιστοποίηση
* Ασφάλιση
* Διαχείριση Έργων
* Υποστήριξη της Λήψης Αποφάσεων
* Ασφάλεια και Έλεγχος
* Πληροφόρηση
* Άλλοι λόγοι
2.Μέθοδος
* Ποιοτική
* Ποσοτική
* Αναγνώριση και Αποτίμηση Αγαθών

* Ανάλυση Απειλών και Αδυναμιών
* Ανάλυση Επιπτώσεων (Impact Analysis)
* Πρόταση Αντιμέτρων(ηθικά, νομικά, διοικητικά, λειτουργικά, τεχνικά)
* Μοντελοποίηση του Οργανισμού Βάσει Διαδικασιών
* Μοντελοποίηση του Ανθρώπινου Περιβάλλοντος
* Ανάλυση Επικινδυνότητας Προσωπικού (Personnel)
* Αυτόματη Δημιουργία Μοντέλου (για δίκτυα)
* Ανάλυση Αποφάσεων(Decision Analysis)
* Δυνατότητα Προσομοίωσης
* Στατιστική Ανάλυση
* Ευρεστικός Υπολογισμός (Heuristics)
* Ασαφείς μετρικές(Fuzzy Metrics)
* Ερωτηματολόγια
* Αυτόματη Διανομή/ Συλλογή/ Συγχώνευση Ερωτηματολογίων
* Ανάλυση Στηριζόμενη στη Βάση Γνώσης
* Ανάλυση με Βάση Προβλέψεις (Prediction analysis)
* Ανάλυση με Βάση Σενάρια(Scenario – Based Analysis)
* Ανάλυση σεναρίων "What – If"
* Πλάνο συνέχειας (Business Continuity /Contingency Plan)
* Κατάλληλο για Συστήματα σε Λειτουργία
* Κατάλληλο για Συστήματα σε Ανάπτυξη
* Κατάλληλο για Μικρά/ Μεγάλα/ Δικτυωμένα Συστήματα
* Ευελιξία
* Λειτουργία σε κάθε Επίπεδο Αναλυτικότητας (Granularity)
* Προσαρμογή (Customization) – Ανασχεδιασμός των Διαδικασιών
* Τροποποίηση – Άμεση Ενημέρωση της Βάσης Γνώσης
3.Κόστος
4.Ευκολία Χρήσης
* Ευχρηστία
* Ποιότητα Εγγραφών /Περιεκτικότητα
* Ευκολία στη Διαδικασία Εγκατάστασης
* Δυνατότητα Αναίρεσης (Undo)
* Δυνατότητα Ανατροφοδότησης (Feedback)
* Άλλες χρήσιμες Δυνατότητες/ πρόσθετες Ευκολίες
5.Χρόνοι
* Διάρκεια Εκτέλεσης της Ανάλυσης της Επικινδυνότητας
* Συχνότητα Πραγματοποίησης Της Ανάλυσης της Επικινδυνότητας
6.Εκθέσεις (Reports)
* Δημιουργία Αυτόματων Εκθέσεων
* Ιχνηλάτηση προς τα εμπρός/ προς τα πίσω
* Γραφική Αναπαράσταση
* Τύπος Εκθέσεων Προσανατολισμένος στη Διοίκηση
* Τύπος Εκθέσεων Προσανατολισμένος σε Τεχνικές Αναλύσεις
* Δυνατότητες Φιλτραρίσματος
* Επαναχρησιμοποίηση των Αποτελεσμάτων
* Προσαρμογή των Εκθέσεων
* Εξαγωγή των Αποτελεσμάτων σε Κατάλληλη Μορφή
7.Εκπαίδευση και Υποστήριξη του Προϊόντος

* Καθοδήγηση
* Εκπαίδευση
* Τεχνική Υποστήριξη
* Μελλοντική Συντήρηση
* Επιτόπια Εκπαίδευση
* Εκπαίδευση- Προσαρμογή στο Νέο Τρόπο Εκτέλεσης Διαδικασιών
* Συμβουλευτικές Υπηρεσίες
* Συχνότητα Εμπλουτισμού/ Ενημέρωσης Βάσεων
8.Ταίριασμα στον Οργανισμό
* Κουλτούρα του Οργανισμού
* Αποδοχή των Χρηστών Αλλαγή κουλτούρας
* Δομή του Οργανισμού
* Μέγεθος του Οργανισμού
* Πολιτικές Ασφαλείας
* Φιλοσοφία Σχετικά με Ασφάλεια
* Πιθανότητα Υλοποίησης Αντιμέτρων
9.Απαιτήσεις Υλικού και Λογισμικού
* Διάρθρωση (Configuration) Υλικού
* Ελάχιστες Απαιτήσεις Υλικού
* Ταχύτητα Λειτουργικών Επιδόσεων
* Λειτουργικό Σύστημα
* Συμβατότητα
10.Απαιτήσεις Ασφάλειας
* Κρυπτογράφηση
* Logon/ Password
* Έλεγχος Πρόσβασης
* Έλεγχος Έκδοσης(Version Control)
* Έλεγχος(Audit)
11.Σύνολο Αντιμέτρων
* Έκταση/ ομάδες κάλυψης/ τύποι
* Όγκος
* Συχνότητα Ενημέρωσης
* Θεώρηση Υπαρχόντων Αντιμέτρων
* Αιτιολόγηση Αντίμετρων
* Τοποθέτηση Προτεραιοτήτων
* Ανάλυση Σεναρίων "What – If"
* Ανάλυση Κόστους- οφέλους / Απόδοσης Επένδυσης(Cost benefit/return on investment)
12.Κάλυψη Περιουσιακών Στοιχείων
* Δυνατότητα μοντελοποίησης ΠΣ ως ολότητα
* Δυνατότητα Μοντελοποίησης Αγαθών
* Υλικά Αγαθά
* Άυλα Αγαθά
13.Κάλυψη Απειλών και Αδυναμιών
* Πηγές Απειλών
* Χρήση Πραγματιστικών Δεδομένων
* Συχνότητα Ενημέρωσης
* Δυναμικές Αλλαγές της Επικινδυνότητας

* Ειδικές ανά περιοχή Απειλές
* Σενάρια
14.Ενοποίση με άλλα Εργαλεία
* Συμβατότητα Υλικού /Λογισμικού
* Μεθοδολογική Συμβατότητα

Από τα χαρακτηριστικά αυτά αξίζει τον κόπο να κάνουμε μια μικρή αναφορά σε μια από τις λειτουργίες ενός πληροφοριακού συστήματος, στην εκπαίδευση και την μάθηση. Η εκπαίδευση και η μάθηση δεν πρέπει να περιορίζονται μόνο στην εκμάθηση του εργαλείου αλλά πρωτίστως στο νέο τρόπο οργάνωσης του οργανισμού και στην αλλαγή της κουλτούρας. **Κανένα αντίμετρο δεν θα επιτύχει αν οι άνθρωποι που το εφαρμόσουν δεν «αλλάξουν».**

Πέρα από την αλλαγή της κουλτούρας που σχετίζεται περισσότερο με την διαχείριση και όχι με την ανάλυση της επικινδυνότητας ,απαιτείται και **η εξέταση του πληροφοριακού συστήματος ως ολότητα,** πέρα από την εξέταση και την εκτίμηση των περιουσιακών στοιχείων του πληροφοριακού συστήματος . Άλλωστε χαρακτηριστικό κάθε συστήματος είναι η ολότητα που το διακρίνει και πρέπει το εργαλείο να εκτιμά και την επικινδυνότητα που το πληροφοριακό σύστημα ως σύνολο έχει.

Τα υπάρχοντα εργαλεία ως επί το πλείστον «αντικειμενοποιούν» την υποκειμενικότητα. Είναι στη κρίση του αναλυτή η αποτίμηση της επικινδυνότητας κάθε περιουσιακού στοιχείου χωρίς κάποια αντικειμενικά κριτήρια. Έτσι κρίνεται σκόπιμη κάποια βάση γνώσης πάνω στην οποία θα στηρίζεται η ανάλυση και η διαχείριση της επικινδυνότητας. Σε συνδυασμό με τη βάση γνώσης πρέπει το εργαλείο να μπορεί να προβλέπει αντί να μαντεύει τους πιθανούς κινδύνους.

Πέρα από τα χαρακτηριστικά αυτά θα πρέπει να αναφέρουμε και κάποια γενικά συμπεράσματα:

- **Η ανάλυση της επικινδυνότητας δεν χρησιμοποιείται για λήψη αποφάσεων αλλά για υποστήριξη της διαδικασίας αυτής.** Όπως έχει αναφερθεί και στον ορισμό, τα αποτελέσματα της ανάλυσης φιλτράρονται από τον αναλυτή ώστε να παρουσιαστούν με ανάλογο τρόπο για επικύρωση από τη διοίκηση.

- Ένας ακόμα πιθανός λόγος χρήσης της ανάλυσης είναι η **πληροφόρηση που μπορεί να παρέχει και στη διοίκηση.** Όπως τονίζεται και από άλλους συγγραφείς ένα πλεονέκτημα της ανάλυσης και διαχείρισης της επικινδυνότητας είναι ότι αποτελεί εργαλείο επικοινωνίας μεταξύ διοίκησης και αναλυτών.

- **Τα αντίμετρα** που προτείνονται πρέπει να **καλύπτουν** θέματα όπως **νομικά ,ηθικά,** (αντλούμενα από τον κώδικα δεοντολογίας), **διοικητικά, λειτουργικά** και **τεχνικά** χωρίς βέβαια να αποκλείεται και κάποια άλλη κατηγοριοποίηση.

- Όπως αναφέρεται και στον ορισμό και προτείνεται μέσω της επιλεγμένης μεθοδολογίας, **πρέπει να πραγματοποιείται μοντελοποίηση του οργανισμού βάσει των διαδικασιών που αυτός επιτελεί**. Έτσι έχουμε τη δυναμική δομή του οργανισμού μέσα στον οποίο εντάσσεται το πληροφοριακό σύστημα προς εξέταση. Το πληροφοριακό σύστημα πρέπει να μοντελοποιείται και ως ολότητα (πέρα από την κάλυψη – μοντελοποίηση των επιμέρους περιουσιακών στοιχείων).

- Πιθανές μέθοδοι για την ανάλυση της επικινδυνότητας θα μπορούσαν να **είναι η ανάλυση στηριζόμενη στη βάση γνώσης ή και στις προβλέψεις** (prediction analysis). Μέσω της δυνατότητας ανατροφοδότησης μπορούμε να δημιουργήσουμε μια βάση γνώσης έτσι ώστε να διευκολύνεται η ανάλυση και αυτή(βάση γνώσης) να ενημερώνεται και να εμπλουτίζεται άμεσα.

- Σημαντική κρίνεται και η δυνατότητα **ανασχεδιασμού των διαδικασιών του οργανισμού.** Όπως έχει ήδη αναφερθεί πιθανά αντίμετρα μπορεί να σχετίζονται με τις ίδιες τις διαδικασίες, έτσι η δυνατότητα πρότασης ανασχεδιασμού αυτών είναι θετική.

- Όσον αφορά την **κουλτούρα** πρέπει να σημειώσουμε πάλι ότι **παίζει σημαντικό ρόλο** ιδίως στον τρόπο εκτέλεσης των εργασιών και στις σχέσεις μεταξύ εργαζομένων και διοίκησης.

- **Η αιτιολόγηση των αντίμετρων είναι σημαντική** αφού η ανάλυση και η διαχείρισης της επικινδυνότητας αποτελεί το εργαλείο επικοινωνίας και τη διεπαφή μεταξύ διοίκηση και αναλυτή.

Από τα προαναφερθέντα χαρακτηριστικά παρήχθησαν διάφορες απαιτήσεις που και αυτές θα τύχουν τροποποίησης ώστε να συμβαδίζουν με τον ορισμό του συγκεκριμένου εργαλείου και με τη μεθοδολογία που αυτή ακολουθεί.

5.2 Λειτουργικές Απαιτήσεις

Το επόμενο βήμα ,μετά τα χαρακτηριστικά που επιδιώκονται να εξεταστούν για την σχεδίαση του εργαλείου, είναι η καταγραφή των σχετικών απαιτήσεων για το συγκεκριμένο εργαλείο.

1.Φάσεις – Βήματα του Εργαλείου

Η μέθοδος ανάλυσης και διαχείρισης της επικινδυνότητας θα πρέπει να περιλαμβάνει τις ακόλουθες φάσεις:

Φάση 1:Ορισμός του προβλήματος (Ορισμός του συστήματος και ανάλυση του οργανισμού)
Φάση 2:Ανάλυση της Επικινδυνότητας
Φάση 3:Υλοποίηση
Φάση 4:Παρακολούθηση
Φάση 5:Αναθεώρηση

1.1 Φάση 1η: Ορισμός του προβλήματος

Με τον όρο ορισμός του προβλήματος εννοούμε **ορισμό του οργανισμού** και **ασφάλειας** αυτού, **ανάλυση του οργανισμού** και **μοντελοποίηση του** οργανισμού. Όπως έχει προαναφερθεί χωρίς τον ορισμό του προβλήματος καμία

λύση δεν θεωρείται σωστή. Πρέπει να δοθεί ένα ορισμός του οργανισμού χρησιμοποιώντας την μεθοδολογία των ευμετάβλητων συστημάτων για κάθε κύριο δικαιούχο (stakeholder). **Η μέθοδος θα πρέπει να δένει το υπολογιστικό σύστημα** (πληροφοριακό σύστημα πλην των ανθρώπων) **με τον οργανισμό** (τις επιχειρηματικές διαδικασίες, τη στρατηγική της επιχείρησης, τη μεταβλητότητα της). Αν υπάρχουν πολλά υποσυστήματα πρέπει αναφέροντας τον ορισμό της ασφάλειας για τον οργανισμό, να συγκεκριμενοποιηθεί αυτός για κάθε υποσύστημα (εντάσσοντας και το πληροφοριακό σύστημα που είναι υπό εξέταση).Για να το πετύχει αυτό η μέθοδος θα πρέπει να ξεκινά με τον ορισμό του συστήματος και την ανάλυση του οργανισμού. Το βήμα αυτό αφορά τον οργανισμό στο σύνολο του και θα βοηθά στον εντοπισμό των περιοχών του οργανισμού που χρήζουν προστασίας.

Στην ανάλυση του οργανισμού πρέπει να προσδιοριστούν τα όρια αυτού και των υποσυστημάτων του. Η μοντελοποίηση του οργανισμού πρέπει να γίνει με στατικό και δυναμικό τρόπο. Στο δυναμικό μοντέλο μπορούν να χρησιμοποιηθούν τα διαγράμματα ροής δεδομένων ή και τα μοντέλα διαδικασιών (process models). Όσον αφορά το στατικό – δομικό μοντέλο αυτό μπορεί να αναπαρασταθεί π.χ. με τη χρήση του μοντέλου οντοτήτων συσχετίσεων E -R.

1.1.1 Ορισμός του Συστήματος

Σε μια πρώτη φάση θα πρέπει να δοθεί ίσως ένας ορισμός του συστήματος προς ανάλυση, **περιγραφή των διαδικασιών** που θα αναφερθούν και διάφορα άλλα στοιχεία όπως τους **πελάτες**(clients), τους **δημιουργούς** (actors), το **μετασχηματισμό** (transformation) του συστήματος, **την κοσμοθεωρία**, τον **ιδιοκτήτη** (owner), τα οποία θα πρέπει να καταγραφούν με στόχο να βοηθηθεί ο χρήστης- αναλυτή σε μια ολοκληρωμένη μελέτη – ανάλυση του οργανισμού. Τα στοιχεία αυτά θα περιληφθούν στην τεκμηρίωση του μοντέλου του οργανισμού που θα δημιουργηθεί κατά την πρώτη φάση της μεθόδου.

1.1.2 Προσδιορισμός των Ορίων του Συστήματος

Ο ορισμός του συστήματος θα βοηθά επίσης στον προσδιορισμό των ορίων του συστήματος που θα μελετάται, εντοπίζοντας τα υποσυστήματα που ανήκουν εντός και εκτός αυτού (ίσως και με τη βοήθεια κάποιου μοντέλου, όπως αυτά που θα περιγραφούν στη συνέχεια).

1.1.3. Διαγραμματικές Τεχνικές Ανάλυσης και Μοντελοποίησης του Οργανισμού.

Η ανάλυση του οργανισμού θα πραγματοποιείται με χρήση κατάλληλων διαγραμματικών τεχνικών. Γενικά οι διαγραμματικές τεχνικές ανάλυσης και μοντελοποίησης που θα χρησιμοποιηθούν θα πρέπει να περιγράφουν τη δομή του οργανισμού και τις διαδικασίες του. Πιο ειδικά, τα είδη των διαγραμμάτων που θα χρησιμοποιηθούν θα πρέπει το πολύ να είναι τρία. Το ένα από αυτά θα πρέπει να είναι **προσανατολισμένο στις διαδικασίες** (process oriented), ενώ ένα θα πρέπει να **περιγράφει τη στατική δομή του οργανισμού**(π.χ. οργανογράμματα) και ίσως

ένα το οποίο **να μοντελοποιεί τα δεδομένα**(π.χ. ΔΡΔ) ή την πληροφορία. Τα στοιχεία αυτά που θα καταγράφονται θα πρέπει να τεκμηριώνονται μέσα στο εργαλείο (με περιγραφές τους και άλλα απαραίτητα χαρακτηριστικά τους) και θα αποθηκεύονται ώστε να χρησιμοποιούνται στα επόμενα βήματα του εργαλείου.

1.2 Φάση 2η : Ανάλυση της Επικινδυνότητας

Στη φάση αυτή θα πρέπει να πραγματοποιηθεί η ανάλυση της επικινδυνότητας αξιοποιώντας στα σημεία που είναι δυνατό τα στοιχεία που καταγράφηκαν στην προηγούμενη φάση. Σε γενικές γραμμές τα βήματα της φάσης αυτής είναι:

i. Αποτίμηση των περιουσιακών αγαθών (assets) του οργανισμού για κάθε μια από τις ιδιότητες (security properties) που αυτά έχουν και σχετίζονται με την ασφάλεια (π.χ. εμπιστευτικότητα, ακεραιότητα).
ii. Προσδιορισμός και αποτίμηση των απειλών και αδυναμιών
iii. Υπολογισμός της συνολική επικινδυνότητας.

1.2.1 Αποτίμηση των Περιουσιακών Αγαθών του Οργανισμού

Η αποτίμηση των αγαθών πραγματοποιείται **αναλύοντας τις επιπτώσεις που θα έχει η ζημιά στα αγαθά αυτά δίνοντας έτσι και τη σχετική τους αξία.** Από τα διαγράμματα που έχουν δημιουργηθεί στην προηγούμενη φάση θα προκύψουν τα περιουσιακά αγαθά των προς ανάλυση συστημάτων, Σε ένα πρώτο στάδιο αυτά θα πρέπει να αναγνωριστούν από το εργαλείο ώστε να μην απαιτείται να γίνει επανάληψη της εισαγωγής τους και στη συνέχεια θα πρέπει να είναι δυνατή κάποια αποσύνθεση τους σε απλούστερα στοιχεία (π.χ. οι προσωπικοί υπολογιστές θα μπορούσαν να αναλυθούν σε σταθμό εργασίας, εξυπηρετητή κ.α.) ή και η κατηγοριοποίηση σε ευρύτερες ομάδες. Η διαδικασία αυτή θα μπορούσε να δοθεί πιο παραστατικά μέσα από τις έννοιες των κλάσεων και των αντικειμένων, αν θεωρήσει κάποιος ότι στο επίπεδο της οργανωτικής ανάλυσης καταγράφονται κάποιες κλάσεις αντικειμένων, ενώ στο αμέσως επόμενο επίπεδο οι κλάσεις αναλύονται σε αντικείμενα.

Στα περιουσιακά αγαθά τα οποία καταγράφονται στην προηγούμενη φάση, θα έχουν ορισθεί κάποια χαρακτηριστικά τα οποία θα διευκολύνουν την αναγνώριση τους ως τέτοια σε αυτή (π.χ. θα μπορεί να υπάρχει η δυνατότητα να οριστεί σε ποια κατηγορία αγαθών ανήκει- υλικό, λογισμικό, δίκτυο-, ποια η ονομασία του, η περιγραφή του ,καθώς και η αξία του). Σε αυτή τη φάση θα μπορούσαν να εμφανίζονται με τη μορφή μιας λίστας όλα τα αγαθά που έχουν περιγραφεί προηγουμένως, ώστε να επιλεγούν οι κατάλληλες για αυτά ερωτήσεις, οι οποίες θα πρέπει να ερωτηθούν ώστε να προσδιοριστεί όσο το δυνατόν καλύτερα η αξία τους.

Είναι πιθανό να υπάρχουν κάποια αγαθά τα οποία κρίνεται ότι δεν χρειάζεται να αναλυθούν περισσότερο, οπότε θα μπορούσε να δηλώνεται αυτό με κάποιο τρόπο.

Ακόμα αν θεωρείται ότι κάποια αγαθά έχουν παραληφθεί θα πρέπει ο χρήστης-αναλυτής να γυρίζει πίσω στα μοντέλα της προηγούμενης φάσης ώστε να τα

συμπληρώσει, καθώς θα πρέπει να υπάρχει συνέπεια με τα στοιχεία των προηγούμενων φάσεων.

Επίσης θα πρέπει να πραγματοποιείται συσχετισμός της αποτίμησης των επιμέρους στοιχείων με το μοντέλο του συστήματος δηλαδή με την αλληλοσυσχέτιση των στοιχείων του πληροφοριακού συστήματος.

Το βήμα αυτό θα πρέπει να **τελειώνει με την πραγματοποίηση μιας ανάλυσης επιπτώσεων (impact analysis) στα αγαθά.**

1.2.2.Προσδιορισμός και Αποτίμηση των Απειλών και Αδυναμιών

Στο βήμα αυτό θα **προσδιορίζονται οι απειλές και οι αδυναμίες οι οποίες αφορούν τα αγαθά και θα αποτιμάται η πιθανότητα εμφάνισης των απειλών και εκμετάλλευσης των αδυναμιών.** Με την αναζήτηση των αδυναμιών μπορούμε να υπολογίσουμε τη σπουδαιότητα τους βάσει του βαθμού ευπάθειας που προσθέτουν στα αγαθά αλλά και στον οργανισμό ως ολότητα. Έτσι αποτιμώνται οι απειλές αφού αυτές εκμεταλλεύονται τις αδυναμίες ώστε να προκαλέσουν τυχόν ζημιά στα αγαθά και στον οργανισμό κατ' επέκταση.

1.2.3. Υπολογισμός της Συνολικής Επικινδυνότητας

Για κάθε συνδυασμό αγαθό – απειλή – αδυναμία υπολογίζεται ο βαθμός επικινδυνότητας, ενώ λαμβάνονται υπόψη η συσχέτιση και οι εξαρτήσεις μεταξύ των στοιχείων του πληροφοριακού συστήματος.

1.3 Φάση 3η :Υλοποίηση

Κάθε τριάδα που προαναφέρθηκε , **περιγράφει ένα σενάριο προσβολής του υπό εξέταση πληροφοριακού συστήματος.** Έτσι στη φάση αυτή απαιτείται μια ιεράρχηση των βαθμών επικινδυνότητας ώστε να προσδιοριστούν οι προτεραιότητες. Με την επικύρωση των αποτελεσμάτων αυτών αναπτύσσεται το σχέδιο ασφαλείας καθώς αυτό θα αντιστοιχείται με τις ανάγκες και τα ιδιαίτερα χαρακτηριστικά του πληροφοριακού συστήματος και του οργανισμού όπως αυτά καταγράφηκαν σε προηγούμενες φάσεις. Ο βαθμός της επικινδυνότητας θα χρησιμοποιηθεί για την επιλογή αντιμέτρων ενώ θα πρέπει να γίνει η καταγραφή της φάσης στην οποία βρίσκεται η υλοποίηση των επιλεχθέντων αντιμέτρων.

Επίσης στο στάδιο αυτό **θα παράγεται και το σχέδιο ασφάλειας το οποίο περιλαμβάνει την πολιτική ασφαλείας, τα μέτρα προστασίας και τη στρατηγική υλοποίησης αυτού.** Η πολιτική ασφαλείας περιλαμβάνει ένα σύνολο έγκυρων και επίσημων δηλωτικών προτάσεων (authoritative statements) που προσδιορίζουν το σύνολο των αποδεκτών πιθανών επιλογών σε μελλοντικές διαδικασίες λήψης αποφάσεων. Τα μέτρα προστασίας ή αλλιώς αντίμετρα πηγάζουν από την πολιτική αυτή και απορρέουν από την ιεράρχηση των προτεραιοτήτων και

από τη βάση γνώσης που υπάρχει στο εργαλείο η οποία θα εμπλουτίζεται ταυτόχρονα. Πρέπει να αναφερθεί ότι τα αντίμετρα πρέπει να καλύπτουν όλες τις πλευρές ηθικά, νομικά , διοικητικά, λειτουργικά και τεχνικά.

1.4 Φάση 4η: Παρακολούθηση

Στα πλαίσια αυτής της φάσης θα πρέπει να είναι δυνατή **η συλλογή και η ενσωμάτωση στατιστικών** (σχετικών με γεγονότα, θέματα ασφαλείας και παραβίασης αυτής) **μέσα στη μέθοδο.** Η δυνατότητα αυτή βελτιώνει την ποιότητα της διαδικασίας ανάλυσης και διαχείρισης της επικινδυνότητας και κατ' επέκταση, βελτιώνει την ασφάλεια του οργανισμού. Θέματα όπως αλλαγές του οργανισμού , του περιβάλλοντος, της νομοθεσίας καθώς και οι τεχνολογικές εξελίξεις πρέπει να λαμβάνονται υπόψη έτσι ώστε να παρέχεται αποδοτικότερα η ασφάλεια. Έρευνες οι οποίες ανακοινώνονται από έγκυρους οργανισμούς, διεθνείς ή ελληνικούς, και κρίνονται ότι αντικατοπτρίζουν και την ελληνική πραγματικότητα θα αποτελούν μια αποδεκτή πηγή. Αν σε μια τέτοια έρευνα αναφέρεται για παράδειγμα μια ετήσια αύξηση 60% σε κλοπές σχετικές με υπολογιστές και το στατιστικό αυτό στοιχείο θα μπορούσε να εισαχθεί στη μέθοδο, τότε οι κίνδυνοι που συνδέονται με τη κλοπή θα έπρεπε να θεωρηθούν υψηλότεροι και θα απαιτούνταν πιο αυστηρά μέτρα τα οποία με τη σειρά τους θα συνεισέφεραν σε ένα βελτιωμένο επίπεδο ασφαλείας .Έτσι απαιτείται μια συνεχής ανάλυση των νέων συνθηκών σε σχέση με αυτές που χαρακτηρίζουν το σύστημα και τον οργανισμό.

1.5 Φάση 5η: Αναθεώρηση

Στη φάση αυτή πρέπει πρωτίστως να παρακολουθείται **η υλοποίηση των αντίμετρων** και κατά πόσο αυτά ανταποκρίνονται στις τρέχουσες ανάγκες και αν επιφέρουν τα ίδια μέτρα προστασίας στις νέες απειλές. Η αναθεώρηση ασχολείται με τον **προγραμματισμό για το πότε πρέπει να επαναληφθεί η ανάλυση της επικινδυνότητας**, ενώ επιπρόσθετα αυτό αποτελεί ουσιαστικά το σημείο από το οποίο θα μπορεί ο χρήστης να γυρίσει πίσω στη διαδικασία και να επανεξετάσει τις επιλογές του, θα μπορεί να αξιοποιήσει και ότι είχε κάνει την προηγούμενη φορά αλλά και τα στοιχεία που έχουν προκύψει κατά την παρακολούθηση. Για παράδειγμα η καταχώρηση ενός συμβάντος παραβίασης θα προκαλέσει την αλλαγή μιας απειλής, η οποία απειλή επηρεάζει κάποια αντίμετρα και τελικά αλλάζει το πλάνο ασφαλείας (security plan). Ακόμα η αγορά ενός νέου μηχανήματος θα αλλάξει τη λίστα με τα περιουσιακά στοιχεία, γεγονός το οποίο πιθανά θα αλλάξει το βαθμό επικινδυνότητας με αποτέλεσμα να πρέπει να αλλάξουν πιθανά και ορισμένα αντίμετρα.

Επισημαίνεται ότι **τα αποτελέσματα παλαιοτέρων αναλύσεων θα πρέπει να είναι επαναχρησιμοποιήσιμα σε μια επαναληπτική ανάλυση** και δεν θα πρέπει να ακυρώνονται εντελώς από οποιεσδήποτε αλλαγές που δεν αλλάζουν δραματικά το βασικό μοντέλο του συστήματος.

Άλλες Απαιτήσεις

2. Εφαρμογή σε κάθε Στάδιο του Κύκλου Ζωής της Ανάπτυξης του Λογισμικού

Θα πρέπει να είναι δυνατή η εφαρμογή της μεθόδου σε κάθε στάδιο του κύκλου ζωής της ανάπτυξης του λογισμικού ,ξεκινώντας από τη μελέτη σκοπιμότητας μέχρι και την τροποποίηση υπαρχόντων συστημάτων. Η οπτική αυτή ταιριάζει και με τις επικρατούσες απόψεις για την ασφάλεια καθώς κρίνεται ως γεγονός ζωτικής σημασίας η ασφάλεια να μπορεί να αντιμετωπιστεί σαν ένα τμήμα μιας υλοποίησης, παρά να προστίθεται η ασφάλεια ως τελευταία σκέψη. Η δυνατότητα να μπορεί να εφαρμοστεί η μέθοδος οποιαδήποτε στιγμή επιτρέπει την αξιολόγηση του κόστους των μέτρων ασφαλείας και των επιπτώσεων με τη συντομότερη δυνατή ευκαιρία.

3.Προσαρμογή στην Ελληνική Γλώσσα/ Δεδομένα/ Κουλτούρα/ Νοοτροπία

Το εργαλείο θα πρέπει να είναι προσαρμοσμένο στην ελληνική γλώσσα, στα ελληνικά δεδομένα (ως προς την κοστολόγηση ,τις μονάδες μέτρησης), στην ελληνική κουλτούρα και στις ιδιαιτερότητες του ελληνικού περιβάλλοντος. Σε αυτά θα πρέπει να περιληφθούν τα εξής:

- Οι Έλληνες δεν είναι ιδιαίτερα νομομαθείς, ειδικότερα όσον αφορά τον ν. 24/72/1997 (αρχή της αναλογίας και προστασία των προσωπικών δεδομένων).
- Είναι πολύ εύκολο, για οποιονδήποτε να εισέλθει σε μια δημόσια και όχι μόνο υπηρεσία και να αποσπάσει έγγραφα με προσωπικά δεδομένα, είτε λόγω εύκολης πρόσβασης σε αυτά (τοποθέτηση σε εμφανές – απροστάτευτο σημείο), είτε λόγω αμάθειας ή και αδιαφορίας από πλευράς υπαλλήλων για την προστασία των δεδομένων.
- Οι Έλληνες διακατέχονται από αίσθημα απειθαρχίας. Τα αντίμετρα που το εργαλείο θα παράγει θα προσκρούσουν στην αντίδραση των Ελλήνων σε κάθε τι νέο και διαφορετικό από τον υπάρχοντα τρόπο εκπλήρωσης των εργασιών αυτών.

Όπως είναι ορατό τα θέματα αυτά σχετίζονται με την κουλτούρα του Έλληνα. **Έτσι το εργαλείο από μόνο του δεν είναι σε θέση να αλλάξει την κουλτούρα.** Εδώ καταλυτική κρίνεται η συνεισφορά του ανθρώπου που θα χρησιμοποιήσει το εργαλείο δηλαδή του αναλυτή. Για αυτό και περισσότερη **έμφαση πρέπει να δίνεται στην υλοποίηση αντίμετρων οργανωτικού χαρακτήρα**, καθότι πρέπει να διαμορφωθεί μια κουλτούρα και μια παιδεία που να ενσωματώνει μέσα της το στοιχείο της ασφάλειας. Άλλα χαρακτηριστικά είναι τα εξής:

- Το μέγεθος των ελληνικών επιχειρήσεων είναι μεσαίο. Το εργαλείο πρέπει να απευθύνεται σε τέτοιους οργανισμούς.
- Οι οργανισμοί διακατέχονται από αδυναμίες όσον αφορά την οργάνωση τους με εξαίρεση εταιρείες πιστοποιημένες με ISO όπου το οργανόγραμμα και τα καθήκοντα κάθε υπαλλήλου είναι καλά ορισμένα και τηρούνται.

Τα θέματα αυτά σχετίζονται με τους οργανισμούς των οποίων η ανάλυση της επικινδυνότητας θα πραγματοποιηθεί και η διαχείριση θα εφαρμοστεί. Οι υπάλληλοι δεν ξέρουν ποια είναι τα καθήκοντα τους είτε γιατί αυτά δεν είναι ορισμένα είτε γιατί δεν υπάρχει αντιστοίχηση θέσεως εργασίας με συγκεκριμένα χαρακτηριστικά του υπαλλήλου που καλύπτει αυτή τη θέση.

4.Εφαρμογή σε Μεγάλου Μεγέθους Οργανισμούς

Η μέθοδος θα είναι κατάλληλη για μεγάλου μεγέθους επιχειρήσεις ή οργανισμούς. Σύμφωνα με τα ελληνικά δεδομένα, μεγάλη επιχείρηση θεωρείται αυτή που απασχολεί περισσότερα από 17 – 20 άτομα.

5.Εφαρμογή σε διάφορους Επιχειρηματικούς Κλάδους ή τύπους Επιχειρήσεων και Οργανισμών.

Η εφαρμογή του εργαλείου δεν θα περιορίζεται σε συγκεκριμένους επιχειρηματικούς κλάδους ή τύπους επιχειρήσεων και οργανισμών. Θα μπορεί να αντιμετωπίσει τα διαφορετικά επίπεδα επικινδυνότητας που παρουσιάζουν οι διάφοροι οργανισμοί ή επιχειρήσεις, θα μπορεί να αντεπεξέρχεται σε αυτά και να αναπτύξει μια ποικίλη και εξεζητημένη βάση γνώσης.

6.Εργαλείο Ευθυγραμμισμένο ως προς την Ελληνική και Ευρωπαϊκή Νομοθεσία

Το εργαλείο θα πρέπει να ενσωματώνει και να διέπεται από κανονιστικό πλαίσιο και την ελληνική και ευρωπαϊκή νομοθεσία. Η απαίτηση αυτή υποδεικνύει ότι η μέθοδος θα πρέπει να εξασφαλίζει ότι οι διαδικασίες που εφαρμόζονται, τα αντίμετρα που προτείνονται είναι σύμφωνα με τους σχετικούς περί ασφαλείας νόμους(Ν. 2472/1997 άρθρο 10 παρ.3 και οδηγία 95/46/ΕC αρθ. 17 παρ.2)

7.Αλληλεξαρτήσεις των Διαφορετικών Συστημάτων

Θα πρέπει να λαμβάνονται υπόψη οι αλληλεξαρτήσεις των διαφορετικών συστημάτων /εφαρμογών. Η λογική αυτή συνοψίζεται στην ακόλουθη πρόταση:αν το σύστημα Α εξαρτάται από το σύστημα Β και το σύστημα Β είναι «επικίνδυνο», τότε το σύστημα Α κληρονομεί την «επικινδυνότητα» του Β.

8.Ύπαρξη διαφόρων Επιπέδων λεπτομέρειας μιας Ανάλυσης.

Θα πρέπει να είναι δυνατή η αλλαγή του επιπέδου λεπτομέρειας μιας ανάλυσης .Αυτού του είδους η ευελιξία θα επιτρέπει την πραγματοποίηση λεπτομερών

αναλύσεων κύριων συστημάτων αλλά και τις υψηλού επιπέδου περιλήψεις αναλύσεων. Επιπρόσθετα η εναλλαγή της αναλυτικότητας θα επιτρέπει στους χρήστες – αναλυτές να επικεντρώσουν την προσοχή τους σε συγκεκριμένες «προβληματικές» περιοχές, χωρίς να υπάρχει ανάγκη να πραγματοποιηθεί μια λεπτομερής ανάλυση.

9.Εφαρμογή της Μεθόδου Γρήγορα και Αποτελεσματικά

Η μέθοδος θα πρέπει να μπορεί να εφαρμοστεί με γρήγορο και αποτελεσματικό τρόπο. Φανερά η έκταση μιας ανασκόπησης έχει σημαντική επίπτωση στο χρόνο που απαιτείται για μια ανάλυση. Μια μεγάλη φυσική και τεχνική ανασκόπηση η οποία θα πρέπει να καλύπτει διάφορες φυσικές τοποθεσίες, θα καταλαμβάνει αναπόφευκτα πολύ περισσότερο χρόνο από ότι η ανασκόπηση μιας εφαρμογής σε μια και μοναδική τοποθεσία. Οι δημιουργοί λογισμικού έχουν γενικά αυστηρούς περιορισμούς χρόνου, ενώ συχνά δεν τους επιτρέπεται η πολυτέλεια μιας εκτενούς διαδικασίας ανάλυσης της επικινδυνότητας. Κατ' επέκταση η μέθοδος θα πρέπει να είναι επαρκώς ευέλικτη, έτσι ώστε οι χρήστες να μπορούν να επικεντρώνουν την προσοχή τους σε υποσύνολα της μεθόδου ανάλυσης της επικινδυνότητας.

10.Βασικός Μηχανισμός

Οι μέθοδοι ανάλυσης και διαχείρισης της επικινδυνότητας παρουσιάζουν μια εγγενή πολυπλοκότητα και σχετική δυσκολία στην κατανόηση τους. Ανεξάρτητα από αυτή την πολυπλοκότητα, μια μέθοδος θα πρέπει να περιλαμβάνει ένα βασικό μηχανισμό ο οποίος να υποστηρίζει τουλάχιστον τα ακόλουθα παραδείγματα:

If	ένα σύνολο περιουσιακών στοιχείων έχουν ***μεγάλη αξία*** για έναν οργανισμό
And if	η πιθανότητα της πραγματοποίησης μιας απειλής είναι ***υψηλή***
And if	υπάρχει μια αδυναμία η οποία μπορεί ***πολύ εύκολα*** να τύχει εκμετάλλευσης από μια απειλή
Then	το επίπεδο επικινδυνότητας είναι ***υψηλό***

Στο άλλο άκρο αυτής της κλίμακας θα πρέπει να ισχύει το εξής:

If	ένα σύνολο περιουσιακών στοιχείων έχουν ***μικρή αξία*** για έναν οργανισμό
And if	η πιθανότητα της πραγματοποίησης μιας απειλής είναι ***χαμηλή***
And if	***δεν υπάρχει κάποια αδυναμία*** η οποία μπορεί να τύχει εκμετάλλευσης από μια απειλή
Then	το επίπεδο επικινδυνότητας είναι ***χαμηλό***

Υπάρχει μια αδυναμία η οποία μπορεί πολύ εύκολα να τύχει εκμετάλλευσης από μια απειλή		Αξία Περιουσιακών Στοιχείων	
		Μεγάλη	Μικρή
Πιθανότητα πραγματοποίησης μιας απειλής	Χαμηλή		
	Υψηλή	**Υψηλό**	

Δεν υπάρχει κάποια αδυναμία η οποία μπορεί να τύχει εκμετάλλευσης από μια απειλή		Αξία Περιουσιακών Στοιχείων	
		Μεγάλη	Μικρή
Πιθανότητα πραγματοποίησης μιας απειλής	Χαμηλή		**Χαμηλό**
	Υψηλή		

Οι έννοιες «υψηλό», «χαμηλό» και «εύκολα» θα μπορούσαν να οριστούν σε μια σχετική κλίμακα τιμών με κάποιο ποιοτικό η ποσοτικό τρόπο . Δηλαδή είτε να πάρουν κάποιες σχετικές τιμές(π.χ. μικρό, μεσαίο, μεγάλο) είτε να πάρουν απόλυτες αριθμητικές τιμές. Κατ' επέκταση οι τιμές που θα παίρνουν τα διάφορα επίπεδα θα μπορούν να είναι πεπερασμένου συνόλου ή και να εκτείνονται προς το άπειρο.

11. Συνδυασμοί Τιμών

Είναι σαφές ότι θα υπάρξουν πολλοί συνδυασμοί τιμών της αξίας των περιουσιακών στοιχείων μα το βαθμό της απειλής και το βαθμό της αδυναμίας. Οι τιμές αυτές είναι δυνατόν να **ανήκουν σε ένα σταθερό, πεπερασμένο σύνολο τιμών** (αριθμητικών ή όχι), **ή στους πραγματικούς αριθμούς**. Κατά συνέπεια ο συνολικός αριθμός των δυνατών συνδυασμών μπορεί να είναι αντίστοιχα, πεπερασμένος ή άπειρος. Δοθέντος ενός συγκεκριμένου συνδυασμού, θα ορίζεται ένα επίπεδο επικινδυνότητας. Όπως και προηγουμένως το σύνολο των τιμών της επικινδυνότητας είναι δυνατόν να είναι πεπερασμένο ή μπορεί να εκτείνεται στο άπειρο.

12.Τιμές Επικινδυνότητας

Ανεξάρτητα από το εύρος των τιμών της επικινδυνότητας η κοινή λογική υποδεικνύει ότι όσο **αυξάνει ο βαθμός της, ανάλογα θα πρέπει να αυξάνουν και τα επίπεδα προστασίας.** Το σημείο αυτό με τη σειρά του , υποδεικνύει ότι τα αντίμετρα θα πρέπει να έχουν κάποια βαθμολόγηση της αποτελεσματικότητας τους, ενώ χωρίς αυτή θα είναι αδύνατη η δικαιολόγηση των επιπέδων προστασίας. Η βαθμολόγηση αυτή θα μπορούσε να γίνει με τη χρήση πιθανοτήτων (π.χ. την πιθανότητα το αντίμετρο να αποτύχει) ή με βάση μια ποιοτική κλίμακα (όπως την κλίμακα χαμηλό/ μέτριο/ υψηλό).

13.Δυνατότητα Ορισμού ενός Αποδεκτού Επιπέδου Επικινδυνότητας

Θα πρέπει να είναι δυνατόν να οριστεί ποιο είναι το αποδεκτό επίπεδο επικινδυνότητας για έναν συγκεκριμένο τύπο εφαρμογής, δηλαδή το επίπεδο της εναπομένουσας επικινδυνότητας την οποία ένας οργανισμός είναι προετοιμασμένος να δεχθεί μετά την επιλογή κάποιων αντιμέτρων. Δίνοντας τέτοιες πληροφορίες θα πρέπει να είναι στη συνέχεια δυνατή η σύγκριση του με το πραγματικό επίπεδο επικινδυνότητας του συστήματος.

14.Το Εργαλείο να Υποδεικνύει που Βρίσκονται τα Σημαντικότερα Προβλήματα

Το εργαλείο θα πρέπει να μπορεί να **ορίζει ανεκτά επίπεδα επικινδυνότητας μέσα από πληροφορίες που ο αναλυτής θα εισάγει.** Τα επίπεδα αυτά προσδιορίζουν την επικινδυνότητα που ο οργανισμός είναι σε θέση να αποδεχθεί και να αναλάβει τις απορρέουσες ευθύνες. Επίσης δίνουν τη δυνατότητα σύγκρισης μεταξύ αυτών και των πραγματικών επιπέδων. Αν το τρέχον επίπεδο επικινδυνότητας για ένα σύστημα είναι απαράδεκτα υψηλό, θα πρέπει να είναι δυνατόν να χρησιμοποιηθεί το εργαλείο ώστε να υποδείξει που βρίσκονται τα σημαντικότερα προβλήματα. Όταν οι τιμές επικινδυνότητας των αγαθών έχουν ξεπεράσει κατά πολύ τα ανεκτά επίπεδα, υπάρχει κάποια ένδειξη σοβαρότητας και κινδύνου. Ένας λόγος που υπάρχει αυτή η απαίτηση είναι ότι οι χρήστες δεν θέλουν να χάνουν χρόνο και να καταβάλουν προσπάθεια για να βελτιώσουν την ασφάλεια μιας συνιστώσας η οποία είναι ήδη επαρκώς προστατευμένη. Επίσης αν το εργαλείο δεν υποδεικνύει τις προβληματικές περιοχές τότε ο χρήστης ίσως θα πρέπει να καταλήξει στη μέθοδο δοκιμής και σφάλματος (εμπειρική μέθοδος) ή να εξετάσει την κάθε συνιστώσα της ανάλυσης ,ώστε να αναγνωρίσει την προβληματική περιοχή (εξαιρετικά χρονοβόρα διαδικασία).

15. Μέθοδος Αυστηρή

Η μέθοδος θα πρέπει να είναι αρκετά αυστηρή έτσι ώστε να μπορεί να βοηθήσει στην **αναγνώριση όλων των βασικών σημείων επικινδυνότητας** σε ένα σύστημα καθώς η αποτυχία να εντοπιστούν είναι δυνατόν να έχει αρνητικές συνέπειες σε έναν οργανισμό.

16.Ενσωμάτωση της Επιχειρηματικής Επικινδυνότητας

Η μέθοδος θα πρέπει να ενσωματώνει την επιχειρηματική επικινδυνότητα στην όλη διαδικασία .Αν μια επιχειρηματική διαδικασία είναι δυνατό να αποτύχει εξαιτίας μιας παραβίασης της ασφάλειας του πληροφοριακού συστήματος, τότε αυτό θα πρέπει να περιληφθεί κατά την πραγματοποίηση της ανάλυσης της επικινδυνότητας.

17.Γενικές Απειλές και Αδυναμίες

Οι απειλές και οι αδυναμίες που θα εμφανίζονται θα πρέπει να είναι αρκετά γενικές ώστε να καλύπτουν όλες τις πιθανές περιπτώσεις αλλά όχι πολύ ειδικές προκειμένου να μην επιβαρυνθεί η μέθοδος με λεπτομέρειες που αυξάνουν την πολυπλοκότητα της. Επιπρόσθετα οι απειλές και οι αδυναμίες θα πρέπει να είναι τόσο επεξηγηματικές και όσο απαιτείται ώστε να δημιουργείται η ανάγκη για συνεχή ενημέρωση τους.

18.Ειδικά και Λεπτομερή Αντίμετρα

Όπου απαιτείται ανάγκη για εξειδίκευση, τα αντίμετρα θα πρέπει να είναι αρκετά ειδικά και λεπτομερή ώστε να είναι άμεσα και γρήγορα υλοποιήσιμα.

19.Οικονομικά Αποδοτικά Αντίμετρα

Το επίπεδο της προστασίας το οποίο επιλέγεται σε ένα σύστημα είναι απόφαση επιχειρηματική (καθώς τα αντίμετρα έχουν οικονομικό κόστος).Το γεγονός αυτό οδηγεί στην απαίτηση ότι για κάθε αντίμετρο θα πρέπει να αναφέρονται και πληροφορίες κοστολόγησης, ώστε να βοηθηθεί όσο το δυνατόν περισσότερο η παροχή οικονομικά αποδοτικών μέτρων (cost- effective).

20.Ισορροπημένο Σύνολο από Αντίμετρα

Δεδομένων των αναγνωρισμένων σημείων της επικινδυνότητας η μέθοδος θα πρέπει να βοηθά τους χρήστες να αναπτύσσουν ένα ισορροπημένο σύνολο από αντίμετρα τα οποία σε ιδανική περίπτωση θα αντιμετωπίζουν όλα τα στάδια του κύκλου ζωής μιας απειλής. Για παράδειγμα αναφέρεται ότι θα πρέπει να υπάρχουν αντίμετρα τα οποία θα εντοπίζουν την ύπαρξη μιας απειλής, μειώνουν την πιθανότητα εμφάνισης μιας απειλής και συνεισφέρουν στην ανάκαμψη μετά την εμφάνιση.

21.Μέτρα που να Βοηθούν στην Αποδοχή των Υπολοίπων Αντιμέτρων

Ένα από τα προβλήματα που αντιμετωπίζονται κατά την προσπάθεια υλοποίησης των αντίμετρων είναι η αδυναμία ορισμένων ανθρώπων στον οργανισμό να αντιληφθούν τη σημασία και την ανάγκη ύπαρξης διαδικασιών και συνηθειών που ενσωματώνουν την ασφάλεια. Για παράδειγμα αναφέρεται ότι θα πρέπει ίσως ανάμεσα στα αντίμετρα που προτείνονται σε συνδυασμό με κάποιες απειλές και αδυναμίες να μπορούσαν να περιληφθούν και ομάδες μέτρων που να βοηθούν στην αποδοχή των υπολοίπων αντίμετρων μέσα στην επιχείρηση ή τον οργανισμό και θα σχετίζονται ίσως με θέματα εκπαίδευσης και αύξησης της ενημερότητας (awareness) κάποιων ανθρώπων σε σχέση με θέματα ασφαλείας.

22.Η Μέθοδος Λαμβάνει Υπόψη τις Πιθανές Αρνητικές Επιπτώσεις από Υιοθέτηση Αντίμετρων.

Η μέθοδος θα πρέπει να λαμβάνει υπόψη τις πιθανές αρνητικές επιπτώσεις που μπορεί να υπάρξουν από την υιοθέτηση οποιονδήποτε αντίμετρων. Τέτοιες επιπτώσεις είναι σε θέση να αυξήσουν την επικινδυνότητα των ίδιων των αγαθών

που θεωρητικά επρόκειτο να μειώσουν ή άλλων αγαθών που επηρεάζονται από αυτά τα αντίμετρα.

Η λογική αυτής της απαίτησης περιγράφεται καλύτερα με το εξής παράδειγμα:Η κρυπτογράφηση αποτελεί ένα εξαιρετικά ισχυρό μέτρο προστασίας που χρησιμοποιείται αρχικά για την παροχή της εμπιστευτικότητας, αν όμως χαθούν ή καταστραφούν με κάποιο τρόπο τα κλειδιά της κρυπτογράφησης είναι δυνατόν να υπάρξει απώλεια της διαθεσιμότητας, συνεπώς απαιτούνται επιπρόσθετα μέτρα για την εξασφάλιση ότι τα ίδια τα κλειδιά είναι επαρκώς προστατευμένα.

23. Σύνδεση Αντίμετρων με Δηλώσεις Πολιτικών Ασφαλείας

Τα αντίμετρα τα οποία θα πρέπει να συνδέονται με δηλώσεις πολιτικών ασφαλείας(policy statements).

24.Δήλωση Τύπου Σχέσης Ανάμεσα σε Δηλώσεις Πολιτικής Ασφάλειας.

Καθότι τα αντίμετρα πηγάζουν από την πολιτική ασφαλείας κρίνεται σκόπιμη η αιτιολόγηση σύνδεσης μεταξύ αντίμετρων και δηλώσεων καθώς και η δήλωση της σχέσης που υπάρχει ανάμεσα τους (σχέση επικάλυψης, σχέση συνεργασίας, σχέση αντιφατική).

25.Δυνητικός Χρόνος Επανάληψης της Ανάλυσης της Επικινδυνότητας

Μέσα στο πλάνο ασφαλείας θα πρέπει να υπάρχει κάποια αναφορά στην ανάλυση της επικινδυνότητας, σε σχέση με το δυνητικό χρόνο επανάληψης της. Μέσα στην πολιτική ασφαλείας θα πρέπει να περιλαμβάνονται και δηλώσεις σχετικές με το χρόνο και τις καταστάσεις που θα πρέπει να επικρατούν έτσι ώστε να επαναληφθεί η διαδικασία για εγκαιροποίηση των αντίμετρων. Οι αιτίες μπορεί να είναι είτε σχετικές με αλλαγές στην τεχνολογία, είτε σχετικές με τη δομή του οργανισμού. Μια συνηθισμένη τέτοια αναφορά θα είναι: «Η ανάλυση της επικινδυνότητας θα πρέπει να πραγματοποιείται τουλάχιστον μια φορά κάθε 3 χρόνια. Οποτεδήποτε συμβεί μια σημαντική αλλαγή σε ένα βασικό τμήμα συστήματος ή εφαρμογής, αυτό θα πρέπει να συνοδεύεται πάντα από μια λεπτομερή ανάλυση της επικινδυνότητας».

26.Δυνατότητα Πειραματισμού με διαφορετικά Σενάρια.

Η δυνατότητα πειραματισμού με διαφορετικά σενάρια (καλούμενα, συχνά, σενάρια «what – if») αποτελεί μια επιθυμητή απαίτηση. Για παράδειγμα, μια τέτοια ευκολία θα μπορούσε να επιτρέπει στους χρήστες να δουν ποια πρόσθετα αντίμετρα θα απαιτηθούν, αν η πληροφορία που τυγχάνει επεξεργασίας γίνει περισσότερο κρίσιμη για τον οργανισμό. Άλλο παράδειγμα θα μπορούσε να είναι η ανάλυση μιας αλλαγής στην πολιτική ασφαλείας ενός οργανισμού.

27.Δυνατότητα Ιχνηλάτησης

Στο τέλος μιας ανάλυσης θα πρέπει οι χρήστες να είναι σε θέση να κατανοήσουν το λόγο για τον οποίο προτάθηκε ένα μέτρο, ιδιαίτερα αν ο χρήστης – αναλυτής πρέπει να δικαιολογήσει τις προτάσεις του στην ανώτερη διοίκηση. Η αιτιολόγηση κρίνεται απαραίτητη έτσι ώστε να υπάρχει επικύρωση από τη διοίκηση του οργανισμού .Συνεπώς θα πρέπει να είναι δυνατή η ιχνηλάτηση (προς τα εμπρός και προς τα πίσω) σε όλη τη διαδικασία ανάλυσης και διαχείρισης της επικινδυνότητας, με ένα τρόπο κατά τον οποίο να είναι δυνατή η υποστήριξη οποιονδήποτε απαιτούμενων δικαιολογήσεων .έτσι η ιχνηλάτηση πρέπει να είναι δυνατή και προς τα εμπρός και προς τα πίσω.

28.Επαλήθευση των Αποτελεσμάτων Μέσα από την Επανάληψη

Τα αποτελέσματα μιας ανάλυσης θα πρέπει να είναι δυνατό να επαναληφθούν και να είναι συνεπή σε όλον τον οργανισμό. Η απαίτηση συνεπάγεται ότι τα αποτελέσματα δεν θα πρέπει να κλίνουν προς τις απόψεις των διαφορετικών χρηστών – αναλυτών.

29.Εκθέσεις για τη Διοίκηση και Εκθέσεις Τεχνικές

Οι εκθέσεις που παράγονται από το εργαλείο πρέπει να έχουν συγκεκριμένη κάθε φορά μορφή. Οι εκθέσεις τις ανάλυσης και διαχείρισης της επικινδυνότητας θα πρέπει **να ικανοποιούν από τη μια τις ανάγκες της διοίκησης και από την άλλη τις ανάγκες αυτών που θα κληθούν να υλοποιήσουν τα αντίμετρα**, καθένας από τους οποίους θα έχει το δικό του σύνολο από απαιτήσεις για τις εκθέσεις. Για παράδειγμα οι διαχειριστές της επιχείρησης (business managers), συνήθως απαιτούν σύντομες και περιεκτικές εκθέσεις οι οποίες ίσως να επικεντρώνονται στα θέματα της επιχείρησης, ενώ αυτοί που θα κληθούν να υλοποιήσουν τα μέτρα προστασίας θα χρειαστούν λεπτομερείς περιγραφές τους. Το εργαλείο θα πρέπει να παρέχει μια ποικιλία από εκθέσεις, οι οποίες θα παράγονται στα διάφορα βήματα του εργαλείου. Ακόμα θα πρέπει να υπάρχει ένας τύπος εκθέσεων που θα αφορά τη δουλεία του χρήστη – αναλυτή για την παρουσίαση της προόδου του.

30.Δυνατότητα Φιλτραρίσματος στις Εκθέσεις

Επιπλέον θα απαιτηθούν και κάποιες δυνατότητες φιλτραρίσματος και επεξεργασίας στις εκθέσεις. Ανάλογα με τις επιθυμίες του οργανισμού οι εκθέσεις πρέπει να φιλτράρονται αλλά και να δίνεται η δυνατότητα επεξεργασίας από τους ίδιους τους υπαλλήλους (όλων των επιπέδων και ρόλων) έτσι ώστε να μπορούν να εισαχθούν σε εργαλεία , όπως επεξεργαστές κειμένου και λογιστικών φύλλων. Για παράδειγμα οι χρήστες είναι δυνατόν να θελήσουν έναν κατάλογο με όλα τα αντίμετρα ελέγχου φυσικής προσπέλασης (physical access control) τα οποία έχουν χαμηλό κόστος και είναι πολύ αποτελεσματικά.

31.Δυνατότητα Επεξεργασίας των Εκθέσεων

Οι χρήστες θέλουν να μπορούν να δομούν τις εκθέσεις με βάση το προσωπικό τους ύφος και απαιτήσεις. Θα πρέπει κατά συνέπεια αν υπάρχει η δυνατότητα να σώζονται τα αποτελέσματα μιας ανάλυσης ερωτηματολογίων, καταλόγων σε μορφή τέτοια ώστε να είναι δυνατή στη συνέχεια η εισαγωγή τους σε μια ποικιλία από εργαλεία όπως επεξεργαστές κειμένου και σε προγράμματα λογιστικού φύλλο (spreadsheets).

32.Ερωτηματολόγια με Μορφή Φόρμας

Τα ερωτηματολόγια τα οποία θα παράγει το εργαλείο θα μπορούσαν ακόμα να έχουν τη μορφή μιας φόρμας ώστε οι απαντήσεις να είναι δυνατό να καταγράφονται κατευθείαν σε αυτή μαζί με άλλα στοιχεία της συνέντευξης, όπως όνομα χρήστη – αναλυτή, όνομα συνεντευξιαζόμενου, τόπος , ημερομηνία κ.α. και να βοηθούν στην εξεύρεση των αδύνατων σημείων του εξεταζόμενου πληροφοριακού συστήματος.

33.Προσεκτική Διατύπωση των Ερωτήσεων των Ερωτηματολογίων

Ιδιαίτερη σημασία θα πρέπει να δοθεί στα ερωτηματολόγια τα οποία πολλές φορές έχουν ένα μεγάλο αριθμό ερωτήσεων προς απάντηση, ενώ συχνά οι ερωτήσεις μπορεί να είναι μακροσκελείς και δυσανάγνωστες. Προκύπτει τελικά ότι η διατύπωση των ερωτήσεων των ερωτηματολογίων θα πρέπει να τις καθιστά συνοπτικές ,σαφείς, και κατανοητές ώστε να είναι εύκολη η διατύπωση τους προς τους χρήστες από τους χρήστες – αναλυτές. Το σύνολο αυτό των ερωτήσεων θα υποδεικνύει κατά πόσο είναι συμβατός ο οργανισμός με την ελληνική νομοθεσία.

34.Παρουσίαση Συνοδευτικών στις Ερωτήσεις Αναφορών Πληροφόρησης

Οι ερωτήσεις πρέπει να έχουν μια ακολουθία που να επιτρέπουν την ομαλή ροή της συνέντευξης. Δηλαδή οι ερωτήσεις που ακολουθούν θα πρέπει να εξειδικεύουν τις προηγούμενες ή να προσθέτουν κάτι καινούριο. Οι αντιφάσεις και οι αλληλεπικαλύψεις πρέπει να αποφεύγονται.

Επιπρόσθετα η κάθε ερώτηση θα μπορούσε να συνοδεύεται από σχετικές με αυτή αναφορές και κείμενα τα οποία θα αποσκοπούν στην πρόσθετη πληροφόρηση του χρήστη – αναλυτή και εμπλουτισμό των γνώσεων γύρω από την κάθε ερώτηση.

35.Ομαδοποίηση των Ερωτήσεων με Βάση την Κατηγορία Χρηστών Συστήματος

Στην ανάλυση της επικινδυνότητας θα πρέπει να εμπλακούν μια σειρά από χρήστες του πληροφοριακού συστήματος. Ανάμεσα σε αυτούς θα περιλαμβάνονται **διαχειριστές επιχειρήσεων** (business managers), **διαχειριστές έργων** (project managers) , **αναπτυκτές συστημάτων** (systems developers) και **διαχειριστές ασφαλείας.** Ως εκ τούτου η μέθοδος θα πρέπει να είναι χρήσιμη σε ανθρώπους

που έχουν διαφορετική άποψη για την ανάλυση της επικινδυνότητας, συνεπώς απαιτείται μια αντίστοιχη ποικιλία ερωτήσεων.

Τα ερωτηματολόγια θα πρέπει να περιέχουν ακριβώς εκείνες τις ερωτήσεις που είναι απαραίτητες για κάθε συγκεκριμένη ομάδα χρηστών του συστήματος. Θα μπορούσε να υπάρξει κάποιου είδους ομαδοποίηση των ερωτήσεων με βάση προδιαγεγραμμένες κατηγορίες χρηστών του συστήματος, ίσως σε σχέση με τη θέση τους στο οργανόγραμμα της εταιρείας (π.χ. διοικητικό συμβούλιο, χρήστης κ.α.)

36.Δυναμικό «Ξεδίπλωμα» των Ερωτήσεων

Το ερωτηματολόγιο θα μπορούσε να εξελίσσεται κατά τρόπο φαινομενικά δυναμικό. Σε μια τέτοια περίπτωση κάθε επόμενη ερώτηση θα εξαρτάται από τις προηγούμενες απαντήσεις που καταγράφει. Το γεγονός αυτό δείχνει ότι θα πρέπει να ορισθούν σχέσεις ανάμεσα στις ερωτήσεις ώστε να μην εμφανίζονται ερωτήσεις που είναι επικαλυπτόμενες ή αντιφατικές.

37.Ερωτηματολόγιο με ένα Ελάχιστο Σύνολο Ερωτήσεων

Επίσης θα μπορούσε να υπάρχει ένα ερωτηματολόγιο με ένα ελάχιστο σύνολο ερωτήσεων, οι απαντήσεις στις οποίες θα μπορούσαν να εκτιμήσουν το κατά πόσο κάποιος οργανισμός ή επιχείρηση είναι συμβατή με την ελληνική νομοθεσία.

38.Διαχείριση της Διαδικασίας Ανάλυσης και Διαχείρισης Επικινδυνότητας.

Η μέθοδος θα πρέπει να περιλαμβάνει μια σειρά οριζόντιων διαδικασιών που θα διευκολύνουν τη διαχείριση της ίδιας της ανάλυσης και διαχείρισης της επικινδυνότητας. Ανάμεσα σε αυτές τις διαδικασίες περιλαμβάνονται:

- Η καταγραφή στοιχείων χρήσιμων για την ανάλυση (π.χ. πελάτες, δημιουργοί, μετασχηματισμό, ιδιοκτήτη, κοσμοθεωρία, περιβάλλον).
- Η καταγραφή στοιχείων σχετικών με τις συνεντεύξεις που λαμβάνονται (π.χ. όνομα χρήστη – αναλυτή, όνομα συνεντευξιαζόμενου, τόπος , ημερομηνία).
- Η καταγραφή στοιχείων σχετικών με τον προγραμματισμό των συνεντεύξεων που θα πρέπει να ληφθούν.
- Για τον προγραμματισμό άλλων μελλοντικών εργασιών, με χρήση Gantt chart.
- Ένα μηχανισμό υπενθύμισης ημερομηνιών (reminders)
- Η ιχνηλάτηση του σημείου που βρίσκεται κάποιος (φάσεις που έχουν ολοκληρωθεί, βήματα που απομένουν).
- Δημιουργία εκθέσεων προόδου για τον χρήστη αναλυτή (progress reports).

39.Δυνατότητα Αλλαγής των Δεδομένων

Θα πρέπει να είναι δυνατή η αλλαγή των δεδομένων. Οι χρήστες θα μπορούν να προσαρμόζουν τα δεδομένα έτσι ώστε να είναι δυνατό να περιλαμβάνεται η ορολογία που χρησιμοποιείται σε ένα συγκεκριμένο οργανισμό. Επιπρόσθετα οι χρήστες μπορεί να θέλουν να προσθέσουν νέες ερωτήσεις, να τροποποιήσουν υπάρχουσες ερωτήσεις ή να προσθέσουν/ τροποποιήσουν τα δεδομένα των αντίμετρων.

40.Ευκολία Προσαρμογής στις Αλλαγές της Τεχνολογίας

Οι ταχύτατες αλλαγές της τεχνολογίας θα έχουν επίδραση σε οποιαδήποτε μέθοδο. Η μέθοδος θα πρέπει να είναι πάντα ενημερωμένη με τις τρέχουσες τεχνολογικές εξελίξεις και τις πιο σύγχρονες πρακτικές ασφαλείας. Η ευκολία με την οποία μια μέθοδος μπορεί να προσαρμοσθεί στο να αντιμετωπίζει τις αλλαγές της τεχνολογίας αποτελεί έναν σημαντικό παράγοντα.

41.Εργαλείο Φιλικό προς τον Χρήστη και Εύχρηστο

Το εργαλείο θα πρέπει να είναι φιλικό προς τον χρήστη και εύχρηστο. Στοιχεία που ενισχύουν αυτή την απαίτηση είναι το να μπορεί το εργαλείο να ενσωματώνει όλες τις λειτουργίες που παρέχονται από το περιβάλλον των Microsoft Windows (π.χ. cut, copy, paste, αξιοποίηση των λειτουργιών των παραθύρων, μέθοδοι minimize, maximize, scale window) on – line βοήθεια, και Tool Tips.

42. Εξαγωγή των Δεδομένων του Εργαλείου

Θα πρέπει να είναι δυνατή η εξαγωγή των δεδομένων της μεθόδου σε αρχεία με κάποια συνεπή μορφή. Η δυνατότητα αυτή θα μπορούσε να καταστήσει δυνατή τη λήψη των αρχείων από κάποιον άλλον χρήστη του εργαλείου και η συνέχιση της ανάλυσης και διαχείρισης της επικινδυνότητας. Στην περίπτωση αυτή θα πρέπει να εξετασθεί και η εφαρμογή ενός μηχανισμού ελέγχου των εκδόσεων των αρχείων, κατά αντιστοιχία με αυτόν που χρησιμοποιείται συχνά, κατά την ανάπτυξη λογισμικού.

Η διαδικασία αυτή θα μπορούσε να χρησιμεύει και ως μηχανισμός λήψης αντιγράφων ασφαλείας.

5.3 Απαιτήσεις από το Υλικό και το Λογισμικό

5.3.1 Λειτουργικό Σύστημα

Το βασικό λειτουργικό σύστημα του εργαλείου θα πρέπει να είναι το σύστημα Microsoft Windows. Οι εκδόσεις του συγκεκριμένου λειτουργικού συστήματος θα πρέπει να είναι από τις περισσότερο διαδεδομένες στην αγορά, για παράδειγμα οι εκδόσεις στις οποίες θα έπρεπε να λειτουργεί σήμερα θα ήταν τα Windows 2001,XP,Professional κ.α

5.3.2 Εναλλακτικό Λειτουργικό Σύστημα

Το λειτουργικό σύστημα Linux θα μπορούσε να αποτελεί εναλλακτικό λειτουργικό σύστημα του εργαλείου, με την προϋπόθεση ότι η ανάπτυξη του εργαλείου σε αυτό καλύπτεται με τους πόρους (άνθρωποι, υπάρχον λογισμικό, μεταγλωττιστές) που έχουν προβλεφθεί για την ανάπτυξη του βασικού λειτουργικού συστήματος.

5.3.3. Λειτουργία του Εργαλείου στο Περιβάλλον ενός Φορητού Προσωπικού Υπολογιστή

Καθότι η ανάλυση και η διαχείριση της επικινδυνότητας θεωρείται εργαλείο επικοινωνίας μεταξύ αναλυτή και διοίκησης, εξυπακούεται ότι οι συναντήσεις στο χώρο του οργανισμού του υπό εξέταση πληροφοριακού συστήματος θα είναι πολλές. Έτσι το εργαλείο θα πρέπει να μπορεί να εκτελείται στο περιβάλλον ενός επιτραπέζιου υπολογιστή (desktop PC), αλλά και ενός φορητού προσωπικού υπολογιστή (laptop PC) ,οι απαιτήσεις για τα οποία θα ικανοποιούνται από τις τρέχουσες ελάχιστες απαιτήσεις που θα καλύπτουν και τις δύο μορφές προσωπικού υπολογιστή, ώστε να διευκολύνεται η εργασία του αναλυτή.

5.4 Απαιτήσεις Απόδοσης

Καθότι οι συνθετότερες εργασίες προϋποθέτουν μεγαλύτερο χρόνο υλοποίησης ,πρέπει το εργαλείο να εκτελεί τις εργασίες αυτές μέσα σε εύλογο χρονικό διάστημα .Ο χρόνος που θα απαιτείται για να γίνουν οι πιο σύνθετες λειτουργίες του εργαλείου θα είναι 15', οι οποίες θα εκτελούνται σε ένα τελευταίας τεχνολογίας (state – of- the –art) μηχανήματα.

5.5 Μη Λειτουργικές Απαιτήσεις - Περιορισμοί

5.5.1 Ανάπτυξη με Βάση του ήδη Υπάρχοντες Πόρους

Η μέθοδος θα πρέπει να αναπτυχθεί με βάση τους ήδη υπάρχοντες πόρους σε υλικό και λογισμικό που υπάρχουν στο εργαστήριο Πληροφοριακών Συστημάτων και Βάσεων Δεδομένων. Καθότι η ερευνητική ομάδα εντάσσεται στο συγκεκριμένο εργαστήριο, πρέπει τόσο το υλικό και το λογισμικό που το εργαστήριο έχει να επαρκεί για την υλοποίηση του εργαλείου.

5.5.2. Όχι Εξάρτηση από Άλλες Εφαρμογές

Δεν θα πρέπει να απαιτείται για την λειτουργία του εργαλείου η αγορά άλλων πακέτων λογισμικού, με την έννοια ότι δεν θα πρέπει να υπάρχει εξάρτηση του από άλλες εφαρμογές λογισμικού.

5.6 Ειδικές Απαιτήσεις- Απαιτήσεις Ασφαλείας

5.6.1 Προστατευμένα Δεδομένα

- Τα δεδομένα της ανάλυσης και διαχείρισης της επικινδυνότητας (ειδικά οι πληροφορίες που αφορούν έναν οργανισμό) θα πρέπει να είναι προστατευμένα, έτσι ώστε να εξασφαλίζεται η διαθεσιμότητα, η ακεραιότητα και η εμπιστευτικότητα τους.
- Αν τα αποτελέσματα υποστούν αλλοίωση τότε αυτό θα μπορούσε να έχει ως συνέπεια την υλοποίηση λανθασμένου πιθανά συνόλου αντίμετρων.
- Η μη εξουσιοδοτημένη αποκάλυψη έχει ανάγκη ιδιαίτερης αναφοράς.
- Η απαίτηση να καταγράφονται οι αποφάσεις που αφορούν τις επιλογές αντίμετρων εισάγει ένα νέο είδος κινδύνου. Αν είναι δυνατή η ανακάλυψη των μέτρων που έχουν υλοποιηθεί από έναν άνθρωπο με κακές προθέσεις η πληροφορία αυτή μπορεί στη συνέχεια να χρησιμοποιηθεί για να βγουν συμπεράσματα σχετικά με τις περιοχές που δεν καλύπτονται από ένα συγκεκριμένο αντίμετρο.
- Η προστασία που παρέχεται για τα δεδομένα της ανάλυσης και διαχείρισης της επικινδυνότητας μπορεί να ενσωματωθεί μέσα στο ίδιο το εργαλείο. Εναλλακτικά το εργαλείο και τα αποτελέσματα θα μπορούσαν να φυλάσσονται σε ένα ασφαλές μέρος.

5.6.2 Έλεγχος της Διαδικασίας Αλλαγών στη Βάση Δεδομένων

Αν το εργαλείο επιτρέπει να πραγματοποιούνται αλλαγές στη βάση του (π.χ. αλλαγές στις ερωτήσεις και εισαγωγή νέων αντίμετρων) θα πρέπει να είναι δυνατό να ασκηθεί ένας υψηλού επιπέδου έλεγχος αυτή της διαδικασίας, συμπεριλαμβανομένου και ενός κατάλληλου μηχανισμού ελέγχου εκδόσεων (version control). Οι ανεξέλεγκτες αλλαγές στη βάση θα μπορούσαν να την καταστήσουν εντελώς άχρηστη. Σε αυτό το σημείο θα πρέπει να δοθεί προσοχή ιδιαίτερα αν επιτρέπεται να γίνονται αλλαγές στη βάση σε άτομα τα οποία δεν έχουν επαρκή εμπειρία σε θέματα ασφαλείας.

5.6.3 Σύστημα Ελέγχου Προσπέλασης

Προκύπτει ότι υπάρχουν τρεις τύποι χρηστών:

- Οι χρήστες που μπορούν να πραγματοποιήσουν την ανάλυση της επικινδυνότητας (είτε να δημιουργήσουν μια νέα ανάλυση ή να ενημερώσουν μια υπάρχουσα είδη).
- Οι χρήστες που μπορούν να τροποποιήσουν τη βάση δεδομένων.
- Χρήστες στους οποίους επιτρέπεται μόνο η ανάγνωση (συμπεριλαμβανομένης και της δυνατότητας να εκτυπώνει τα αποτελέσματα μιας ανάλυσης).

Υπάρχει κατά συνέπεια η απαίτηση για ένα σύστημα ελέγχου προσπέλασης το οποίο ξεχωρίζει τους παραπάνω τύπους χρηστών.

5.7 Σημεία Προβληματισμού

Η ανάλυση της επικινδυνότητας αποτελεί αναμφίβολα μια αρκετά πολύπλοκη διαδικασία. Παρά τις επισταμένες προσπάθειες και τη χρήση αυστηρών τεχνικών εξακολουθούν να εντοπίζονται ορισμένες δυσκολίες σε αυτή οι οποίες εξαιτίας της φύσης τους δεν έχουν αντιμετωπιστεί αποτελεσματικά από τις υπάρχουσες μεθόδους.

Προσδιορισμός της Επικινδυνότητας

Μια βασικά απαίτηση από μια μέθοδο ανάλυσης και διαχείρισης της επικινδυνότητας αποτελεί αυτή που αναφέρεται στην αντιμετώπιση όλων των σημαντικών σημείων επικινδυνότητας, ενώ αποτυχία ικανοποίηση της θα ήταν δυνατό να αποδειχτεί καταστροφική.

Όπως αναφέρθηκε προηγουμένως το πεδίο των τιμών της επικινδυνότητας είναι πολύ μεγάλο εξαιτίας του πλήθους και των πεδίων τιμών των μεταβλητών οι οποίες πρέπει να συμπεριληφθούν στη διαδικασία υπολογισμού της επικινδυνότητας. Το γεγονός αυτό έχει σαν συνέπεια την ύπαρξη τεράστιου αριθμού τιμών επικινδυνότητας οι οποίες θα πρέπει να προσδιοριστούν .Κατ' επέκταση είναι πιθανό περιστασιακά να μην προσδιοριστούν ορισμένες ,μικρής πιθανότητας , τιμές επικινδυνότητας.

Κόστος Μέσων Προστασίας

Η κοστολόγηση των αντίμετρων αποτελεί μια ιδιαίτερα δύσκολη διαδικασία. Ο ευκολότερος τρόπος να εξηγηθούν οι αιτίες για αυτό, είναι μέσα από την εξέταση ενός συγκεκριμένου παραδείγματος όπως την αντικατάσταση ενός τυπικού συστήματος ελέγχου προσπέλασης με ένα σύστημα βιομετρικών μεθόδων. Το κόστος θα περιελάμβανε μεταξύ των άλλων:

- Τον εντοπισμό και την επιλογή ενός συγκεκριμένου προϊόντος
- Το κόστος του καινούριου υλικού (hardware)
- Το κόστος ανάπτυξης συμπεριλαμβανομένης της ολοκλήρωσης με τις υπάρχουσες εφαρμογές
- Το κόστος εγκατάστασης
- Το λειτουργικό κόστος

Παρόλο που το υλικό θεωρείται εύκολο να κοστολογηθεί τα υπόλοιπα στοιχεία κόστους παρουσιάζουν αρκετή δυσκολία στον προσδιορισμό τους. Για παράδειγμα το λειτουργικό κόστος περιλαμβάνει το κόστος εγγραφής χρηστών, συντήρησης της βάσης δεδομένων, διαγραφή χρηστών, διερεύνηση περιπτώσεων λανθασμένης απόρριψης και συντήρησης του εξοπλισμού.

Γενικά οι πλειοψηφία των μέσων προστασίας έχει φύση διαδικαστική, ενώ το κόστος τους τις περισσότερες είναι δύσκολο αν όχι αδύνατο να υπολογιστεί με ακρίβεια.

Μειονεκτήματα από τη Χρήση Μηχανιστικών Προσεγγίσεων

Η χρήση ενός εργαλείου αποτελεί μια ελκυστική επιλογή και μάλιστα η βάση γνώσης που έχει δημιουργηθεί από διακεκριμένους ειδικούς, οι χρήστες θα δείχνουν και εμπιστοσύνη στα παραγόμενα αποτελέσματα. Στην περίπτωση αυτή υποτίθεται ότι οι χρήστες μελετούν με μεγάλη προσοχή όλα τα δεδομένα που εισάγουν στο εργαλείο. Δυστυχώς όμως όσο αποκτούν εμπειρία με αυτό υπάρχει πάντα ο κίνδυνος να αναπτύξουν μια μηχανιστική αντιμετώπιση της ανάλυσης της επικινδυνότητας. Αν οι χρήστες εισάγουν δεδομένα χωρίς να σκέφτονται τους κινδύνους, τα αποτελέσματα θα παρουσιάζουν σημαντικά μειωμένη αξία.

Η Αποτελεσματικότητα των Μέσων Προστασίας

Τα αντίμετρα συνδυάζονται συνήθως με ένα μέτρο της αποτελεσματικότητας τους. Μερικά μέτρα παρουσιάζουν πολύ υψηλή αποτελεσματικότητα προδιαθέτοντας ότι τέτοιου είδους μέτρα θα παρέχουν υψηλά επίπεδα προστασίας. Δυστυχώς αυτό δεν συμβαίνει σε όλες τις περιπτώσεις όπως για παράδειγμα σε αυτές όπου δεν έχει γίνει σωστή υλοποίηση των μέσων προστασίας έχοντας ως συνέπεια τη δημιουργία μιας ψευδούς αίσθησης ασφαλείας.

Τροποποίηση της Βάσης Γνώσης

Όπως αναφέρθηκε σε σχετική απαίτηση θα πρέπει να είναι δυνατή η τροποποίηση των δεδομένων. Για παράδειγμα θα πρέπει να επιτρέπεται σε κάποιον να κάνει εισαγωγή, διαγραφή και τροποποίηση των ερωτήσεων, Ωστόσο μια τέτοια δυνατότητα δημιουργεί μια σειρά προβλημάτων:

- Είναι δυνατόν να διαγραφούν σημαντικές ερωτήσεις χωρίς να γίνονται αντιληπτές οι συνέπειες αυτής της πράξης.
- Είναι επίσης δυνατόν να εισαχθούν άχρηστες και παράλογες ερωτήσεις.
- Η αλλαγή αριθμητικών τιμών μπορεί να προκαλέσει την απαξίωση των αποτελεσμάτων.

Αναμφισβήτητα θα πρέπει να διασφαλίζεται ο έλεγχος και η επικύρωση της διαδικασίας τροποποίησης των δεδομένων, διαφορετικά οι αλλαγές θα μπορούσαν να καταστήσουν το εργαλείο άχρηστο.

Επίσης κρίνεται πως οι τροποποιήσεις που θα απαιτείται να γίνονται θα πρέπει να αναθέτονται σε άτομα με αρκετή εμπειρία σε θέματα ασφαλείας.

5.8. Κριτική - Σύνοψη

Όπως έχει ήδη αναφερθεί το εργαλείο θα τύχει χρήσης από ερευνητική ομάδα, έτσι δεν απαιτείται η ευχρηστία του εργαλείου για να υλοποιηθεί το ίδιο. Η εμπειρία και οι γνώσεις της ομάδας είναι σε θέση να ξεπεράσουν το εμπόδιο αυτό. Έτσι θα μπορούσαμε να θεωρήσουμε την ύπαρξη μιας αυστηρής μεθόδου και της απαίτησης το εργαλείο να είναι εύχρηστο και φιλικό περιττές. Βέβαια αυτό δεν σημαίνει ότι πρέπει το εργαλείο να είναι εξαιρετικά στρυφνό.

Επίσης πολλές από τις πιο πάνω απαιτήσεις θα μπορούσαν να παραληφθούν καθώς ορισμένες από αυτές αποτελούν η μια επακόλουθο της άλλης. Για παράδειγμα οι απαιτήσεις για την μορφή των εκθέσεων θα μπορούσαν να ενσωματωθούν σε μια (Διαφορετικές μορφές εκθέσεων – δυνατότητα φιλτραρίσματος και επεξεργασίας). Το ίδιο ισχύει και για τα αντίμετρα (Αντίμετρα γενικά, ειδικά και οικονομικώς αποδεκτά). Παρόλα αυτά προτίμησα στην συγκεκριμένη εργασία να γίνει μια λεπτομερής περιγραφή των απαιτήσεων προκειμένου να αποφευχθούν παρανοήσεις σχετικά με τη σχεδίαση του εργαλείου.

5.9 Τοποθέτηση Στοιχείων Προτεραιότητας στις Απαιτήσεις

Στον παρακάτω πίνακα δίδεται η κλίμακα που θα χρησιμοποιηθεί για την τοποθέτηση χαρακτηριστικών προτεραιότητας στις απαιτήσεις.

Κλίμακα τοποθέτησης χαρακτηριστικών προτεραιότητας στις απαιτήσεις

Απαραίτητη - Essential	Το προϊόν δεν γίνεται αποδεκτό αν δεν ικανοποιηθούν αυτού του είδους οι απαιτήσεις.
Γενόμενη υπό Όρους - Conditional	Θα ενίσχυαν το προϊόν μα αν μείνουν ανικανοποίητες δεν θα το καταστήσουν αποδεκτό
Προαιρετική - Optional	Λειτουργίες οι οποίες ίσως αξίζει να ικανοποιηθούν, ίσως και όχι

Αξιολόγηση Απαιτήσεων με Βάση Την Κλίμακα Προτεραιοτήτων

Απαίτηση	Προτεραιότητα
1. Φάσεις- Βήματα του Εργαλείου	Απαραίτητη
1.1 Φάση 1η:Ορισμός του προβλήματος	Απαραίτητη
1.1.1 Ορισμός του Συστήματος	Απαραίτητη
1.1.2 Προσδιορισμός των Ορίων του Συστήματος	Απαραίτητη
1.1.3 Διαγραμματικές Τεχνικές Ανάλυσης και Μοντελοποίησης	Απαραίτητη
1.2 Φάση 2η: Ανάλυση της Επικινδυνότητας	Απαραίτητη
1.2.1 Αποτίμηση των Περιουσιακών Αγαθών του Οργανισμού	Απαραίτητη
1.2.2 Προσδιορισμός και Αποτίμηση των Απειλών και Αδυναμιών	Απαραίτητη
1.2.3 Υπολογισμός της Συνολικής Επικινδυνότητας	Απαραίτητη
1.3 Φάση 3η: Υλοποίηση	Απαραίτητη
1.4 Φάση 4η: Παρακολούθηση	Απαραίτητη
1.5 Φάση 5η: Αναθεώρηση	Απαραίτητη
2. Εφαρμογή σε κάθε Στάδιο του Κύκλου Ζωής της Ανάπτυξης Του Λογισμικού	Απαραίτητη
3. Προσαρμογή στην Ελληνική Γλώσσα/	Απαραίτητη

Δεδομένα / Κουλτούρα	
4. Εφαρμογή σε Μεγάλου Μεγέθους Οργανισμούς	Απαραίτητη
5. Εφαρμογή σε Διάφορους Επιχειρηματικούς Κλάδους ή Τύπου Επιχειρήσεων και Οργανισμών	Απαραίτητη
6.Εργαλείο Ευθυγραμμισμένο ως προς την Ελληνική και Ευρωπαϊκή Νομοθεσία	Απαραίτητη
7. Αλληλεξαρτήσεις των Διαφορετικών Συστημάτων	Απαραίτητη
8. Ύπαρξη Διάφορων Επιπέδων Λεπτομέρειας μιας Ανάλυσης	Απαραίτητη
9. Εφαρμογή της Μεθόδου Γρήγορα και Αποτελεσματικά	Απαραίτητη
10. Βασικός Μηχανισμός	Απαραίτητη
11. Συνδυασμοί Τιμών	Απαραίτητη
12. Τιμές Επικινδυνότητας	Απαραίτητη
13. Δυνατότητα Ορισμού ενός Αποδεκτού Επιπέδου Επικινδυνότητας	Γενόμενη Υπό Όρους
14. Το Εργαλείο να Υποδεικνύει που Βρίσκονται τα Σημαντικότερα Προβλήματα	Γενόμενη Υπό Όρους
15. Μέθοδος Αυστηρή	Γενόμενη Υπό Όρους
16. Ενσωμάτωση της Επιχειρηματικής Επικινδυνότητας	Γενόμενη Υπό Όρους
17. Γενικές Απειλές και Αδυναμίες	Γενόμενη Υπό Όρους
18. Ειδικά και Λεπτομερή Αντίμετρα	Απαραίτητη
19. Οικονομικώς Αποδοτικά Αντίμετρα	Απαραίτητη
20. Ισορροπημένο Σύνολο από Αντίμετρα	Απαραίτητη
21. Μέτρα που να Βοηθούν στην Αποδοχή των Υπόλοιπων Αντιμέτρων	Απαραίτητη
22. Η Μέθοδος Λαμβάνει Υπόψη τις Πιθανές Αρνητικές Επιπτώσεις από την Υιοθέτηση Αντιμέτρων	Γενόμενη Υπό Όρους
23. Σύνδεση Αντιμέτρων με Δηλώσεις Πολιτικών Ασφαλείας	Απαραίτητη
24. Δήλωση Τύπου Σχέσης Ανάμεσα σε Δηλώσεις Πολιτικής Ασφαλείας	Απαραίτητη
25. Δυνητικός Χρόνος Επανάληψης της Ανάλυσης Επικινδυνότητας	Προαιρετική
26. Δυνατότητα Πειραματισμού μα Διαφορετικά Σενάρια	Γενόμενη Υπό Όρους
27. Δυνατότητα Ιχνηλάτησης	Απαραίτητη
28. Επαλήθευση των Αποτελεσμάτων μέσα από την Επανάληψη	Απαραίτητη
29. Εκθέσεις για τη Διοίκηση και Εκθέσεις Τεχνικές	Απαραίτητη
30. Δυνατότητα Φιλτραρίσματος	Απαραίτητη
31.Δυνατότητα Επεξεργασίας Εκθέσεων	Απαραίτητη
32. Ερωτηματολόγια με τη Μορφή Φόρμας	Γενόμενη Υπό Όρους
33. Προσεκτική Διατύπωση των Ερωτήσεων των Ερωτηματολογίων	Απαραίτητη
34. Παρουσίαση Συνοδευτικών στις Ερωτήσεις Αναφορών Πληροφόρησης	Γενόμενη Υπό Όρους
35. Ομαδοποίηση των Ερωτήσεων με Βάση την	Γενόμενη Υπό Όρους

Κατηγορία Χρηστών Του Συστήματος	
36. Δυναμικό «Ξεδίπλωμα» των Ερωτήσεων	Απαραίτητη
37. Ερωτηματολόγιο με ένα Ελάχιστο Σύνολο Ερωτήσεων	Προαιρετική
38. Διαχείριση της Διαδικασίας Ανάλυσης και Διαχείρισης της Επικινδυνότητας	Γενόμενη Υπό Όρους
39.Δυνατότητα Αλλαγής των Δεδομένων	Απαραίτητη
40.Ευκολία Προσαρμογής στις Αλλαγές της Τεχνολογίας	
41. Εργαλείο Φιλικό προς τον Χρήστη και Εύχρηστο	Απαραίτητη
42. Εξαγωγή των Δεδομένων του Εργαλείου	Απαραίτητη
43. Λειτουργικό Σύστημα	Απαραίτητη
44. Εναλλακτικό Λειτουργικό Σύστημα	Γενόμενη Υπό Όρους
45. Λειτουργία του Εργαλείου στο Περιβάλλον ενός Φορητού Προσωπικού Υπολογιστή	Απαραίτητη
46. Προστατευμένα Δεδομένα	Απαραίτητη
47. Έλεγχος της Διαδικασίας Αλλαγών στη Βάση Δεδομένων	Απαραίτητη
48.Σύστημα Ελέγχου Προσπέλασης	Γενόμενη Υπό Όρους
49. Χρόνος για τις Σύνθετες Εργασίες	Γενόμενη Υπό Όρους
50. Ανάπτυξη με Βάση τους Ήδη Υπάρχοντες Πόρους	Απαραίτητη
51. Όχι Εξάρτηση από Άλλες Εφαρμογές	Απαραίτητη
52. Κόστος	Απαραίτητη

Σχόλια

Το εργαλείο θα πρέπει να **τυγχάνει χρήσης από ερευνητές του εκάστοτε ιδρύματος που θα αναλάβει τη σχεδίαση του και αυτοσκοπός του είναι και παραμένει να είναι η ανάλυση.** Αυτό όμως δεν αποκλείει και τη χρήση του από άλλους οργανισμούς, βασιζόμενοι όμως στην παραδοχή ότι αυτοί είναι γνώστες του χώρους της ασφάλειας των πληροφοριακών συστημάτων. Παρόλα αυτά το εργαλείο δεν μπορεί να θεωρηθεί αυτοπρασαρμοζόμενο αλλά παραμένει ένα κλασικό εργαλείο. Μέσα από ένα πλήθος αναλύσεων θα συλλέγονται στοιχεία όπου με κατάλληλη επεξεργασία θα συντελούν σε μια νέα έκδοση.

Επιπλέον ένα μειονέκτημα των εργαλείων ανάλυσης και διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων είναι η διαδικασία μοντελοποίησης της ασφάλειας πληροφοριών. Μπορεί να υπάρχουν πολλά σχετικά μοντέλα, παρόλα αυτά η μοντελοποίηση κρίνεται δύσκολη καθώς απαιτείται πλήρης ορισμός του τι είναι πληροφορία. Κατ' επέκταση και η μοντελοποίηση του οργανισμού κρίνεται δύσκολη.

Παρότι η μοντελοποίηση του οργανισμού με δυναμικό και στατικό τρόπο είναι επιθυμητή , προς το παρόν, **μόνο η μοντελοποίηση των διαδικασιών είναι εφικτή.** Μια άλλη μοντελοποίηση (π.χ. οντολογίας που ερμηνεύει δεδομένα) είναι πιο ευφυής, έξυπνη αλλά όχι τόσο πρακτική αυτή τη στιγμή. Η μοντελοποίηση αυτή είναι και η αδυναμία που παρουσιάζουν τα υπάρχοντα εργαλεία.

Συγκεκριμένα το μοντέλο των περιουσιακών στοιχείων (asset model) που παράγουν τα εργαλεία αυτά δεν βοηθούν τον αναλυτή, αλλά τον αναγκάζουν να παρέμβει ο ίδιος ώστε να παραχθεί το σωστό μοντέλο, ιδίως στους μεγάλους οργανισμούς. Δηλαδή αντί να είναι απλοϊκό, διευκολύνοντας την περαιτέρω ανάλυση, την περιπλέκει.

Επιπλέον **οι τιμές επικινδυνότητας που παράγονται στα περισσότερα εργαλεία είναι «κλειδωμένες» , δηλαδή δεν μπορούν να μεταβληθούν.** Αυτό έχει σαν αποτέλεσμα τον περιορισμό του πεδίου δράσης του αναλυτή καθώς δεν του δίνεται η δυνατότητα όταν αντιλαμβάνεται από την εμπειρία του και τις ιδιαιτερότητες του προς ανάλυση οργανισμού ότι οι τιμές επικινδυνότητας δεν συμβαδίζουν με την πραγματική κατάσταση. Το εργαλείο θα υποστηρίζει τον αναλυτή , οπότε πρέπει να έχει την ευχέρεια να επεμβαίνει όποτε κρίνεται αναγκαίο.

Ένα άλλο σημείο που χρήζει περαιτέρω εξήγησης είναι και η αιτιολόγηση **μέσω σεναρίων (case based reasoning).** Σε αυτήν την περίπτωση η χρήση ερωτηματολογίων κρίνεται περιττή αφού η βάση σεναρίων θα επιλέγει κάθε φορά το σενάριο που πλησιάζει τον συγκεκριμένο προς εξέταση – ανάλυση οργανισμό. Δηλαδή, το πλησιέστερο σενάριο θα προσαρμόζεται στα εκάστοτε δεδομένα. Τα σενάρια θα πρέπει να είναι οργανωμένα και παραμετροποιημένα προς χρήση.

Επίσης πολλές φορές κρίνεται αναγκαία η απαίτηση για διαχείριση της διαδικασίας της ανάλυσης και της διαχείρισης της επικινδυνότητας. Συγκεκριμένα πιστεύεται ότι είναι χρήσιμο να υπάρχουν κάποιοι μηχανισμοί που να παρακολουθούν την ροή της διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων, την υλοποίηση της πολιτικής ασφαλείας και των αντίμετρων, γιατί έτσι η διοίκηση θα είναι σε θέση να ελέγχει την πορεία υλοποίησης και να λαμβάνει κάποια σήματα σε περίπτωση προβλήματος.

Το σημαντικότερο συμπέρασμα όμως **είναι η ανάγκη για ένα έξυπνο εργαλείο.** Θεωρείται ότι είναι απαραίτητο να έχει το εργαλείο κάποια «εξυπνάδα», κάποια νοημοσύνη (intelligent, smart tool). Πάντως δεν έχει βρεθεί ακόμα τρόπος για το πώς μπορεί να ενσωματωθεί αυτή η εξυπνάδα στο εργαλείο, αν και αποτελεί επιθυμία να δούμε στο μέλλον ένα καινούριο εργαλείο πιο έξυπνο ή να βελτιωθεί ως προς το σημείο αυτό ένα υπάρχον εργαλείο με μια νέα έκδοση του.

Μετά την επεξεργασία των απαιτήσεων είμαστε πλέον σε θέση να προχωρήσουμε στην ανάλυση των απαιτήσεων. Στα επόμενα κεφάλαια πραγματοποιείται η ανάλυση των απαιτήσεων και η σχεδίαση (στο μέγιστο δυνατό σημείο) ακολουθώντας το μοντέλο του κύκλου ζωής λογισμικού του IEEE.

ΚΕΦΑΛΑΙΟ 6

Έγγραφο Περιγραφής Απαιτήσεων Λογισμικού(ΕΠΑΛ)

Όπως προαναφέρθηκε η ανάλυση απαιτήσεων θα ακολουθήσει το μοντέλο του κύκλου ζωής του λογισμικού IEEE. Στο κεφάλαιο αυτό θα παραχθεί το Έγγραφο Περιγραφής Απαιτήσεων Λογισμικού (καθώς το υπό εξέταση εργαλείο είναι λογισμικό), όπως αυτό προσδιορίζεται από το πρότυπο ANSI/IEEE Std 830-1984. Θα προσπαθήσουμε να διατηρήσουμε την πρότυπη μορφή του προσαρμόζοντας το στις ανάγκες της εργασίας αυτής.

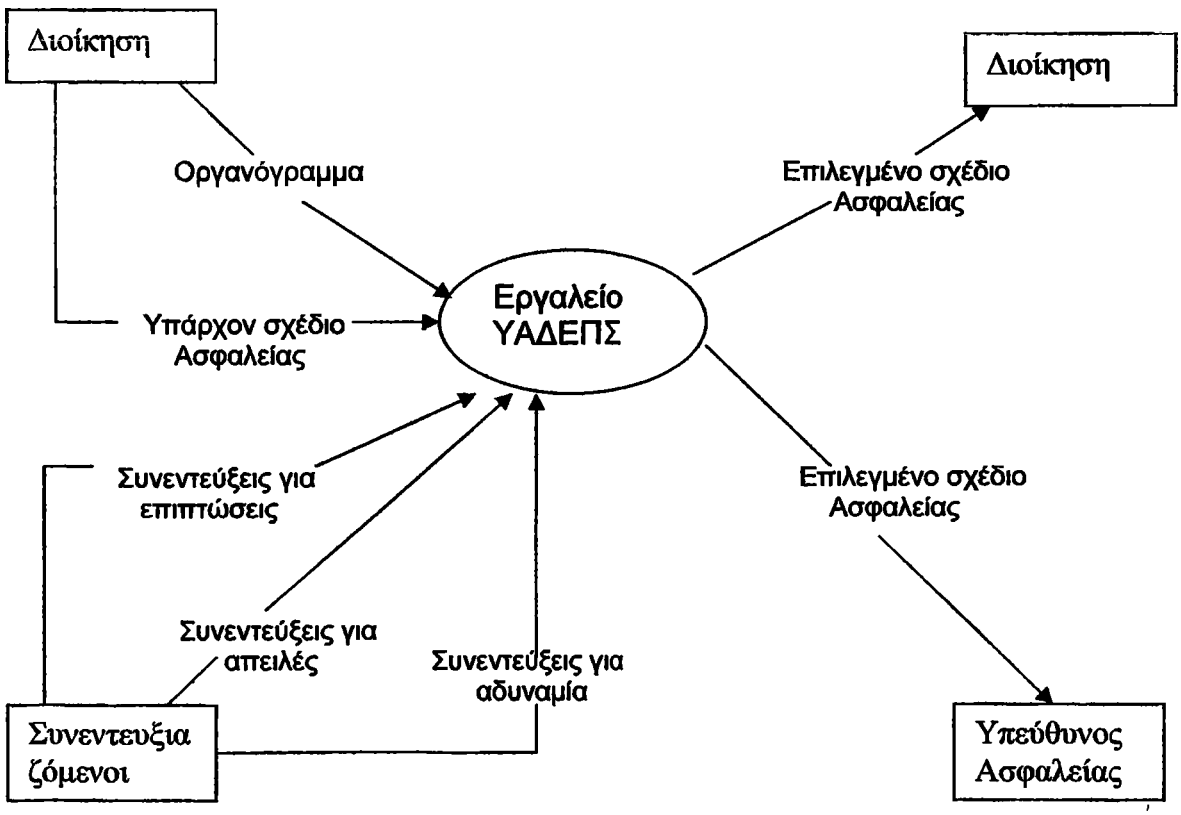
6.1 Διαγράμματα Ροής Δεδομένων και Λεξικό Δεδομένων

Προτού περιγραφεί το ΕΠΑΛ πρέπει να παρατεθούν τα ΔΡΔ και το σχετικό Λεξικό Δεδομένων. Τα ΔΡΔ που θα παρουσιαστούν θεωρούνται επικυρωμένα έτσι ώστε να προχωρήσει η σχεδίαση του εργαλείο – λογισμικού αυτού.

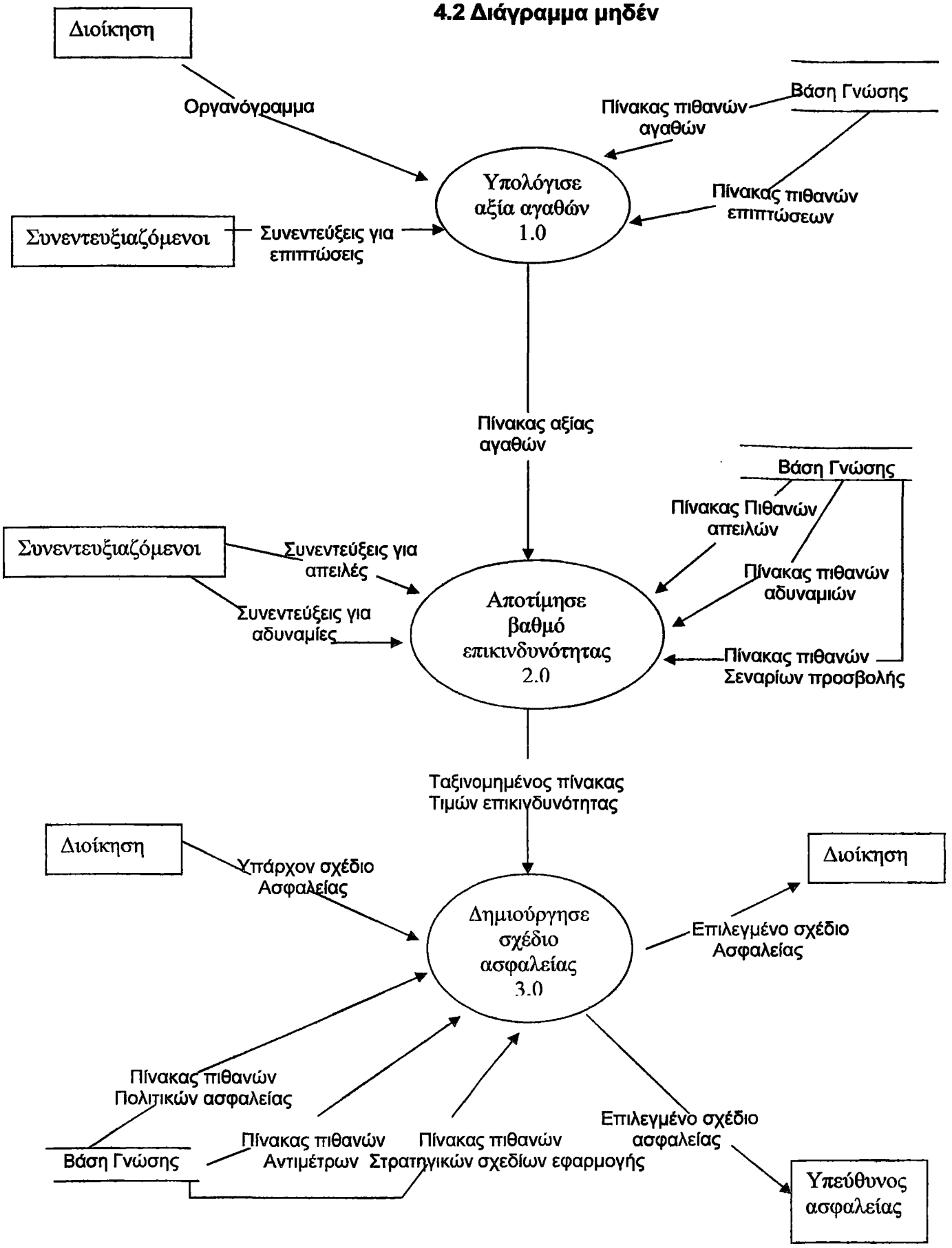
6.1.1. Διαγράμματα Ροής Δεδομένων

Παρακάτω παρατίθενται τα ΔΡΔ ξεκινώντας από το Διάγραμμα Πλαίσιο και προχωρώντας στα παρακάτω επίπεδα. Το τελικό ΔΡΔ έχει παραληφθεί για λόγους διευκόλυνσης.

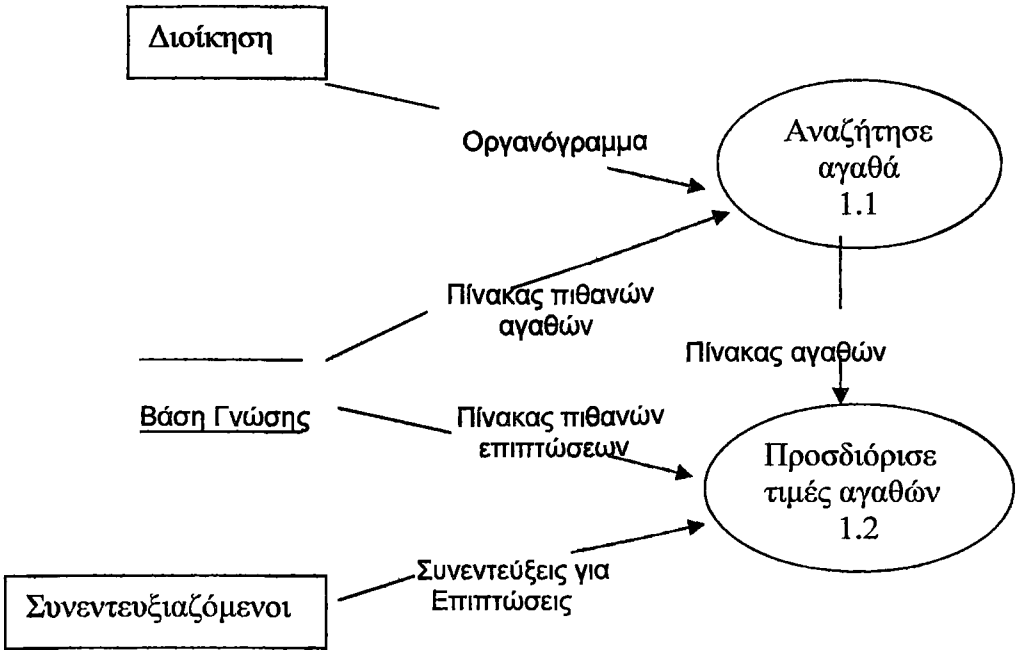
4.1 Διάγραμμα Πλαίσιο



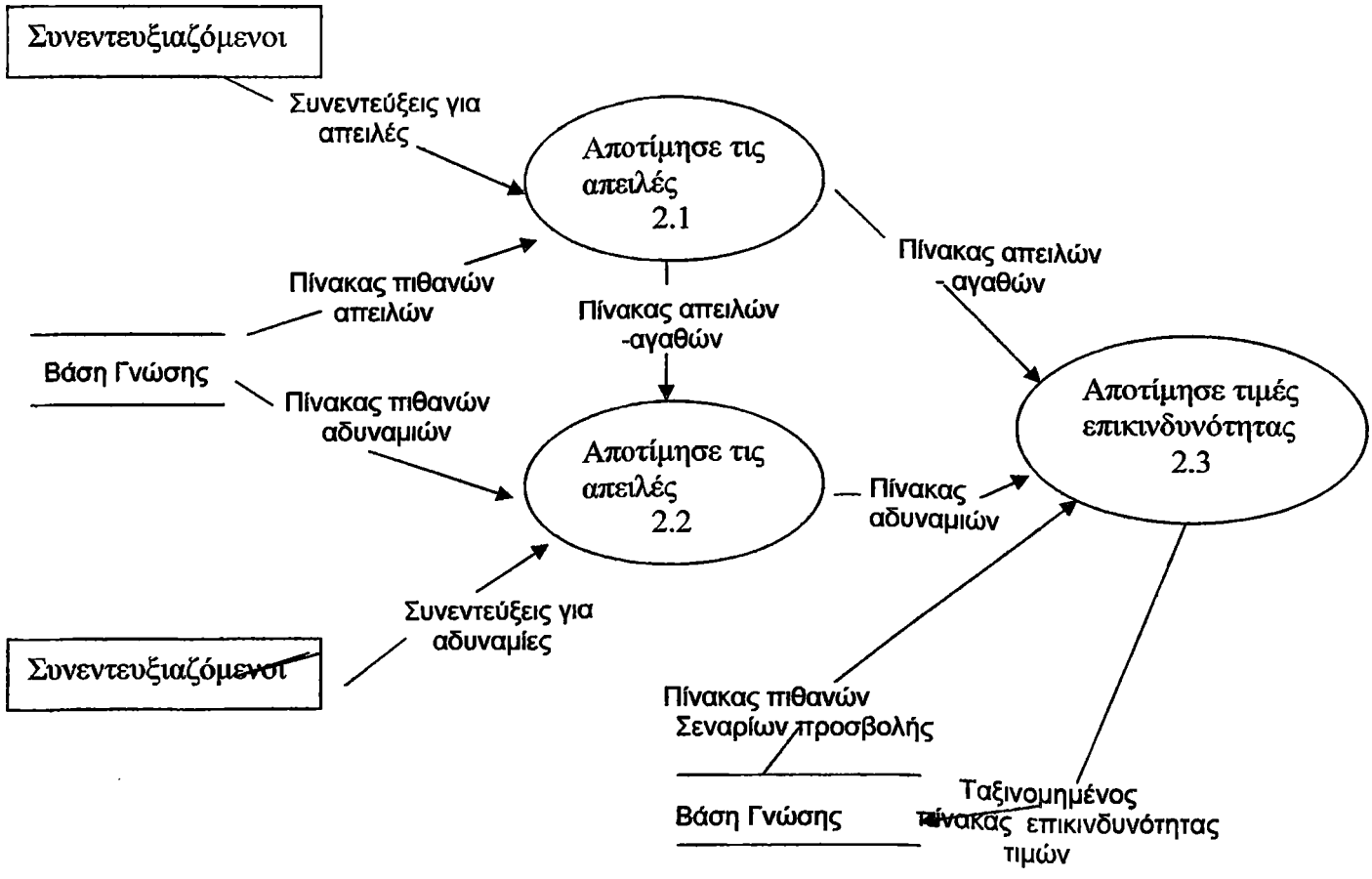
4.2 Διάγραμμα μηδέν



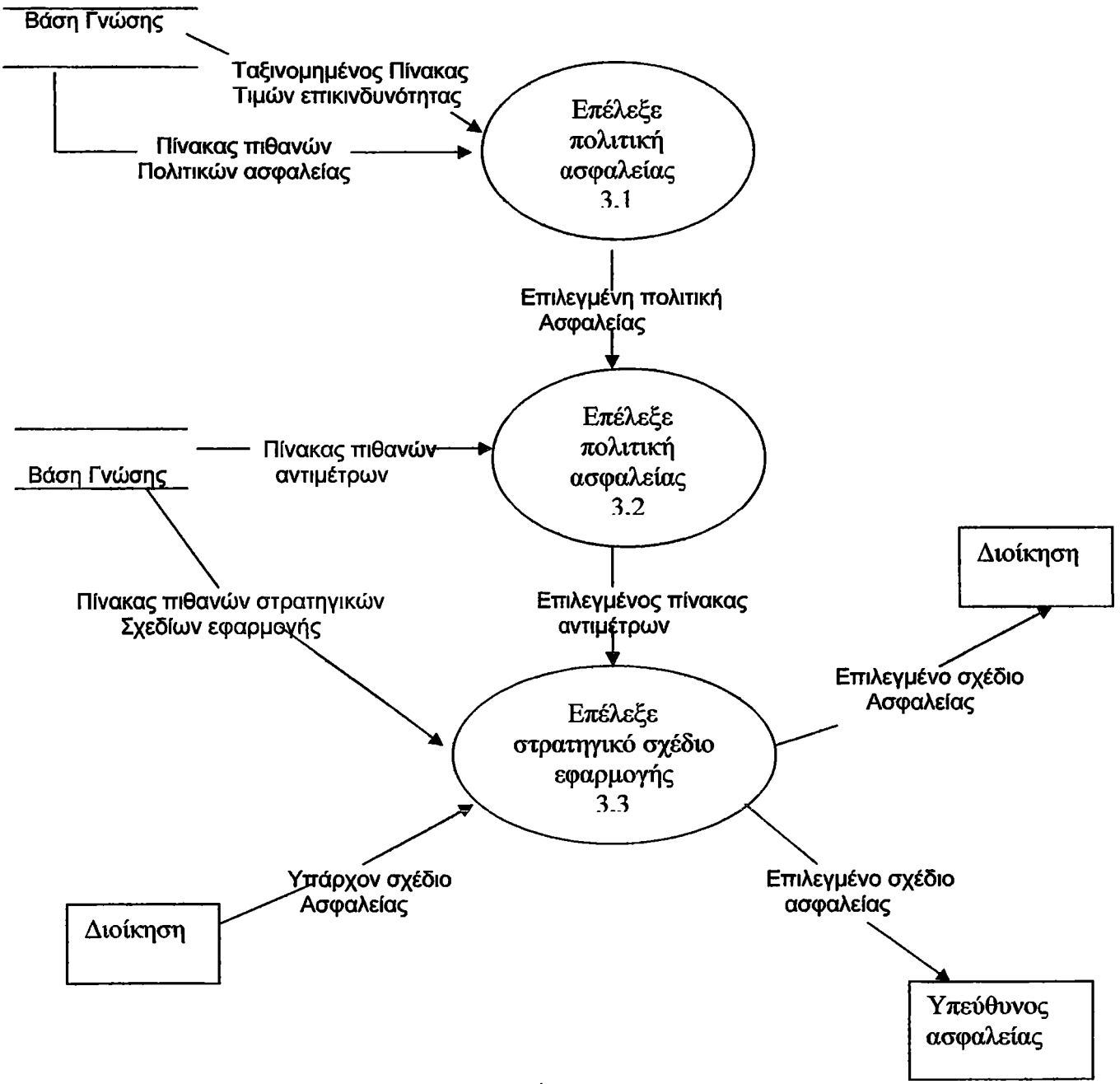
4.3 Υπολόγισε Αξία Αγαθών 1.0



4.4 Αποτίμησε Βαθμό Επικινδυνότητας 2.0



4.5 Δημιούργησε Σχέδιο Ασφαλείας 3.0



6.1.2 Λεξικό Δεδομένων

Στο λεξικό δεδομένων περιλαμβάνονται ορισμοί δεδομένων, των αποθηκευτικών χώρων και των εξωτερικών οντοτήτων (πηγές /καταλήξεις) του Διαγράμματος Ροής Δεδομένων. Οι ορισμοί παρατίθενται ξεκινώντας από το Διάγραμμα Πλαίσιο και προχωρώντας στα παρακάτω επίπεδα.

ΔΙΟΙΚΗΣΗ	Τα ανώτερα στελέχη του προς εξέταση οργανισμού που μπορούν να παρέχουν πληροφορίες σχετικά με το ΟΡΓΑΝΟΓΡΑΜΜΑ και με το ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ που προϋπάρχει της ανάλυσης και επικυρώνουν το ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ (καθώς και τα ενδιάμεσα προϊόντα του σχεδίου αυτού).
ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΙ	Το σύνολο των υπαλλήλων του προς εξέταση οργανισμού που επιλέγει ο αναλυτής και είναι σε θέση να παρέχουν πληροφορίες για τον προσδιορισμό του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ, του ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ – ΑΓΑΘΩΝ και του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ
ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ	Ο υπάλληλος του προς εξέταση οργανισμού που είναι υπεύθυνος του τομέα ασφαλείας και διαχειρίζεται – επιβλέπει το ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ. Μπορεί ύστερα από εισήγηση του αναλυτή (μέσα από το ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ) και αποδοχή από τη ΔΙΟΙΚΗΣΗ το άτομο αυτό να είναι διαφορετικό σε σχέση με εκείνο πριν της ανάλυση.
ΟΡΓΑΝΟΓΡΑΜΜΑ	Διάγραμμα που παρέχεται από τη ΔΙΟΙΚΗΣΗ και απεικονίζει στατικά τον προς εξέταση οργανισμό. Δείχνει τις σχέσεις μεταξύ των τμημάτων.
ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ	Το σχέδιο ασφαλείας που παρέχεται από τη ΔΙΟΙΚΗΣΗ του προς εξέταση οργανισμού και προϋπάρχει της ανάλυσης που πρόκειται να πραγματοποιηθεί.
ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ	Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ για τον υπό εξέταση οργανισμό.
ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΠΕΙΛΕΣ	Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ –ΑΓΑΘΩΝ για τον υπό εξέταση οργανισμό
ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ	Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΔΥΝΑΜΙΩΝ για τον υπό εξέταση οργανισμό
ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ	Το σχέδιο ασφαλείας που παραδίδεται από στη ΔΙΟΙΚΗΣΗ από τον αναλυτή ύστερα από επικύρωση

ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με αγαθά του τυχόν ο υπό εξέταση οργανισμός έχει με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΓΑΘΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με επιπτώσεις πάνω στα αγαθά του υπό εξέταση οργανισμού για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ
ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ	Πίνακας με τα αγαθά του υπό εξέταση οργανισμού και την αξία για καθένα από αυτά.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανές απειλές για τον υπό εξέταση οργανισμό για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ – ΑΓΑΘΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείο με αδυναμίες που τυχόν ο υπό εξέταση οργανισμός έχει για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανά σενάρια προσβολής(τριάδες αγαθό- απειλή-αδυναμία) του υπό εξέταση οργανισμού με σκοπό την παραγωγή του ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ.
ΤΑΞΙΝΟΜΗΜΕΝΟΣ ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ	Πίνακας με τιμές επικινδυνότητας για κάθε αγαθό του υπό εξέταση οργανισμού ταξινομημένες κατά φθίνουσα σειρά.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πολιτικές ασφαλείας με σκοπό την ΕΠΙΛΟΓΗ της ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ για τον υπό εξέταση οργανισμό.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΝΤΙΜΕΤΡΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανά αντίμετρα για τον υπό εξέταση οργανισμό με σκοπό την παραγωγή του ΕΠΙΛΕΓΜΕΝΟΥ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με στρατηγικά σχέδια εφαρμογής για την παραγωγή του ΕΠΙΛΕΓΜΕΝΟΥ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ για τον υπό εξέταση οργανισμό.

ΠΙΝΑΚΑΣ ΑΓΑΘΩΝ	Πίνακας με τα αγαθά του υπό εξέταση οργανισμού για την παραγωγή του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ
ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ	Πίνακας με συνδυασμούς απειλών για κάθε αγαθό του υπό εξέταση οργανισμού με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ και ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

ΠΙΝΑΚΑΣ ΑΔΥΝΑΜΙΩΝ	Πίνακας με τις αδυναμίες του υπό εξέταση οργανισμού με σκοπό την παραγωγή του ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ	Η πολιτική ασφαλείας που επιλέγεται για τον υπό εξέταση οργανισμό από τον αναλυτή και επικυρώνεται από τη ΔΙΟΙΚΗΣΗ.
ΕΠΙΛΕΓΜΕΝΟΣ ΠΙΝΑΚΑΣ ΑΝΤΙΜΕΤΡΩΝ	Πίνακας με τα αντίμετρα που επιλέγονται από τον αναλυτή και επικυρώνονται από τα η ΔΙΟΙΚΗΣΗ του υπό εξέταση οργανισμού.
ΒΑΣΗ ΓΝΩΣΗΣ	Περιλαμβάνει δεδομένα σχετικά με τα αγαθά, επιπτώσεις, απειλές, αδυναμίες, σενάρια προσβολής, αντίμετρα, πολιτικές ασφαλείας και στρατηγικά σχέδια εφαρμογής.
ΥΑΔΕΠΣ	Υποστήριξη της Ανάλυσης και Διαχείρισης της Επικινδυνότητας Πληροφοριακών Συστημάτων.

ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με αγαθά του τυχόν ο υπό εξέταση οργανισμός έχει με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΓΑΘΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με επιπτώσεις πάνω στα αγαθά του υπό εξέταση οργανισμού για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ
ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩ	Πίνακας με τα αγαθά του υπό εξέταση οργανισμού και την αξία για καθένα από αυτά.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανές απειλές για τον υπό εξέταση οργανισμό για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ – ΑΓΑΘΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείο με αδυναμίες που τυχόν ο υπό εξέταση οργανισμός έχει για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΑΔΥΝΑΜΙΕΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανά σενάρια προσβολής(τριάδες αγαθό- απειλή-αδυναμία) του υπό εξέταση οργανισμού με σκοπό παραγωγή του ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ.
ΤΑΞΙΝΟΜΗΜΕΝΟΣ ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ	Πίνακας με τιμές επικινδυνότητας για κάθε αγαθό του εξέταση οργανισμού ταξινομημένες κατά φθίνουσα σειρά.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πολιτικές ασφαλείας με σκοπό την ΕΠΙΛΟΓΗ της ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ για τον υπό εξέταση οργανισμό.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με

ΑΝΤΙΜΕΤΡΩΝ	πιθανά αντίμετρα για τον υπό εξέταση οργανισμό με σκοπό την παραγωγή του ΕΠΙΛΕΓΜΕΝΟΥ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ.
ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ	Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με στρατηγικά σχέδια εφαρμογής για την παραγωγή ΕΠΙΛΕΓΜΕΝΟΥ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ για τον υπό εξέταση οργανισμό.
ΠΙΝΑΚΑΣ ΑΓΑΘΩΝ	Πίνακας με τα αγαθά του υπό εξέταση οργανισμού για παραγωγή του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ
ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ ΑΓΑΘΩΝ	Πίνακας με συνδυασμούς απειλών για κάθε αγαθό του ι εξέταση οργανισμού με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ και ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
ΠΙΝΑΚΑΣ ΑΔΥΝΑΜΙΩΝ	Πίνακας με τις αδυναμίες του υπό εξέταση οργανισμού με σκοπό την παραγωγή του ΤΑΞΙΝΟΜΗΜΕΝΟΥ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ
ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ	Η πολιτική ασφαλείας που επιλέγεται για τον υπό εξέταση οργανισμό από τον αναλυτή και επικυρώνεται από τη ΔΙΟΙΚΗΣΗ.
ΕΠΙΛΕΓΜΕΝΟΣ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ	Πίνακας με τα αντίμετρα που επιλέγονται από τον αναλυτή και επικυρώνονται από τα η ΔΙΟΙΚΗΣΗ του ι εξέταση οργανισμού.
ΒΑΣΗ ΓΝΩΣΗΣ	Περιλαμβάνει δεδομένα σχετικά με τα αγαθά, επιπτώσεις, απειλές, αδυναμίες, σενάρια προσβολής, αντίμετρα, πολιτικές ασφαλείας και στρατηγικά σχέδια εφαρμογής.
ΥΑΔΕΠΣ	Υποστήριξη της Ανάλυσης και Διαχείρισης της Επικινδυνότητας Πληροφοριακών Συστημάτων.

6.2 Έγγραφο Παραστατικό Απαιτήσεων Λογισμικού(ΕΠΑΛ)

Όπως προαναφέρθηκε από το ΕΠΑΛ θα περιγραφούν τα τμήματα που είναι απαραίτητα για την εκπόνηση της εργασίας αυτής. Έτσι οι εισαγωγικές ενότητες αυτού θα παραβλεφθούν και θα περιγραφούν οι ειδικές απαιτήσεις.

6.2.1 Λειτουργικές Απαιτήσεις

Η ενότητα αυτή περιλαμβάνει τη διάσπαση του λογισμικού σε επιμέρους λειτουργίες με σκοπό τη βελτίωση της αναγνωσιμότητας του ΕΠΑΛ. Όπως γίνεται

αντιληπτό στις παρακάτω σελίδες, οι λειτουργίες μπορούν να αντιστοιχηθούν με τις φάσεις της μεθοδολογίας που το εργαλείο ακολουθεί.

6.2.1.1 1η Λειτουργία

ΟΝΟΜΑ	◦ ΥΠΟΛΟΓΙΣΜΟΣ ΑΞΙΑΣ ΑΓΑΘΩΝ ◦ Η λειτουργία αυτή αποτελείται από επιμέρους λειτουργίες την ΑΝΑΖΗΤΗΣΗ ΑΓΑΘΩΝ και τον ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΩΝ ΤΙΜΩΝ ΤΩΝ ΑΓΑΘΩΝ
ΕΙΣΑΓΩΓΗ	◦ Η λειτουργία αυτή έχει ως σκοπό να υπολογιστεί η αξία των αγαθών του υπό εξέταση οργανισμού, αφου πρώτα αυτά αναζητηθούν. Η υπολογισμένη αξία των αγαθών βοηθά στην εκπλήρωση των επόμενων λειτουργιών.
ΕΙΣΟΔΟΙ	◦ ΟΡΓΑΝΟΓΡΑΜΜΑ ◦ ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ ◦ ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ ◦ ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ
ΕΠΕΞΕΡΓΑΣΙΑ	◦ Πάρε ΟΡΓΑΝΟΓΡΑΜΜΑ από τη ΔΙΟΙΚΗΣΗ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ. ◦ Σύγκρινε τις πληροφορίες αυτές για ΑΝΑΖΗΤΗΣΗ ΑΓΑΘΩΝ και παρήγαγε ΠΙΝΑΚΑ ΑΓΑΘΩΝ για ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΙΜΩΝ ΑΓΑΘΩΝ. ◦ Στα αγαθά θα περιλαμβάνονται και τα επιμέρους – υποστηρικ αυτών. ◦ Πάρε ΠΙΝΑΚΑ ΑΓΑΘΩΝ από ΑΝΑΖΗΤΗΣΗ ΑΓΑΘΩΝ, ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ και ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ από ΣΥΝΕΝΤ/ΟΜΕΝΟΥΣ. ◦ Σύγκρινε τις πληροφορίες για ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΙΜΩΝ ΑΓΑΘ και παρήγαγε ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ για ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ. ◦ Οι επιπτώσεις θα υπολογιστούν και για τα επιμέρου υποστηρικτικά αγαθά των κυρίων αγαθών.
ΕΞΟΔΟΙ	◦ ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ

6.2.1.2 2η Λειτουργία

ΟΝΟΜΑ	◦ ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ Η λειτουργία αυτή αποτελείται από τις επιμέρους λειτουργίες ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ, ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ και ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ.
ΕΙΣΑΓΩΓΗ	◦ Η λειτουργία αυτή έχει ως σκοπό να αποτιμηθεί ο βαθμός επικινδυνότητας του υπό εξέταση οργανισμού για κάθε αγαθό αυτού και για το σύνολο του. Ο βαθμός επικινδυνότητας βοηθά στη ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ
ΕΙΣΟΔΟΙ	◦ ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ ◦ ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΠΕΙΛΕΣ

	• ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ • ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ • ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ • ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ
ΕΠΕΞΕΡΓΑΣΙΑ	• Πάρε ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ από ΥΠΟΛΟΓΙΣΜΟ ΑΞΙΑΣ ΑΓΑΘΩΝ, ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΠΕΙΛΕΣ από ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες αυτές για ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ και παρήγαγε ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ –ΑΓΑΘΩΝ για ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ και ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ. • Πάρε ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ –ΑΓΑΘΩΝ από ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ, ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ από ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες για ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ και παρήγαγε ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ για ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ. • Πάρε ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ –ΑΓΑΘΩΝ από ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ, ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ από ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες αυτές για ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ και παρήγαγε ΤΑΞΙΝΟΜΗΜΕΝΟ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ για ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ.
ΕΞΟΔΟΙ	• ΤΑΞΙΝΟΜΗΜΕΝΟΣ ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

6.2.1.3 3η Λειτουργία

ΟΝΟΜΑ	• ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ Η λειτουργία αυτή αποτελείται από τις επιμέρους λειτουργίες ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ, ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ και ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ.
ΕΙΣΑΓΩΓΗ	• Η λειτουργία αυτή έχει ως σκοπό να σχεδιασθεί το σχέδιο ασφαλείας του υπό εξέταση οργανισμού. Στο σχέδιο ασφαλείας θα περιλαμβάνεται και ο τρόπος υλοποίησης και η δυνατότητα ιχνηλάτησης μέσα σε αυτό.
ΕΙΣΟΔΟΙ	• ΤΑΞΙΝΟΜΗΜΕΝΟΣ ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ • ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ • ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ • ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΝΤΙΜΕΤΡΩΝ • ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ
ΕΠΕΞΕΡΓΑΣΙΑ	• Πάρε ΤΑΞΙΝΟΜΗΜΕΝΟ ΠΙΝΑΚΑ ΤΙΜΩΝ

	ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ από ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες αυτές για ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ και παρήγαγε την ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ για ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ. • Πάρε ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ από ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΝΤΙΜΕΤΡΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες για ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ και παρήγαγε ΕΠΙΛΕΓΜΕΝΟ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ για ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ. • Πάρε ΕΠΙΛΕΓΜΕΝΟ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ από ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ, ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ από ΔΙΟΙΚΗΣΗ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ από ΒΑΣΗ ΓΝΩΣΗΣ. • Σύγκρινε τις πληροφορίες αυτές για ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ για επικύρωση από τη ΔΙΟΙΚΗΣΗ και εφαρμογή από ΥΠΕΥΘΥΝΟ ΑΣΦΑΛΕΙΑΣ.
ΕΞΟΔΟΣ	• ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

6.2.2 Απαιτήσεις Εξωτερικών Διεπαφών

Στην ενότητα αυτή περιγράφονται οι απαιτήσεις εξωτερικών διεπαφών, δηλαδή οι διεπαφές με το χρήστη, με το υλικό, με το λογισμικό και με τις επικοινωνίες.

6.2.2.1 Διεπαφές Χρήστη

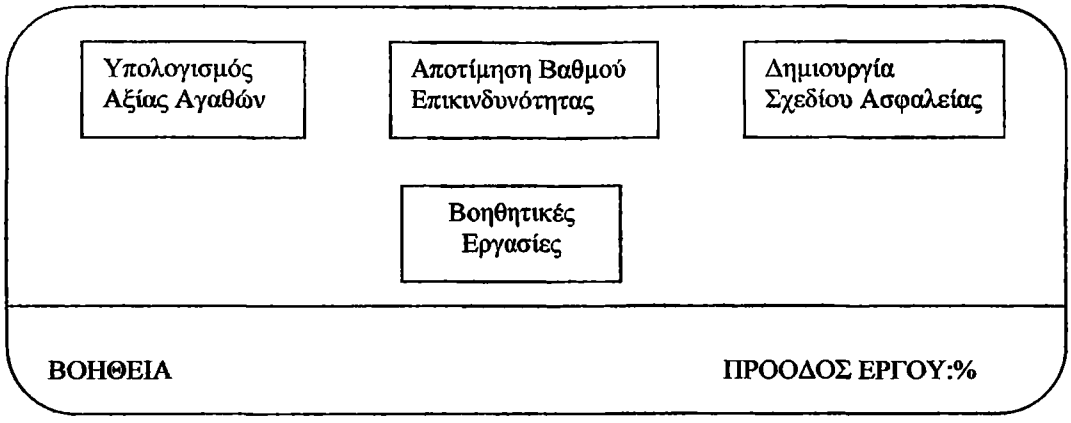
Εδώ προσδιορίζονται οι μορφές κάθε οθόνης και κάθε περιεχομένου έκθεσης ή ερωτηματολογίου ή πίνακα.

6.2.2.1.1 Μορφή Οθονών

Πρέπει να επισημανθεί το γεγονός ότι κατά την εισαγωγή στο εργαλείο εμφανίζεται παράθυρο σύνδεσης για την πληκτρολόγηση των στοιχείων του αναλυτή. Όπως έχει αναφερθεί οι ενέργειες του αναλυτή περιορίζονται στα δικαιώματα πρόσβασης που ο καθένα έχει. Έτσι κάποιες από τις παρακάτω λειτουργίες μπορεί να μην είναι δυνατές για όλους τους αναλυτές.

Η πρώτη οθόνη αποτελεί και το κεντρικό μενού επιλογών. Σε αυτό εντάσσονται οι προαναφερθείσες λειτουργίες: ΥΠΟΛΟΓΙΣΜΟΣ ΑΞΙΑΣ ΑΓΑΘΩΝ,

ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ και ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ.

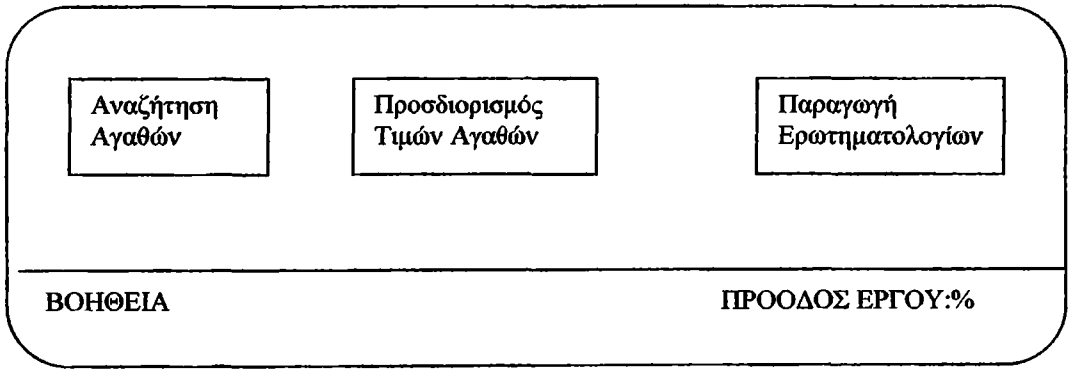


Οθόνη 6-1:Κεντρικό Μενού Επιλογών

Ο αναλυτής επιλέγει ποια λειτουργία θέλει να επιτελέσει και εμφανίζεται σχετική οθόνη. Η επιλογή μπορεί να γίνει είτε με το ποντίκι είτε μέσω του πλήκτρου Tab .Το ίδιο ισχύει και για οποιαδήποτε άλλη οθόνη.

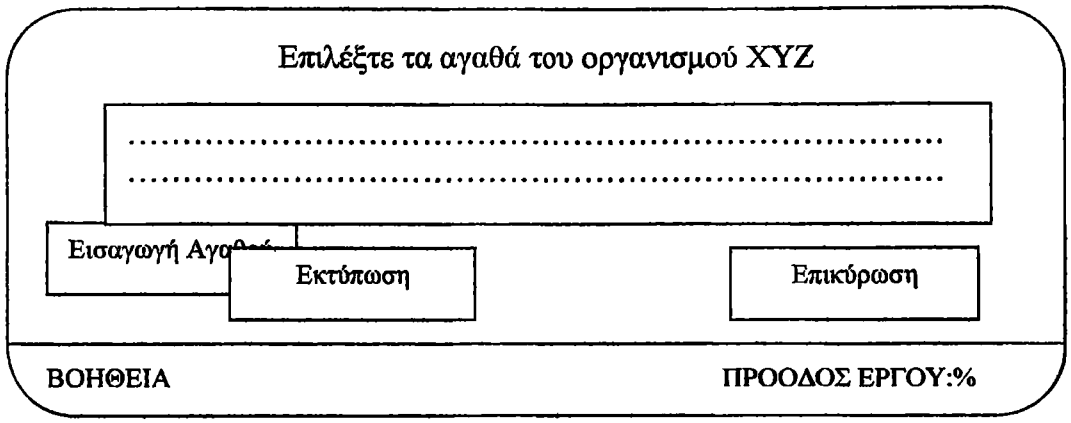
Στο δεξιό κάτω μέρος της οθόνης εμφανίζεται μήνυμα προσδιορισμού του σημείου στο οποίο βρίσκεται η ανάλυση (δυνατότητα ιχνηλάτησης) , Αντίστοιχα στο αριστερό μέρος υπάρχει η επιλογή για βοήθεια η οποία επιλέγεται με τους προαναφερόμενους τρόπους, όπου εμφανίζεται παράθυρο με πληροφορίες σχετικά με την προς εκτέλεση ενέργεια.

Επιλέγοντας τον ΥΠΟΛΟΓΙΣΜΟ ΑΞΙΑΣ ΑΓΑΘΩΝ εμφανίζεται το παρακάτω παράθυρο:

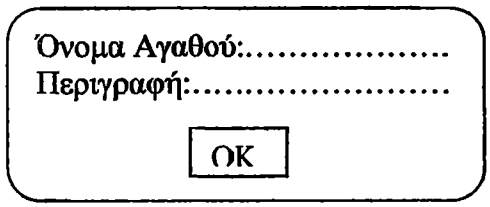


Οθόνη 6.2:Υπολογισμός Αξίας Αγαθών

Στην ΑΝΑΖΗΤΗΣΗ ΑΓΑΘΩΝ εμφανίζεται το κάτω παράθυρο:



Εδώ είναι ευθύνη του αναλυτή χρησιμοποιώντας το οργανόγραμμα να επιλέξει από τον πίνακα πιθανών αγαθών που εμφανίζεται στην οθόνη ποια είναι τα αγαθά του οργανισμού. Σε αντίθετη περίπτωση εισάγει καινούριο αγαθό. Η εισαγωγή του πραγματοποιείται μέσω της σχετικής ενέργειας όπου εμφανίζεται το παρακάτω παράθυρο:



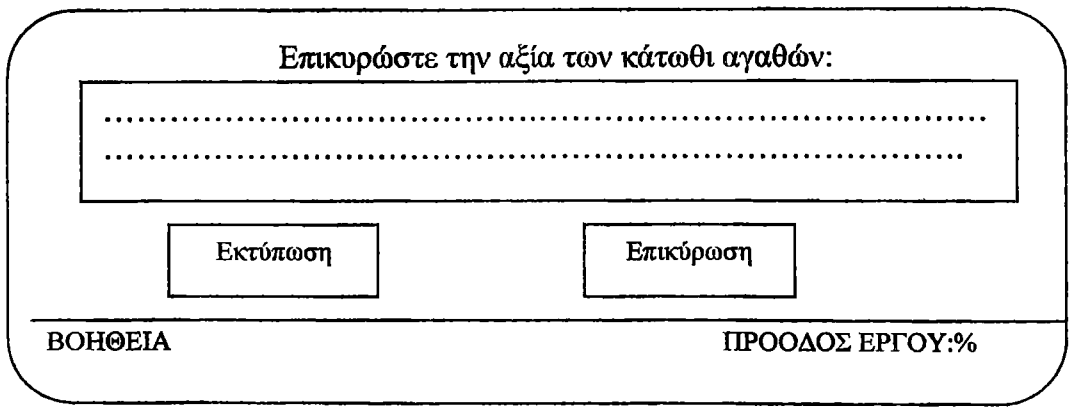
Οθόνη 6-4:Εισαγωγή Αγαθού

Ο αναλυτής πληκτρολογεί τα σχετικά στοιχεία και επιλέγει ΟΚ για τερματισμό της ενέργειας αυτής. Η ενέργεια αυτή επαναλαμβάνεται για κάθε νέο αγαθό προς εισαγωγή.

Όταν τελειώσει η εύρεση τότε μέσω της επιλογής ΕΚΤΥΠΩΣΗ γίνεται εκτύπωση του πίνακα αγαθών έτσι ώστε να επικυρωθεί από τη διοίκηση. Όταν επικυρωθεί τότε επιλέγεται η ΕΠΙΚΥΡΩΣΗ ώστε να ενημερωθεί η βάση γνώσης με τον πίνακα αγαθών για τον συγκεκριμένο οργανισμό.

Στον ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΙΜΩΝ ΑΓΑΘΩΝ εμφανίζεται το παρακάτω παράθυρο:

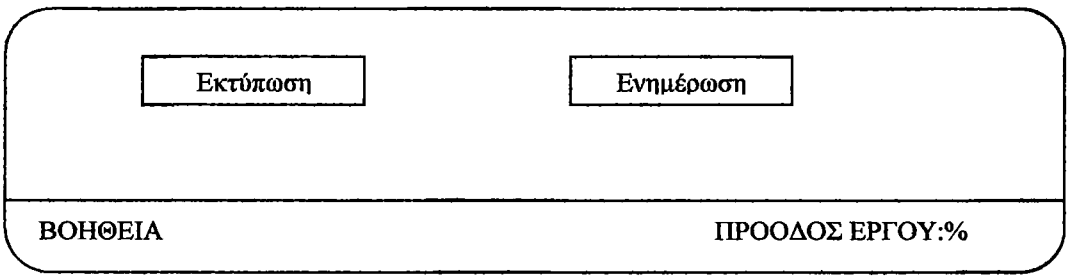
Οθόνη 6-5:Προσδιορισμός τιμών αγαθών



Στον εσωτερικό πίνακα εμφανίζεται η τιμή κάθε αγαθού για κάθε μια δυνατότητα αυτού σε περίπτωση απώλειας της. Αν δεν έχουν πραγματοποιηθεί οι συνεντεύξεις για τις επιπτώσεις ώστε να ενημερωθεί αυτόματα ο πίνακας αυτός τότε εμφανίζεται σχετικό μήνυμα και ο αναλυτής πρέπει να επιλέξει την ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ.

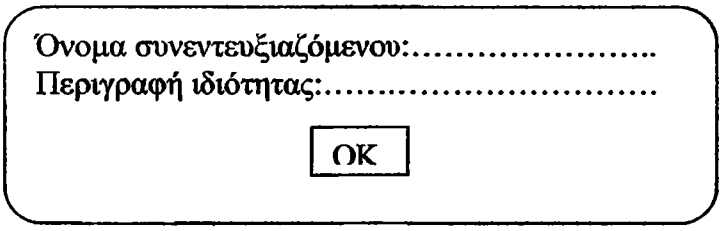
Ο αναλυτής εκτυπώνει τον πίνακα αξίας αγαθών και αφού επικυρωθεί από τη Διοίκηση τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-6: Παραγωγή Ερωτηματολογίων

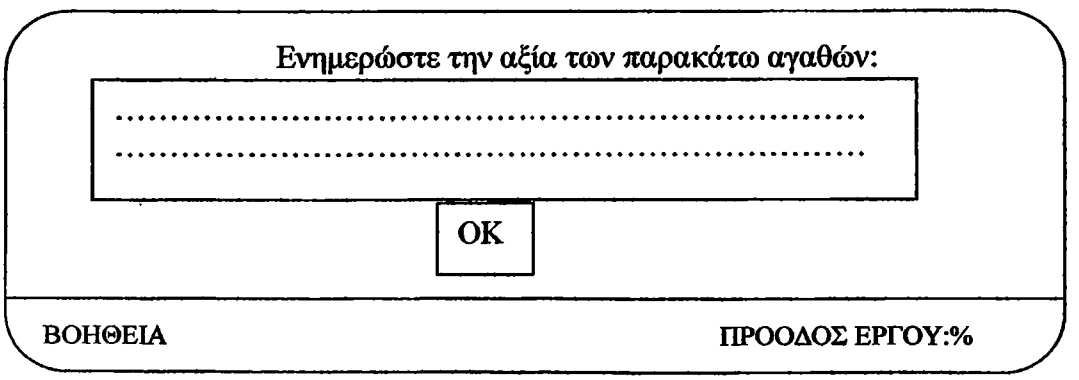
Με την επιλογή ΕΚΤΥΠΩΣΗ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-7: Εκτύπωση

Ο αναλυτής εισάγει τα σχετικά στοιχεία και μέσω του OK ενημερώνεται η βάση γνώσης για παραγωγή των ερωτηματολογίων σχετικά με τις επιπτώσεις λαμβάνοντας υπόψη την ιδιότητα του συνεντευξιαζόμενου ώστε η ορολογία να είναι ανάλογη. Η διαδικασία αυτή επαναλαμβάνεται για κάθε διαφορετικό συνεντευξιαζόμενο.

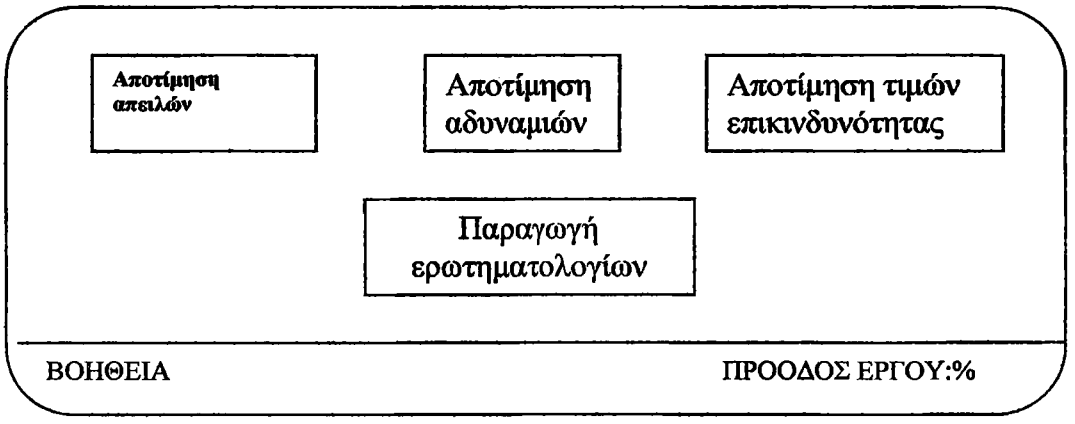
Με την επιλογή ΕΝΗΜΕΡΩΣΗ εμφανίζεται το κάτωθι παράθυρο:



Οθόνη 6-8:Ενημέρωση

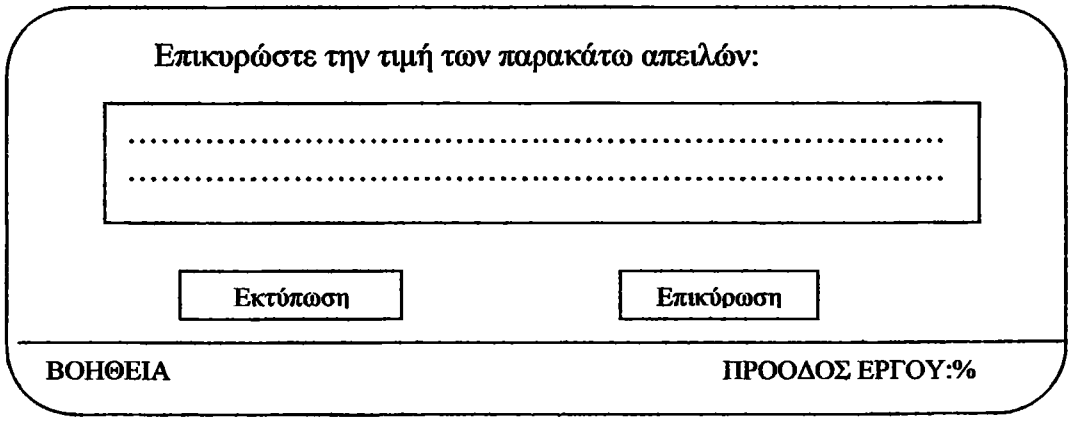
Ο αναλυτής εισάγει τις σχετικές τιμές και μέσω του ΟΚ ενημερώνεται η βάση γνώσης.

Επιλέγοντας την ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-9:Αποτίμηση βαθμού επικινδυνότητας

Στην ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ εμφανίζεται το παρακάτω παράθυρο:

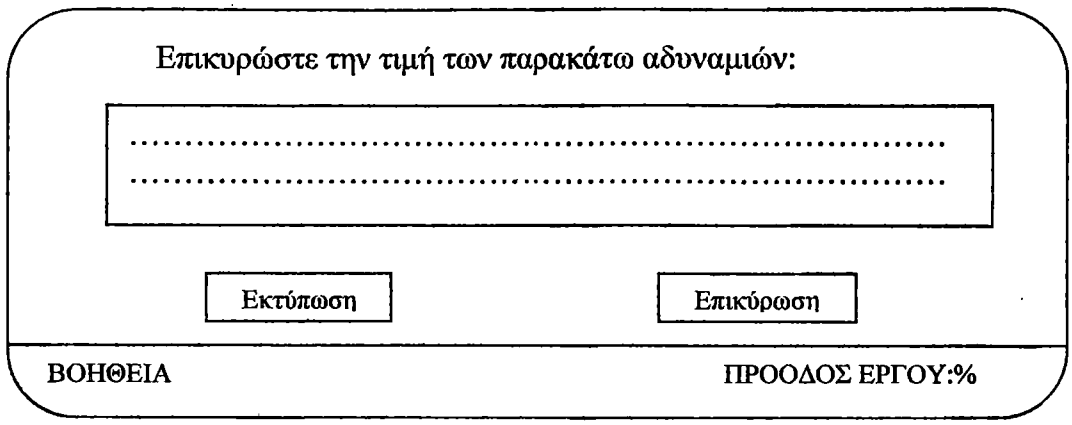


Οθόνη 6-10:Αποτίμηση απειλών

Στον εσωτερικό πίνακα εμφανίζεται η τιμή κάθε απειλής βάσει του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ και των ΣΥΝΕΝΤΕΥΞΕΩΝ ΓΙΑ ΑΠΕΙΛΕΣ. Αν δεν έχουν πραγματοποιηθεί οι συνεντεύξεις για τις απειλές ώστε να ενημερωθεί αυτόματα ο πίνακας αυτός τότε εμφανίζεται σχετικό μήνυμα και ο αναλυτής πρέπει να επιλέξει την ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ.

Ο αναλυτής εκτυπώνει τον πίνακα απειλών – αγαθών και αφου επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ εμφανίζεται το παρακάτω παράθυρο:

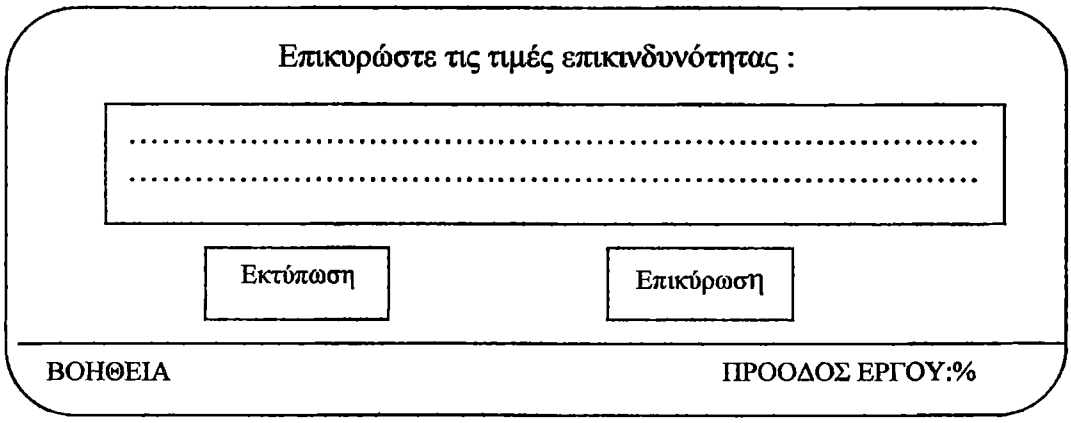


Οθόνη 6-11:Αποτίμηση αδυναμιών

Στον εσωτερικό πίνακα εμφανίζεται η τιμή κάθε αδυναμίας λαμβάνοντας υπόψη τον πίνακα απειλών –αγαθών και τις συνεντεύξεις για αδυναμίες. Αν δεν έχουν πραγματοποιηθεί οι συνεντεύξεις για τις αδυναμίες ώστε να ενημερωθεί αυτόματα ο πίνακας αυτός τότε εμφανίζεται σχετικό μήνυμα και ο αναλυτής πρέπει να επιλέξει την ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ.

Ο αναλυτής εκτυπώνει τον πίνακα αδυναμιών και αφου επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

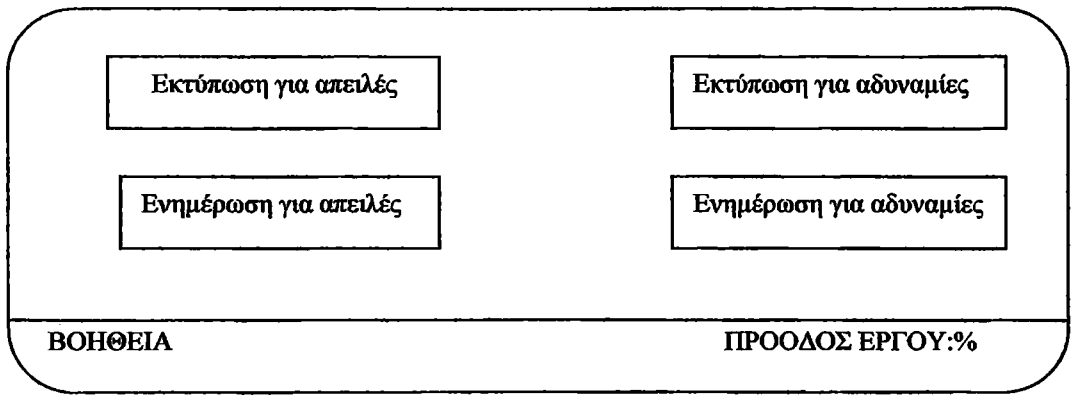
Με την επιλογή ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-12:Αποτίμηση τιμών επικινδυνότητας

Στον εσωτερικό πίνακα εμφανίζεται η τιμή επικινδυνότητας για κάθε αγαθό του οργανισμού και στο σύνολο του κατά φθίνουσα σειρά, λαμβάνοντας υπόψη τον ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ –ΑΓΑΘΩΝ, τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ και τον ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ. Ο αναλυτής εκτυπώνει τον ταξινομημένο πίνακα αδυναμιών τιμών επικινδυνότητας και αφού επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

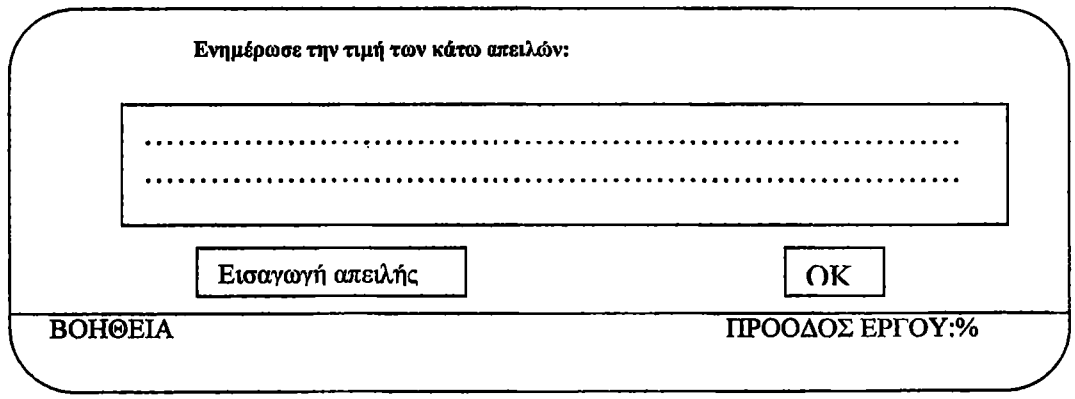
Με την επιλογή ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-13:Παραγωγή ερωτηματολογίων

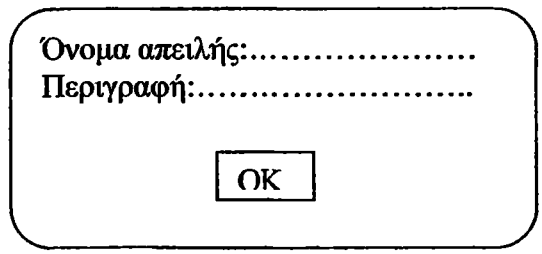
Τα δύο αριστερά πλήκτρα σχετίζονται με τις συνεντεύξεις για τις απειλές και τα δύο δεξιά για τις αδυναμίες. Με την επιλογή ΕΚΤΥΠΩΣΗ ΓΙΑ... θα εκτυπωθούν τα κατάλληλα ερωτηματολόγια χωρίς την ανάγκη εισαγωγής στοιχείων σχετικών με τους συνεντευξιαζόμενους. Ήδη τα σχετικά στοιχεία έχουν εισαχθεί στο προηγούμενο βήμα, αυτό του υπολογισμού της αξίας των αγαθών.

Με την επιλογή ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΑΠΕΙΛΕΣ εμφανίζεται το παρακάτω παράθυρο στο οποίο ο αναλυτής εισάγει τα σχετικά στοιχεία για τις απειλές μέσω συνεντεύξεων που πραγματοποιήθηκαν. Αν διαπιστωθούν νέες απειλές τότε επιλέγει την ΕΙΣΑΓΩΓΗ ΑΠΕΙΛΗΣ.



Οθόνη 6-14:Ενημέρωση για απειλές

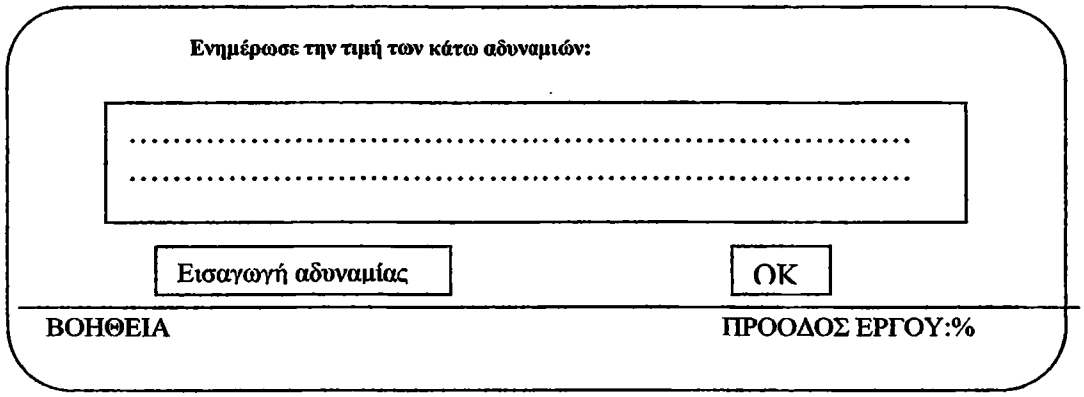
Μέσω της επιλογής αυτής εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-15:Εισαγωγή απειλής

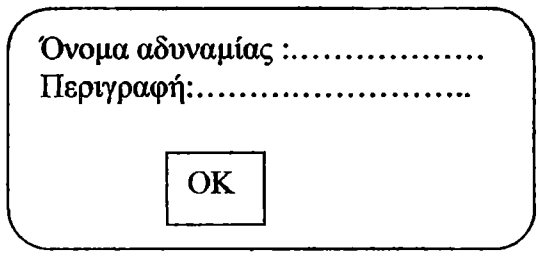
Ο αναλυτής πληκτρολογεί τα στοιχεία της απειλής και μέσω του ΟΚ ενημερώνεται η βάση γνώσης. Η ενέργεια αυτή επαναλαμβάνεται για κάθε νέα απειλή προς εισαγωγή.

Με την επιλογή ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΑΔΥΝΑΜΙΕΣ εμφανίζεται το παρακάτω παράθυρο στο οποίο ο αναλυτής εισάγει τα σχετικά στοιχεία για τις αδυναμίες μέσω των συνεντεύξεων που πραγματοποιήθηκαν. Αν διαπιστωθούν νέες αδυναμίες τότε επιλέγει την ΕΙΣΑΓΩΓΗ ΑΔΥΝΑΜΙΑΣ.



Οθόνη 6-16:Ενημέρωση για αδυναμίες

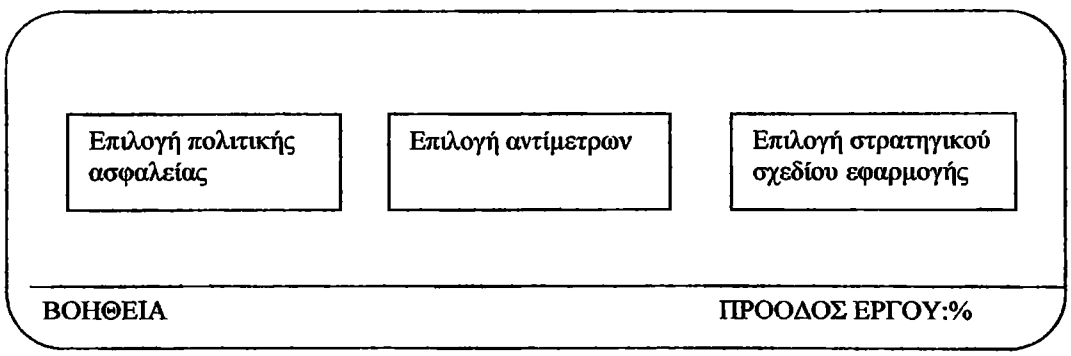
Μέσω της επιλογής αυτής εμφανίζεται το κάτω παράθυρο:



Οθόνη 6-17:Εισαγωγή αδυναμίας

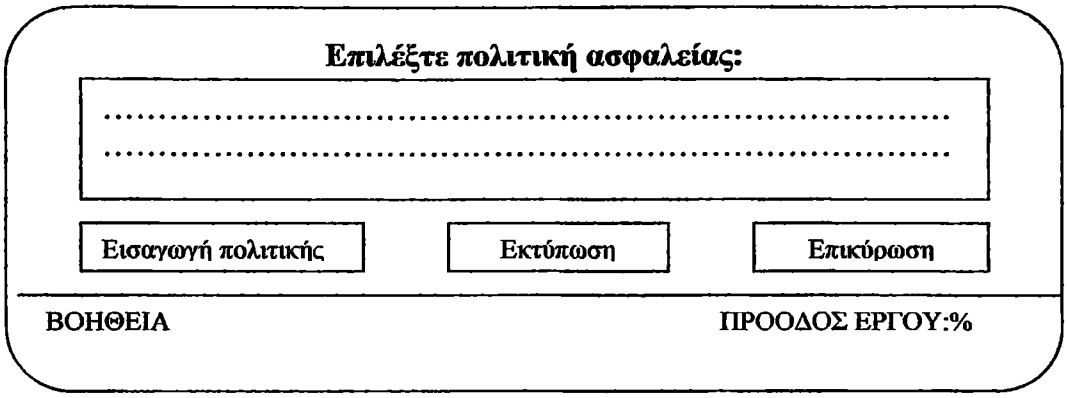
Ο αναλυτής πληκτρολογεί τα στοιχεία της αδυναμίας και μέσω του ΟΚ ενημερώνεται η βάση γνώσης. Η ενέργεια αυτή επαναλαμβάνεται για κάθε νέα αδυναμία προς εισαγωγή.

Επιλέγοντας τη ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ εμφανίζεται το παρακάτω παράθυρο:



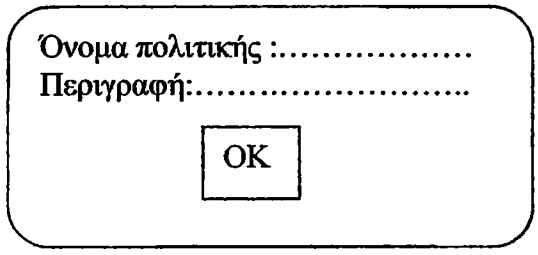
Οθόνη 6-18:Δημιουργία σχεδίου ασφαλείας

Στην επιλογή ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-19:Επιλογή πολιτικής ασφαλείας

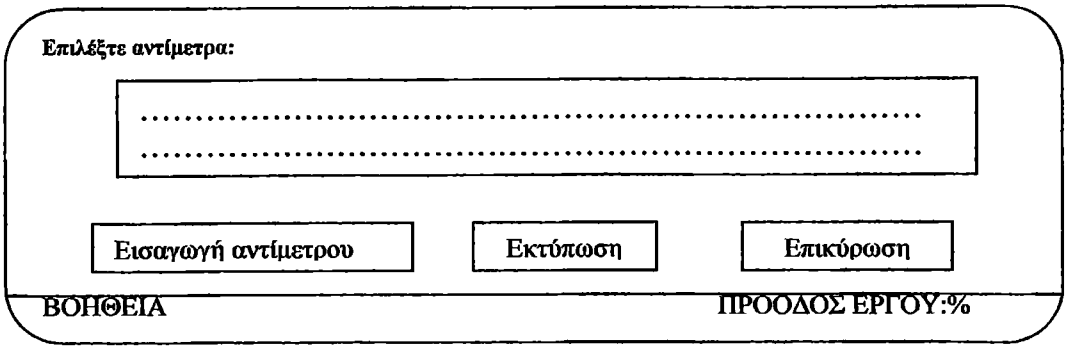
Στον πίνακα εμφανίζονται οι πολιτικές ασφαλείας που είναι σχετικές με τα στοιχεία που συλλέγονται από τον ταξινομημένο πίνακα τιμών επικινδυνότητας και από τον πίνακα πιθανών πολιτικών ασφαλείας. Αν ο αναλυτής κρίνει ότι πρέπει να δημιουργηθεί μια καινούρια πολιτική ασφαλείας ή να τροποποιηθεί κάποια υπάρχουσα επιλέγει το αντίστοιχο πλήκτρο με το οποίο εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-20:Εισαγωγή πολιτικής

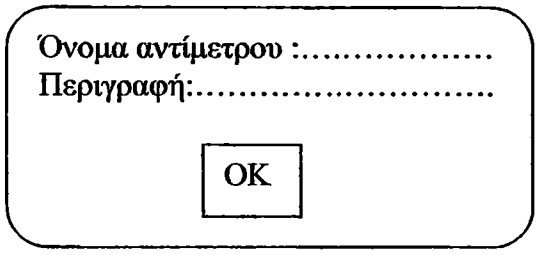
Ο αναλυτής πληκτρολογεί όλα τα σχετικά στοιχεία και με το ΟΚ ενημερώνεται κατάλληλα η βάση γνώσης. Ο αναλυτής εκτυπώνει την κατάλληλη πολιτική ασφαλείας και αφου επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην επιλογή ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-21:Επιλογή αντίμετρων

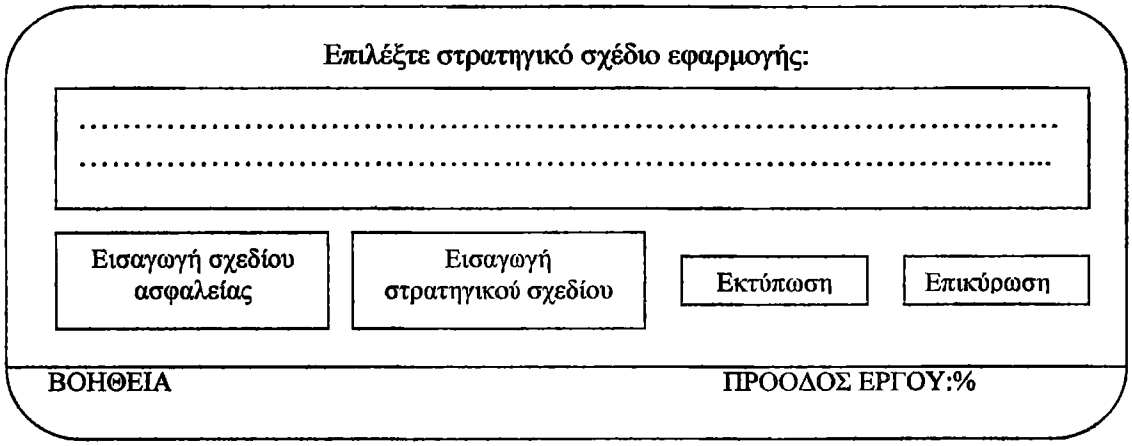
Στον πίνακα εμφανίζονται τα αντίμετρα που είναι σχετικά με τα στοιχεία που συλλέγονται από την επιλεγμένη πολιτική ασφαλείας και από τον πίνακα πιθανών αντίμετρων. Αν ο αναλυτής κρίνει ότι πρέπει να δημιουργηθεί ένα νέο αντίμετρο επιλέγει το πλήκτρο ΕΙΣΑΓΩΓΗ ΑΝΤΙΜΕΤΡΟΥ με το οποίο εμφανίζεται το παρακάτω παράθυρο:



Οθόνη 6-22:Εισαγωγή αντίμετρου

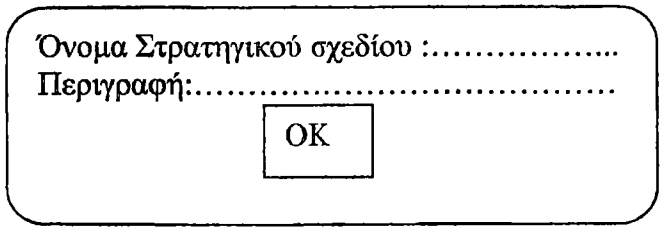
Ο αναλυτής πληκτρολογεί όλα τα σχετικά στοιχεία και με το ΟΚ ενημερώνεται κατάλληλα η βάση γνώσης. Ο αναλυτής στη συνέχεια εκτυπώνει τον επιλεγμένο πίνακα αντίμετρων και αφού επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην επιλογή ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ εμφανίζεται το παρακάτω παράθυρο:

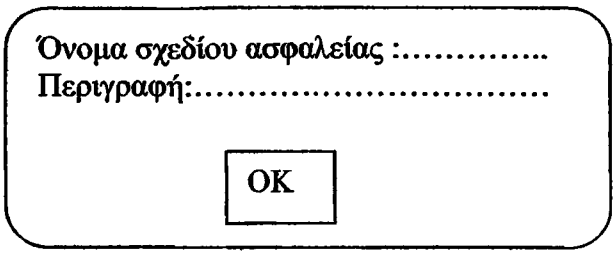


Οθόνη 6-23:Επιλογή στρατηγικού σχεδίου εφαρμογής

Ο πίνακα περιλαμβάνει τα στρατηγικά σχέδια εφαρμογής βάσει των στοιχείων του επιλεγμένου πίνακα αντίμετρων και του πίνακα στρατηγικού σχεδίου εφαρμογής. Αν ο αναλυτής θεωρήσει ότι πρέπει να υπάρχει ένα νέο στρατηγικό σχέδιο ή αν ο προς εξέταση οργανισμός έχει κάποιο σχέδιο ασφαλείας τότε η βάση γνώσης πρέπει να ενημερωθεί χρησιμοποιώντας τα αντίστοιχα πλήκτρα που εμφανίζουν τα παρακάτω παράθυρα:



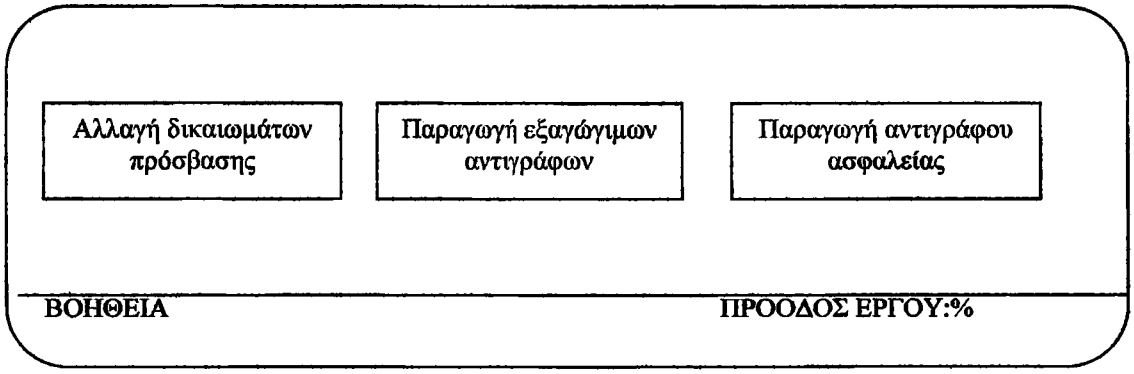
Οθόνη 6-24:Εισαγωγή στρατηγικού σχεδίου



Οθόνη 6-25:Εισαγωγή σχεδίου ασφαλείας

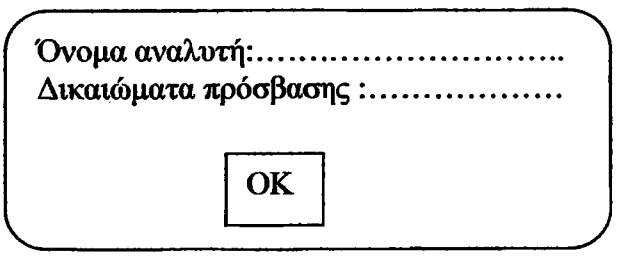
Ο αναλυτής πληκτρολογεί όλα τα σχετικά στοιχεία και με το ΟΚ ενημερώνεται κατάλληλα η βάση γνώσης. Ο αναλυτής στη συνέχεια εκτυπώνει το επιλεγμένο σχέδιο ασφαλείας και αφου επικυρωθεί από τη ΔΙΟΙΚΗΣΗ τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Επιλέγοντας τις βοηθητικές λειτουργίες εμφανίζεται το παρακάτω παράθυρο:



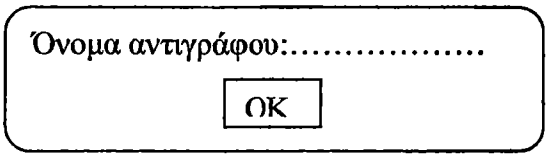
Οθόνη 6-26:Βοηθητικές λειτουργίες

Στην επιλογή ΑΛΛΑΓΗ ΔΙΚΑΙΩΜΑΤΩΝ ΠΡΟΣΒΑΣΗΣ εμφανίζεται το παρακάτω παράθυρο στο οποίο ο αναλυτής με δικαιώματα υπέρ χρήστη (super – user) πληκτρολογεί τα στοιχεία του αναλυτή και αλλάζει τα δικαιώματα πρόσβασης αυτού στα επιθυμητά. Με τι ΟΚ επιβεβαιώνονται οι αλλαγές. Η ενέργεια αυτή επαναλαμβάνεται για κάθε νέα αδυναμία εισαγωγής.



Οθόνη 6-27:Αλλαγή δικαιωμάτων πρόσβασης

Στην επιλογή ΠΑΡΑΓΩΓΗ ΕΞΑΓΩΓΙΜΩΝ ΑΝΤΙΓΡΑΦΩΝ εμφανίζεται το παρακάτω παράθυρο στο οποίο ο αναλυτής πληκτρολογεί το όνομα του αντιγράφου προς εξαγωγή και πατώντας το OK το αντίγραφο εισάγεται στη δισκέτα ή στοCD ROM. Το αντίγραφο μπορεί να είναι είτε κάποια έκθεση προς τη διοίκηση είτε κάποιος πίνακας.



Οθόνη 6-28:Παραγωγή εξαγώγιμων αντιγράφων

Στην επιλογή παραγωγή αντιγράφου ασφαλείας εισάγεται στο CD ROM η βάση γνώσης του εργαλείου καθώς και το εκτελέσιμο αρχείο.

6.2.2.1.2 Μορφή Εκθέσεων

Οι εκθέσεις μπορεί να είναι είτε ερωτηματολόγια για επιπτώσεις και αδυναμίες του οργανισμού, είτε πίνακας αγαθών, αξίας αγαθών, απειλών – αγαθών και αδυναμιών. Επίσης μπορεί να είναι ο ταξινομημένος πίνακας των τιμών επικινδυνότητας, η έκθεση με την επιλεγμένη πολιτική ασφαλείας ή με το επιλεγμένο πίνακα αντίμετρων ή τέλος το επιλεγμένο σχέδιο ασφαλείας.

Στα ερωτηματολόγια θα αναγράφονται τα στοιχεία του συνεντευξιαζόμενου και η ημερομηνία πάνω αριστερά. Θα υπάρχει στην πρώτη σελίδα ο τίτλος τους καθώς και στην κεφαλίδα, ενώ στο υποσέλιδο θα αναγράφεται ο αριθμός κάθε σελίδας. Στην πρώτη σελίδα κάτω από τον τίτλο θα υπάρχει ένα σύντομο κείμενο γύρω από τον σκοπό του ερωτηματολογίου.

Στις εκθέσεις πρέπει να υπάρχει μια περίληψη (executive summary) έτσι ώστε να ξέρει η διοίκηση και να τονίζεται σε ποιο στάδιο είμαστε. Τα υποσέλιδα και οι κεφαλίδες έχουν την ίδια μορφή όπως έχει προαναφερθεί αντίστοιχα καθώς και τα στοιχεία του απευθυνόμενου πάνω αριστερά.

6.2.2.2Διεπαφές Υλικού

Εδώ προσδιορίζονται τα λογικά χαρακτηριστικά κάθε διεπαφής μεταξύ του προϊόντος Λογισμικού και των στοιχείων υλικού του συστήματος. Οι συσκευές είναι ένας υπολογιστής με επεξεργαστή Pentium IV 755MHz,128 MB SDRAM, HDD 18GB,Κάρτα οθόνης AGP, Ποντίκι PS/2, Πληκτρολόγιο PS/2, Οθόνη 17 inch, φίλτρο οθόνης και Εκτυπωτής υψηλής ποιότητας (Laser).

6.2.2.3 Διεπαφές Λογισμικού

Εδώ προσδιορίζεται η χρήση άλλων προϊόντων λογισμικού. Ήδη σε προηγούμενα κεφάλαια έχει αναφερθεί η ανάγκη χρήσης του εργαλείου σε διαφορετικά Λειτουργικά Συστήματα. Επίσης στο εργαλείο ενσωματώνεται και το πρόγραμμα διαχείρισης του σχεδίου ασφαλείας που παραδίδεται στον προς εξέταση οργανισμό για χρονοπρογραμματισμό των ενεργειών του. Τέλος έχουμε το Σύστημα Διαχείρισης Βάσεως Δεδομένων για διαχείριση της βάσης γνώσης που είναι ενσωματωμένη μέσα στο εργαλείο.

6.2.2.4 Διεπαφές Επικοινωνιών

Το εργαλείο δεν έχει διεπαφές με επικοινωνίες.

6.2.3 Απαιτήσεις Επίδοσης

Εδώ προσδιορίζονται οι στατικές και οι δυναμικές αριθμητικές απαιτήσεις από το εργαλείο ή από την επικοινωνία του με τον άνθρωπο. Οι απαιτήσεις χωρίζονται σε στατικές και δυναμικές.

6.2.3.1 Στατικές Απαιτήσεις

1) Μέγιστο πλήθος αρχείων 1.000.000
2) Μέγιστο πλήθος εγγράφων 100.000.000

Οι απαιτήσεις αυτές προέρχονται από τη βάση γνώσης που είναι από τη φύση της ογκώδης.

6.2.3.2 Δυναμικές Απαιτήσεις

1) Οι τετριμμένες ενέργειες δηλαδή αυτές που γίνονται συχνά (πάνω από π.χ. 50 φορές) θα πρέπει να εκτελούνται μέσα σε 1 ½ δευτερόλεπτο.
2) Οι ενέργειες με μικρή συχνότητα θα πρέπει να εκτελούνται μέσα σε 15 με 20 λεπτά.

6.2.3 Περιορισμοί Σχεδίασης

Οι περιορισμοί σχεδίασης μπορούν να επιβάλλονται από άλλα πρότυπα , περιορισμούς του υλικού καθώς και από νόμους και οδηγίες. Οι περιορισμοί για το συγκεκριμένο εργαλείο έχουν αναφερθεί σε προηγούμενα κεφάλαια της εργασίας αυτής.

ΚΕΦΑΛΑΙΟ 7

ΚΡΙΤΗΡΙΑ ΕΠΙΚΥΡΩΣΗΣ ΚΑΙ ΑΠΟΔΟΧΗΣ ΠΡΟΪΟΝΤΟΣ

7.1 Έλεγχος Κώδικα και Ενοτήτων

Η φάση ελέγχου κώδικα και ενοτήτων αφορά τον έλεγχο του κώδικα και των ενοτήτων κώδικα του εργαλείου. Ο έλεγχος εστιάζεται στα μικρότερα δομικά τμήματα του προγράμματος, τα μεμονωμένα υποπρογράμματα, υπορουτίνες ή διαδικασίες. Ανάμεσα στους ελέγχους που πραγματοποιούνται περιλαμβάνονται : **ο έλεγχος παλινδρόμησης (regression), ο λειτουργικός (functional) έλεγχος** και ο **έλεγχος απόδοσης (performance).** Οι έλεγχοι σχεδιάζονται με τρόπο τέτοιο ώστε να εντοπίζουν σφάλματα το συντομότερο δυνατό, προσπαθώντας να εξασφαλίσουν ότι αυτά δεν θα περάσουν στα επόμενα στάδια του κύκλου ζωής του προϊόντος.

Οι ενέργειες που θα πρέπει να γίνουν σχετικά με τον έλεγχο κώδικα και ενοτήτων έχουν ως εξής:

- Οι προγραμματιστές θα πρέπει να βεβαιωθούν ότι οι περιπτώσεις ελέγχου με έγκυρα και μη έγκυρα δεδομένα καταγράφονται.
- Θα πρέπει οπωσδήποτε να γίνει έλεγχος από κάτω προς τα πάνω, των χαμηλού επιπέδου τμημάτων.
- Μετά την εύρεση και διόρθωση κάθε σφάλματος, θα πρέπει να γίνεται επαναεφαρμογή των προηγούμενων δοκιμών ελέγχου.

1) Θα πρέπει να γίνει αναθεώρηση του πλάνου ελέγχου λαμβάνοντας υπόψη πιθανές αβλεψίες όσον αφορά τα χρονικά περιθώρια.

2) Κωδικοποίηση:

i. Θα πρέπει να γράφονται σχόλια σύμφωνα με κάποιο από τα σχετικά πρότυπα.
ii. Ο κώδικας θα πρέπει να γράφεται σύμφωνα με κάποιο πρότυπο

3) Διόρθωση Λαθών:

i. Οποιεσδήποτε σχεδιαστικές αλλαγές θα πρέπει να συμμορφώνονται ως προς τις προδιαγραφές των απαιτήσεων.
ii. Η συγγραφή του κώδικα και των σχολίων θα πρέπει να γίνεται σύμφωνα με τα πρότυπα
iii. Θα πρέπει να γίνεται ενημέρωση της τεκμηρίωσης σύμφωνα με τα «Πρότυπα Ενημέρωσης Εγγράφων Τεκμηρίωσης».

4) Έλεγχος Παλινδρόμησης:

Όλες οι προηγούμενες δοκιμές ελέγχου θα πρέπει να επαναλαμβάνονται μετά τον εντοπισμό και την διόρθωση ενός σφάλματος.

5) Λειτουργικές Δίαυλοι:

i. Δεδομένα εισόδου της ονομαστικής αξίας, τα αναμενόμενα αποτελέσματα των οποίων είναι γνωστά.
ii. Δεδομένα εισόδου με οριακές τιμές (ελάχιστη, μέγιστη και όλες οι τιμές στα όρια λειτουργίας και ακριβώς έξω από αυτά).
iii. Όρια του πεδίου τιμών των αποτελεσμάτων.
iv. Οποιεσδήποτε ειδικές τιμές:
   a) Δεδομένα εισόδου με λογική συσχέτιση
   b) Τα πρώτα και τα τελευταία στοιχεία συνόλων.

6) Δομική Ανάλυση: Η ανάλυση αυτή αφορά τη δομή του προγράμματος

i. Θα πρέπει να προσδιοριστούν τα μονοπάτια εκτέλεσης που θα ελεγχθούν.
ii. Θα παραχθούν τα δεδομένα για τον έλεγχο των μονοπατιών.
iii. Θα επιλεχθούν τα κριτήρια κάλυψης των ελέγχων:
   a. Κάλυψη δηλώσεων και εντολών
   b. Κάλυψη κλάδων
   c. Κάλυψη λογικών μονοπατιών

7) Έλεγχος Απόδοσης:

Αποδεκτές τιμές ρυθμοαπόδοσης του προγράμματος, του χρόνου απόκρισης και χρησιμοποίησης των πόρων σύμφωνα με την ανάλυση των απαιτήσεων.

8) Η συμμόρφωση των ενοτήτων ενός αλγόριθμου θα πρέπει να καταγράφεται και να ενημερώνεται.

9) Θα πρέπει να ορισμούμε κάποιος έλεγχος των απόψεων (versions control) μετά από αλλαγές στον κώδικα.

10) Περιηγήσεις Κώδικα (Walkthroughs). Θα πρέπει να εξασφαλίζεται ότι:

i. Η δουλεία αναθεωρείται βάσει προγραμματισμού
ii. Μια θετική ατμόσφαιρα για την πραγματοποίηση των περιηγήσεων
iii. Η έμφαση θα δίνεται στον εντοπισμό των λαθών
iv. Συζητούνται σημαντικά θέματα όπως η αποδοτικότητα του κώδικα
v. Ορίζεται ένα χρονικό όριο προκείμενου να υπάρχει εξασφάλιση ότι γίνεται επικέντρωση στα σημαντικά θέματα έτσι ώστε να περιοριστεί το υλικό που θα εξεταστεί και να ενισχυθούν τα κύρια ζητήματα.

11) Αν ο έλεγχος ενοτήτων πραγματοποιηθεί από τα άτομα που υλοποιούν τα τμήματα του κώδικα θα πρέπει να [illegible]. Ορισμένα τμήματα θα πρέπει να υποστούν επανέλεγχο από ανεξάρτητους ελεγκτές, χρησιμοποιώντας ένα διαφορετικό σύνολο από δοκιμές ελέγχου.

12) Ανάλυση της Ευπαθειότητας (Vulnerability): Θα πρέπει να αναπτυχθούν περιπτώσεις ελέγχου με βάση τον κώδικα και όχι τις απαιτήσεις. Στη συνέχεια θα πρέπει να συγκριθούν με τα έγγραφα τεκμηρίωσης της σχεδίασης ώστε να υπάρχει η βεβαιότητα ότι έχουν καλυφθεί όλες οι απαιτήσεις.

)Θα πρέπει να εξασφαλιστεί ότι σε περίπτωση που υπάρχει η δυνατότητα να χρησιμοποιηθούν εργαλεία ελέγχου, αυτά θα πρέπει να ρυθμίζονται , να συντηρούνται και [illegible] καθώς και να ελέγχεται ότι έχουν την δυνατότητα να πραγματοποιήσουν την προτεινόμενη επαλήθευση.

Πρότυπα Σχετικά με τον Έλεγχο του Κώδικα Ενοτήτων

Κωδική Ονομασία	Τίτλος
ANSI/ IEEE 1008-1987	IEEE Standard for Software Unit Testing
ANSI/ IEEE 829-1983	IEEE Standard for Software Documentation

1.Κώδικας – Εσωτερική Τεκμηρίωση – Σχόλια

Ο κώδικας του εργαλείου θα πρέπει να περιλαμβάνει εσωτερική τεκμηρίωση (σχόλια), η οποία θα ακολουθεί τα ακόλουθα πρότυπα:

- Κάθε κλάση ή διαδικασία θα περιέχει ένα σχόλιο που θα περιγράφει τι κάνει και όχι το πώς το κάνει.
- Το σχόλιο θα γράφεται αμέσως μετά την δήλωση του ονόματος αλλά όχι μέσα στο σώμα του κώδικα(δηλαδή όχι μέσα στις αγκύλες { })
- Αν μια διαδικασία δηλώνεται σε ένα αρχείο κεφαλίδας (header file),το σχόλιο θα τίθεται μέσα στο αρχείο κεφαλίδας.
- Αν μια διαδικασία έχει περισσότερες από μια δηλώσεις το σχόλιο θα τίθεται μόνο στην πρώτη από αυτές.
- Σε μια εικονική διαδικασία το σχόλιο εμφανίζεται μόνο στη δήλωση της πιο γενικής κλάσης
- Ο σχολιασμός του ΠΩΣ λειτουργεί μια διαδικασία είναι προαιρετικός ενώ θα τοποθετείται μέσα στο σώμα της διαδικασίας.
- Σχολιασμός ρουτινών, modules, αρχείων και προγραμμάτων:
    1. Modules/ ρουτίνες: ονομασία, περιγραφή, σκοπός, αλγόριθμοι, συγγραφέας.
    2. Ονόματα αρχείων τα οποία καλούνται από το module/συνάρτηση.
    3. Διαφοροποίηση των δεδομένων εισόδου και εξόδου
    4. Προσθήκη μιας δήλωσης για copyright στο τέλος των εντολών.

2.Ονοματοδοσία Αρχείων. Μεταβλητών. Τύπων. Ετικετών:

i. Ένα όνομα σχηματίζεται με χρήση μιας ή περισσότερων λέξεων ή συντμήσεων. Το πρώτο γράμμα κάθε λέξης ή σύντμησης γράφεται κεφαλαίο ενώ τα υπόλοιπα γράμματα γράφονται με πεζά, εκτός από τα ονόματα τύπων στους οποίους το πρώτο γράμμα είναι πεζό (π.χ. Total Amount, Lines Read, Files Checked ενώ οι τύποι int Values,real Numbers κλπ).

ii. Για την ονομασία μιας ομάδας ή μια λίστας θα μπορούσε να χρησιμοποιηθεί ο πληθυντικός αριθμός μιας λέξης.

iii. Στα ονόματα επιλέγεται η χρήση συντμήσεων προκειμένου να μεγιστοποιηθεί το σημασιολογικό περιεχόμενο κάθε ονόματος αλλά και να διατηρηθεί σε λογικά πλαίσια το μήκος του. Αν υπάρχει μια σύντμηση ενός ονόματος δεν χρησιμοποιείται το πλήρες όνομα. Στη συνέχεια δίνονται κάποιες γνωστές συντμήσεις:

Ενδεικτικές Συντμήσεις Ονομάτων

String	str
Integer	int
Option	opt
Check	chk
Count	cnt
Argument	arg
Number	num
Long	ln

7.2 Έλεγχος

Αυτή η φάση ελέγχου αφορά το εργαλείο στο σύνολο του παρά στα επιμέρους μέρη ή ενότητες. Προτού το εργαλείο να είναι διαθέσιμο στην αγορά θα πρέπει να πραγματοποιηθούν μια σειρά από ελέγχους, όπως έλεγχος συνένωσης, παλινδρόμησης, σε συνθήκες πίεσης,alpha και beta. Επιπρόσθετα θα πρέπει να πραγματοποιηθεί έλεγχος ασφάλειας ,συμβατότητας, ευχρηστίας, ανάκαμψης και τεκμηρίωσης. Οι έλεγχοι που πραγματοποιούνται είναι αυτοί που απαιτούνται από το πλάνο ποιότητας. Το εργαλείο δεν μπορεί να διατεθεί στην αγορά αν δεν ολοκληρωθεί ο έλεγχος φτάνοντας σε ένα επίπεδο ποιότητας που ορίζεται από τις απαιτήσεις.

Οι ενέργειες που θα πρέπει να γίνουν σχετικά με τον έλεγχο έχουν ως εξής:

- Θα πρέπει να αναθεωρηθεί το πλάνο ελέγχου με βάση την τεκμηρίωση και τις περιπτώσεις ελέγχου οι οποίες έχουν συνταχθεί κατά τη φάση σχεδιασμού του εργαλείου.
- Οι περιπτώσεις ελέγχου συνένωσης θα πρέπει να αναπτυχθούν παράλληλα με την ανάπτυξη του πακέτου λογισμικού. Το γεγονός αυτό δίνει τη δυνατότητα οι έλεγχοι να γίνουν περισσότερο λεπτομερειακοί καθώς προχωρά η ανάπτυξη του εργαλείου.

Ακολουθεί μια εισήγηση σχετικά με τη σειρά εκτέλεσης των ελέγχων και κάποιες συνοδευτικές προτάσεις.

Πλήρης έλεγχος ομάδων ενοτήτων μετά την συνένωση τους σε υποσυστήματα. Ο έλεγχος επικεντρώνεται στον εντοπισμό λαθών και προβλημάτων των διεπαφών, μέσα από την αυστηρή χρήση αυτών. Θα

πρέπει να επιλέγουν περιπτώσεις ελέγχου οι οποίες χρησιμοποιούν τις διεπαφές με τον επιθυμητό τρόπο.

Ελέγχει τη συμμόρφωση του προϊόντος με τις προδιαγραφές του συστήματος όπως αυτές έχουν οριστεί κατά την φάση της ανάλυσης των απαιτήσεων. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στα λάθη ερμηνείας που έγιναν κατά την φάση του σχεδιασμού.

Όλοι οι προηγούμενοι έλεγχοι επαναλαμβάνονται μετά την ανακάλυψη και την διόρθωση ενός σφάλματος.

Ο έλεγχος αυτός συμβάλλει στην επικύρωση ότι τι εργαλείο λειτουργεί σε ακραίες περιπτώσεις πίεσης και επιβεβαιώνει ότι μπορεί να χειριστεί τον προβλεπόμενο φόρτο. Οι συγκεκριμένοι έλεγχοι που θα πραγματοποιηθούν θα μπορούσαν να προσομοιώνουν «ανυπόφορες» καταστάσεις, ωστόσο τα σφάλματα που πιθανά θα προκύψουν θεωρούνται εξαιρετικά σημαντικά καθώς είναι δυνατό τα ίδια σφάλματα να παρουσιαστούν και συνθήκες κανονικής λειτουργίας.

Θα πρέπει να εξεταστούν οι ακόλουθες σκέψεις:

1. Αν έχει κάθε διεπαφή χρήστη, αν μπορεί να προσαρμοστεί στο επίπεδο ευφυΐας και μόρφωσης καθώς και σε συνθήκες πίεσης του περιβάλλοντος του τελικού χρήστη.

2. Αν είναι όλα τα μηνύματα λάθους ξεκάθαρα στην κατανόηση τους.

3. Αν παρέχει το εργαλείο κάποιο είδος άμεσης επιβεβαίωσης σε όλα τα δεδομένα εισόδου και αν ενημερώνει τον χρήστη για το τι συμβαίνει ανά πάσα στιγμή.

4. Αν είναι το εργαλείο εύκολο στη χρήση του.

Ο έλεγχος αυτός περιλαμβάνει τη διαδικασία επινόησης και εφαρμογής ελέγχων οι οποίοι υπονομεύουν τους ελέγχους ασφαλείας του εργαλείου. Μια μέθοδος που θα μπορούσε να βοηθήσει σε αυτό είναι η μελέτη γνωστών προβλημάτων ασφαλείας σε παρόμοιες εφαρμογές και η προσπάθεια να αναδειχτεί η συμπεριφορά του εργαλείου σε αντίστοιχα προβλήματα.

Η διαδικασία αυτή ελέγχει τον τρόπο με τον οποίο το εργαλείο ανακάμπτει από προγραμματιστικά λάθη, αποτυχίες υλικού και λάθη δεδομένων. Στην περίπτωση αυτή θα μπορούσαν να εισαχθούν σκόπιμα προγραμματιστικά λάθη μέσα στον κώδικα προκειμένου να φανεί ο τρόπος που αντιδρά σε αυτά το εργαλείο.

Γίνεται εσωτερική χρήση του εργαλείου προκειμένου να ανακαλυφθούν άλλα σφάλματα. Θα πρέπει να εφαρμοστεί μέχρι ο μέσος χρόνος μεταξύ αποτυχιών να είναι αρκετά μεγάλος.

Στα πλαίσια του ελέγχου αυτού θα δοκιμαστούν μια σειρά διαφορετικών σεναρίων και περιπτώσεων πληροφοριακών συστημάτων στα οποία θα πραγματοποιηθεί ανάλυση και διαχείριση της επικινδυνότητας με τη χρήση του εργαλείου.

Χρήστες εξωτερικά του φορέα ανάπτυξης του εργαλείου επιλέγονται για να ελέγξουν την λειτουργικότητα του εργαλείου. Οι αναπτυκτές του εργαλείου θα πρέπει να διατηρούν συνεχή επικοινωνία με τους χρήστες του ελέγχου beta.

- Συμμόρφωση ή μη του εργαλείου σε συγκεκριμένα σύνολα δεδομένων
- Πλήρη αποτελέσματα ελέγχων συνοδευόμενα από ημερομηνία και αριθμό έκδοσης.

Κριτήρια Ολοκλήρωσης

1.Οι ενημερώσεις στην τεκμηρίωση χρήστη και συστήματος έχουν ολοκληρωθεί σύμφωνα με τα πρότυπα τροποποίησης εγγράφων τεκμηρίωσης.
2.Υπάρχουν εγγραφές ελέγχου και ικανοποιούν το πρότυπο
3.Οι εγγραφές ελέγχου είναι ενημερωμένες. Θα πρέπει να υπάρχουν αποδείξεις ότι το εργαλείο έχει ελεγχθεί με σαφή αναφορά στους ελέγχους και τις επισκοπήσεις που έχουν πραγματοποιηθεί στο εργαλείο.

7.3 Έλεγχος Αποδοχής

Ο έλεγχος αποδοχής αποτελεί το τελευταίο στάδιο της διαδικασίας ελέγχου, προτού το εργαλείο να μπορεί να χρησιμοποιηθεί τυπικά για εμπορική εκμετάλλευση. Περιλαμβάνει τον έλεγχο του εργαλείου με δεδομένα πραγματικά, σε αντιδιαστολή με τα προσομοιωμένα τα οποία παράχθηκαν ως μέρος της διαδικασίας ελέγχου. Ο έλεγχος αυτός είναι δυνατόν να δείξει ότι το εργαλείο δεν παρουσιάζει την αναμενόμενη απόδοση και λειτουργικότητα.

Οι ενέργειες που θα πρέπει να γίνουν στη φάση αυτή είναι οι εξής:

1) Αναθεώρηση του Πλάνου Αποδοχής. Μεταξύ των άλλων θα πρέπει να περιλαμβάνονται:
- **i.**Οι έλεγχοι που θα πραγματοποιηθούν.
- **ii.**Τα δεδομένα ελέγχου.
- **iii.**Η κατανομή του χρόνου.

Ο έλεγχος αποδοχής θα πρέπει να γίνει σε πραγματικές συνθήκες χρήσης του εργαλείου, χρησιμοποιώντας πραγματικά δεδομένα.

2) Πραγματοποίηση ελέγχου αποδοχής:
- **i.**Εντοπισμός στοιχείων ανεπαρκούς απόδοσης, αδυναμίες ή παραλήψεις απαιτήσεων του συστήματος. Τα σφάλματα αυτά θα πρέπει να διορθωθούν σύμφωνα με τον έλεγχο κώδικα ενοτήτων. Θα πρέπει να πραγματοποιηθούν δυο ομάδες ελέγχων.
  - **a)** Ο έλεγχος που αναπτύχθηκε από την ομάδα εξασφάλισης ποιότητας.

b) Ο έλεγχος που αναπτύχθηκε από τους χρήστες.

ii. Η διαδικασία (2.1) θα επαναληφθεί μέχρι το εργαλείο να παρουσιάζει το απαιτούμενο επίπεδο λειτουργικότητας όπως αυτό ορίζεται στην ανάλυση απαιτήσεων και να γίνει αποδεκτό από το χρήστη για εγκατάσταση και κανονική χρήση.

3) Οποιεσδήποτε αλλαγές στις απαιτήσεις του συστήματος , στο σχέδιο , στον έλεγχο ή στα έγγραφα τεκμηρίωσης του χρήστη θα πρέπει να εγκριθούν από την ομάδα διαχείρισης του έργου.

7.4 Τεκμηρίωση

Η τεκμηρίωση περιλαμβάνει όλα τα έγγραφα στα οποία περιγράφεται η υλοποίηση του εργαλείου από την ανάλυση απαιτήσεων ως το τελικό πλάνο ελέγχου. Η τεκμηρίωση η οποία αφορά το σχεδιασμό, την υλοποίηση και τον έλεγχο του λογισμικού, έχει εξαιρετική σημασία ιδιαίτερα αν πρέπει αυτό να γίνει κατανοητό και να υποστεί και να υποστεί κάποιου είδους συντήρηση. Η τεκμηρίωση του χρήστη παρέχει στον χρήστη μια περιγραφή του προϊόντος συμπεριλαμβανομένων και των λειτουργιών που αυτό θα επιτελεί με την ολοκλήρωση της ανάπτυξης του. Η δημιουργία υψηλής ποιότητας εγγράφων τεκμηρίωσης έχει εξαιρετική σημασία, ενώ οι παράγοντες που επηρεάζουν την ποιότητα είναι:

- Τα σχετικά με την τεκμηρίωση πρότυπα
- Η διαδικασία εξασφάλισης ποιότητας για τεκμηρίωση και
- Η αποτελεσματικότητα του ύφους γραφής.

Οι ενέργειες που θα πρέπει να γίνουν σχετικά με την τεκμηρίωση έχουν ως εξής:

1. Θα πρέπει να οριστεί ένας συντονιστής τεκμηρίωσης. Το άτομο αυτό θα μπορούσε να είναι ένα από τα μέλη της ομάδας ανάπτυξης το οποίο έχει επιφορτιστεί ειδικά με αυτό το ρόλο.

2. Θα πρέπει να υιοθετηθούν κατάλληλα πρότυπα τεκμηρίωσης για τα έγγραφα των χρηστών και του συστήματος:

I. Προσδιορίζουν τη διαδικασία που θα ακολουθηθεί για την παραγωγή υψηλής ποιότητας εγγράφων τεκμηρίωσης.

i. Θα πρέπει να οριστούν τα εργαλεία λογισμικού που θα χρησιμοποιηθούν για την παραγωγή των εγγράφων.

ii. Θα πρέπει να οριστούν διαδικασίες εξασφάλισης ποιότητας. Αυτές θα είναι αρκετά ευέλικτες ώστε να είναι ικανές να αντιμετωπίσουν κάθε τύπο εγγράφου τεκμηρίωσης ενώ θα πρέπει να αναφέρονται σε θέματα όπως το ποιος θα εξουσιοδοτεί αλλαγές στα έγγραφα που παράγονται και το πώς θα εξασφαλίζεται ότι όλες οι πληροφορίες που χρησιμοποιούνται, θα ενημερώνονται.

iii. Θα πρέπει να ακολουθείται μια επαναληπτική διαδικασία συγγραφής, διόρθωσης και αναθεώρησης μέχρι να γίνει η αποδοχή του εγγράφου από τον συντονιστή της τεκμηρίωσης.

II. Τα πρότυπα αυτά αφορούν τον έλεγχο των εγγράφων που παράγονται. Αυτά περιλαμβάνουν:

i. Πρότυπα προσδιορισμού εγγράφων τεκμηρίωσης: Τα πρότυπα αυτά ορίζουν κανόνες για τον προσδιορισμό των εγγράφων τεκμηρίωσης για το συγκεκριμένο έργο.

ii. Πρότυπα δόμησης των εγγράφων τεκμηρίωσης: Αυτά τα πρότυπα καθορίζουν την κατάλληλη δομή για κάθε τύπο εγγράφου τεκμηρίωσης που θα παραχθεί.

iii. Πρότυπα παρουσίασης εγγράφων τεκμηρίωσης: Αυτά περιγράφουν τα απαιτούμενα φυσικά χαρακτηριστικά των εγγράφων ,όπως τη χρήση γραμματοσειρών, στυλ, χρωμάτων.

iv. Πρότυπα ενημέρωσης εγγράφων τεκμηρίωσης: Αυτά περιγράφουν τον τρόπο με τον οποίο το σύστημα ξεχωρίζει τις διαφορετικές εκδόσεις εγγράφων τεκμηρίωσης. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στην ενημέρωση της τεκμηρίωσης που βρίσκεται σε ηλεκτρονική μορφή.

III. Αυτά εξασφαλίζουν ότι όλα τα ηλεκτρονικά αντίγραφα των εγγράφων είναι συμβατά.

3. **Τα έγγραφα του χρήστη θα πρέπει να είναι πλήρη και κατατοπιστικά**. Σε αυτά θα πρέπει να περιλαμβάνονται:

i. Μια συνολική άποψη του εργαλείου
ii. Μια συνοπτική αναφορά των απαιτήσεων του εργαλείου
iii. Μια σύντομη περιγραφή των υπηρεσιών που παρέχονται από το εργαλείο.

i. Μια ανεπίσημη εισαγωγή στο εργαλείο
ii. Μια περιγραφή της κανονικής χρήσης του εργαλείου
iii. Συμβουλές για το πώς να ξεκινήσει κάποιος τη χρήση του εργαλείου
iv. Εξήγηση της χρήσης των συνηθέστερων ευκολιών/ λειτουργιών του εργαλείου
v. Παραδείγματα χρήσεων του εργαλείου
vi. Συμβουλές για την ανακάλυψη λαθών.

III. Αυτό περιλαμβάνει:

i. Πως θα πρέπει να γίνει η εγκατάσταση του εργαλείου σε ένα συγκεκριμένο περιβάλλον.
ii. Μια περιγραφή των μέσων για τα οποία παρέχεται το εργαλείο, αρχεία του εργαλείου, ελάχιστες απαιτήσεις για τη διόρθωση του υλικού, μόνιμα αρχεία που δημιουργούνται στο σύστημα κατά την εγκατάσταση και το πώς πρέπει να γίνεται η έναρξη του εργαλείου.

i. Αναλυτική παρουσίαση εντολών του εργαλείου και τη χρησιμότητα τους
ii. Παροχή λίστας με μηνύματα λάθους και πώς μπορεί να γίνει επαναφορά μετά από την εμφάνιση σφάλματος.

V. Αυτό περιλαμβάνει:

i. Περιγραφή των μηνυμάτων τα οποία παράγονται όταν το εργαλείο αλληλεπιδρά με άλλα συστήματα και πώς ο διαχειριστής συστήματος θα πρέπει να αντιδρά.
ii. Αναφορά των διαδικασιών για τη συντήρηση του υλικού
iii. Περιγραφή μια γενικής άποψης του συστήματος.

4. Θα πρέπει να δημιουργηθούν και όλα τα απαραίτητα έγγραφα τεκμηρίωσης του συστήματος. Αυτά περιλαμβάνουν:

I. Το έγγραφο απαιτήσεων λογισμικού
II. Ένα έγγραφο που να περιγράφει την αρχιτεκτονική του συστήματος
III. Μια περιγραφή της δομής κάθε τμήματος του εργαλείου
IV. Περιγραφή των προδιαγραφών και του σχεδίου για κάθε τμήμα (component)
V. Παράθεση του πηγαίου κώδικα του προγράμματος
VI. Έγγραφα επικύρωσης τα οποία θα περιγράφουν πως επικυρώνεται κάθε τμήμα του προγράμματος και τη σχέση ανάμεσα στην επικύρωση και τις απαιτήσεις
VII. Έναν οδηγό συντήρησης του συστήματος το οποίο θα πρέπει να περιλαμβάνει:
   i. Περιγραφή γνωστών προβλημάτων
   ii. Περιγραφή των τμημάτων του συστήματος τα οποία εξαρτώνται από υλικό ή λογισμικό
   iii. Περιγραφή του τρόπου με τον οποίο η εξέλιξη του εργαλείου έχει ληφθεί υπόψη κατά τη σχεδίαση του.

5. Θα πρέπει να πραγματοποιηθεί μια **εσωτερική αναθεώρηση** ,προκειμένου να βεβαιωθεί η ακρίβεια και πληρότητα της τεκμηρίωσης.

6. Αναθεώρηση και επικύρωση των εγχειριδίων χρήστη και των σχετικών εγγράφων του συστήματος με την ομάδα συντήρησης και με πιθανούς πελάτες.

Παράδειγμα Διάταξης Σελίδων ενός Προτύπου Μορφότυπου για Τεκμηρίωση

1. Εξώφυλλο

a) Συγγραφέας του εγγράφου/ ομάδα ανάπτυξης λογισμικού
b) Τίτλος του εγγράφου
c) Ημερομηνία παραγωγής και αριθμός έκδοσης
d) Τύπος εγγράφου
e) Πληροφορίες διαχείρισης διάρθρωσης (configuration management) και εξασφάλισης ποιότητας
f) Αποδέκτες
g) Κλάση εμπιστευτικότητας
h) Στοιχεία ανάκτησης (retrieval) του εγγράφου και σημείωση περί πνευματικών δικαιωμάτων.

2. Κεφάλαια / Παράγραφοι και Υποπαράγραφοι

a) Πίνακας περιεχομένων
b) Συνεπές σχήμα αρίθμησης
c) Κεφάλαια με μεμονωμένη αρίθμηση

3. Ευρετήριο
Σε περίπτωση που το έγγραφο περιέχει λεπτομερείς πληροφορίες αναφοράς.

4. Γλωσσάριο Όρων
Αν πρόκειται να δοθεί σε ανθρώπους οι οποίοι δεν είναι εξοικειωμένοι με την ορολογία.

Πρότυπα Σχετικά με Τεκμηρίωση

Κωδική Ονομασί	Τίτλος
IEEE STD 1063-1987	IEEE standard for Software User Documentation
IEEE STD 1362-1998	IEEE Guide for Information Technology – System Definition- Concept of Operations (ConOps) Document
IEEE STD 610.12-1990	IEEE Standard Glossary of Software Engineering Terminology
IEEE STD 830-1993	IEEE Recommended Practice for Software Requirements Specifications
ISO 6592:1985	Information Processing. Guidelines for the Documentation of computer – based application systems
ISO/ IEC TR 9294:1990	Information Technology. Guidelines for the management of software documentation

ΚΕΦΑΛΑΙΟ 8

ΕΚΤΙΜΗΣΗ ΧΡΟΝΟΔΙΑΓΡΑΜΜΑΤΟΣ ΤΩΝ ΕΡΓΑΣΙΩΝ ΠΟΥ ΘΑ ΑΚΟΛΟΥΘΗΘΟΥΝ

ΔΙΑΧΕΙΡΙΣΗ ΕΡΓΟΥ

Η ανάπτυξη ενός εργαλείου υποστήριξης της ανάλυσης και διαχείρισης της επικινδυνότητας των πληροφοριακών συστημάτων παρουσιάζει ορισμένες ιδιαιτερότητες και δυσκολίες σε σύγκριση με άλλα περισσότερο παραδοσιακά έργα ανάπτυξης εφαρμογών λογισμικού.

- Δεν υπάρχει η δυνατότητα να εξεταστούν ως προς τη λειτουργία τους να συγκριθούν άλλα εργαλεία (πέρα από ένα το οποίο έχει αγοραστεί), τα οποία να ενσωματώνουν σχετικές με το προς ανάπτυξη εργαλείο, λειτουργίες. Ο λόγος που συμβαίνει αυτό είναι γιατί η απόκτηση υψηλών αξιώσεων αντίστοιχων εργαλείων έχει μεγάλο ως υπέρογκο κόστος για έναν ακαδημαϊκό φορέα.

- Ο αριθμός των ατόμων που έχουν κάποια εμπειρία σχετική με την ανάλυση και διαχείριση της επικινδυνότητας στον ελλαδικό χώρο είναι σχετικά μικρός. Αυτό έχει σαν συνέπεια να υπάρχει μια δυσκολία στην εύρεση ικανοποιητικού πλήθους αντιπροσωπευτικών χρηστών.

➔ Η ανάπτυξη μιας αποτελεσματικής μεθόδου ανάλυσης και διαχείρισης είναι μια αρκετά πολύπλοκη και γεμάτη δυσκολίες διαδικασία. Το πόσο αποτελεσματική θα είναι η αντιμετώπιση της πολυπλοκότητας θα κρίνει και την επιτυχία του τελικού προϊόντος.

➔ Μια ακόμα ιδιαιτερότητα της ανάπτυξης ενός τέτοιου εργαλείου είναι η ανάγκη συμμετοχής και συνεργασίας πολλών διαφορετικών ειδικοτήτων μέσα από τον κλάδο της πληροφορικής. Ανάμεσα στις ειδικότητες που θα εμπλακούν είναι οι εξής:

1. Ειδικός σε θέματα ασφαλείας.
2. Ειδικός σε θέματα ασφαλείας με έμφαση σε θέματα τεχνικά και υλοποίησης της ασφαλείας.
3. Ειδικός σε θέματα δικτύων.
4. Ειδικός σε θέματα επικοινωνίας ανθρώπου μηχανής.
5. Ψυχολόγος (συμμετοχή στη σύνταξη των ερωτηματολογίων).
6. Ειδικός σε θέματα ελέγχου λογισμικού.
7. Ειδικός σε θέματα που αφορούν επιχειρήσεις
8. Αναλυτής ο οποίος θα έχει γνώσεις γύρω από τη λειτουργία των επιχειρήσεων αλλά και γνώσεις σε θέματα ασφαλείας.
9. Σχεδιαστής συστημάτων με αρκετή εμπειρία.
10. Ειδικός σε θέματα βάσεων Δεδομένων.
11. Ειδικός σε θέματα εξασφάλισης ποιότητας λογισμικού.
12. Διαχειριστής έργων πληροφορικής με αρκετή εμπειρία.
13. Προγραμματιστής με αρκετή εμπειρία.

ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ ΕΡΓΑΣΙΩΝ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΑΚΟΛΟΥΘΗΘΟΥΝ

ID	Ονομασία Εργασίας	Διάρκεια	Έναρξη	Ολοκλήρωση
1	Διερευνητική Μελέτη	96 days	4/10/2005	14/2/2006
2	Προκαταρκτική σύνταξη των Απαιτήσεων Του εργαλείου	72 days	4/10/2005	11/1/2006
3	Συλλογή παρατηρήσεων και διορθώσεων	8 days	12/1/2006	21/1/2006
4	Υποβολή παρατηρήσεων και διορθώσεων	0 days	21/1/2006	21/1/2006
5	Αναθεώρηση της προκαταρκτικής σύνταξης απαιτήσεων	16 days	24/1/2006	14/2/2006
6	Μελέτη σκοπιμότητας	45 days	14/2/2006	14/4/2006
7	Προκαταρκτικό σχέδιο του έργου (project plan) και προδιαγραφών των απαιτήσεων	30 days	14/2/2006	24/3/2006
8	Συλλογή παρατηρήσεων και διορθώσεων	5 days	27/3/2006	31/3/2006
9	Αναθεώρηση του σχεδίου του έργου και των προδιαγραφών	10 days	3/4/2006	14/4/2006
10	Ανάλυση απαιτήσεων	58 days	17/4/2006	05/7/2006
11	Έρευνα αγοράς	20 days	17/4/2006	12/5/2006
12	Προετοιμασία ερωτηματολογίων	5 days	17/4/2006	21/4/2006
13	Αναζήτηση συμμετεχόντων στην αγορά	5 days	17/4/2006	21/4/2006
14	Συλλογή στοιχείων	15 days	24/4/2006	12/5/2006
15	Συνεντεύξεις	14 days	17/4/2006	04/5/2006

16	Προετοιμασία ερωτηματολογίου - πιλότου	3 days	17/4/2006	19/4/2006
17	Επικύρωση ερωτηματολογίου	1 day	20/4/2006	20/4/2006
18	Πραγματοποίηση συνεντεύξεων	10 days	21/4/2006	04/5/2006
19	Επεξεργασία στοιχείων	10 days	17/4/2006	28/4/2006
20	Ανάπτυξη ενός γενικού μοντέλου του εργαλείου	25 days	28/4/2006	01/6/2006
21	Σύνταξη εγγράφου «Προδιαγραφών απαιτήσεων»	20 days	01/6/2006	28/6/2006
22	Επικύρωση των απαιτήσεων από τους χρήστες	5 days	29/6/2006	05/7/2006
23	Σύσταση ομάδας σχεδίασης	5 days	30/6/2006	06/7/2006
24	Σχεδιασμός του συστήματος	86 days	07/7/2006	03/11/2006
25	Αναθεώρηση του πλάνου του έργου	1 day	07/7/2006	07/7/2006
26	Ανασκόπηση συστημάτων που κάνουν παρόμοιες λειτουργίες	10 days	10/7/2006	21/7/2006
27	Σύνταξη προκαταρκτικών προδιαγραφών σχεδίασης	15 days	21/7/2006	10/8/2006
28	Πάγωμα του προκαταρκτικού σχεδίου	5 days	11/8/2006	17/8/2006
29	Ανάπτυξη του τυπικού σχεδίου	60 days	24/7/2006	13/10/2006
30	Αναθεώρηση και επικύρωση του σχεδίου από τους χρήστες	10 days	16/10/2006	27/10/2006
31	Πάγωμα του τυπικού σχεδίου	5 days	30/10/2006	03/11/2006
32	Σύσταση ομάδας προγραμματισμού	10 days	06/11/2006	17/11/2006
33	Σύνταξη του κώδικα	301 days	20/11/2006	14/01/2006
34	Αναθεώρηση του πλάνου του έργου	1 day	20/11/2006	20/11/2006
35	Κωδικοποίηση	300 days	21/11/2006	14/01/2006
36	Σύσταση ομάδας ελέγχου	15 days	14/01/2006	01/02/2006
37	Έλεγχος κώδικα	121 days	04/02/2006	22/07/2006
38	Αναθεώρηση του πλάνου του έργου	1 day	04/02/2006	04/02/2006
39	Έλεγχος κώδικα ενοτήτων	40 days	05/02/2006	01/04/2006
40	Έλεγχος συστήματος και αποδοχής	80 days	02/04/2006	22/07/2006
41	Σύνταξη εγγράφων τεκμηρίωσης του χρήστη	60 days	23/07/2006	14/10/2006

ΚΕΦΑΛΑΙΟ 9

ΛΥΣΕΙΣ ΧΡΗΜΑΤΟΔΟΤΗΣΗΣ

Εναλλακτικές πηγές χρηματοδότησης:

1. Το ακαδημαϊκό ίδρυμα με τους δικούς του πόρους.

Η ανάπτυξη του λογισμικού θα γίνει με τους πόρους και τις δυνατότητες που παρέχονται από το ακαδημαϊκό ίδρυμα. Η υλοποίηση θα γίνει για την χρήση του από έμπειρους χρήστες, ωστόσο ο κώδικας του εργαλείου θα δίνεται σε μορφή open source.

Εκμετάλλευση:Πώληση των εγχειριδίων χρήσης.
Πλεονεκτήματα:Η λύση open source.
Μειονεκτήματα:1)Χρονοβόρος διαδικασία
2)Καλή διαχείριση του open source

Η ανάπτυξη θα αποτελέσει πρόταση ερευνητικού προγράμματος και θα χρηματοδοτηθεί στα πλαίσια αυτού.

Εκμετάλλευση:Θα ορίζεται από το είδος του ερευνητικού έργου.
Πλεονεκτήματα:Οργανωμένη προσπάθεια ανάπτυξης.
Μειονεκτήματα:1)Για να ανατεθεί θα πρέπει να προβάλλει στοιχεία καινοτομίας και ερευνητικής προσπάθειας τα οποία δεν περιλαμβάνονται απαραίτητα σε αυτό.
2)Χρονοβόρος διαδικασία
3)Πολύ γραφειοκρατική εργασία
4)Θα απαιτηθεί η αναζήτηση συνεργασιών οι οποίες δεν είναι σίγουρο ότι θα βρεθούν.

Η χρηματοδότηση θα γίνει από εταιρεία συμβούλων και η ανάπτυξη θα γίνει στο χώρο του ακαδημαϊκού ιδρύματος και με χρήση των πόρων αυτού.

Εκμετάλλευση:1)Μισά – μισά τα δικαιώματα χρήσης. Χρησιμοποιείται από τα δύο μέρη για ιδία χρήση.
2)Το ακαδημαϊκό ίδρυμα το χρησιμοποιεί για ιδία ρήση μόνο , η εταιρεία εκτός από ιδία χρήση μπορεί να το πουλήσει σε εταιρείες πελατών.
Πλεονεκτήματα:Μικρότερος χρόνος ανάπτυξης.
Μειονεκτήματα:Υψηλό κόστος, γιατί χρειάζονται άνθρωποι με υψηλή εμπειρία και γνώση. Αν μοναδικό κίνητρο για αυτούς είναι η αμοιβή τότε η αμοιβή θα πρέπει να είναι πολύ υψηλή.

Η χρηματοδότηση θα γίνει από εταιρεία συμβούλων και η ανάπτυξη θα γίνει από εταιρεία ανάπτυξης λογισμικού υπό την εποπτεία και με τη συνεργασία του ακαδημαϊκού ιδρύματος.

Εκμετάλλευση:Το ακαδημαϊκό ίδρυμα το χρησιμοποιεί για ιδία χρήση μόνο, η εταιρεία εκτός από ιδία χρήση μπορεί και να το πουλήσει σε εταιρείες πελατών. Η εταιρεία ανάπτυξης δεν έχει κανένα δικαίωμα.
Πλεονεκτήματα:Μικρότερος χρόνος ανάπτυξης.
Μειονεκτήματα:1)Υψηλό κόστος γιατί χρειάζονται άνθρωποι με υψηλή εμπειρία και γνώση. Αν μοναδικό κίνητρο για αυτούς είναι η αμοιβή θα πρέπει να είναι πολύ υψηλή.
2)Οι εταιρείες λογισμικού δεν έχουν την τεχνογνωσία άρα καταλήγουμε πάλι στα προηγούμενα μειονεκτήματα.

ΚΕΦΑΛΑΙΟ 10

ΣΧΕΔΙΑΣΗ ΕΡΓΑΛΕΙΟΥ

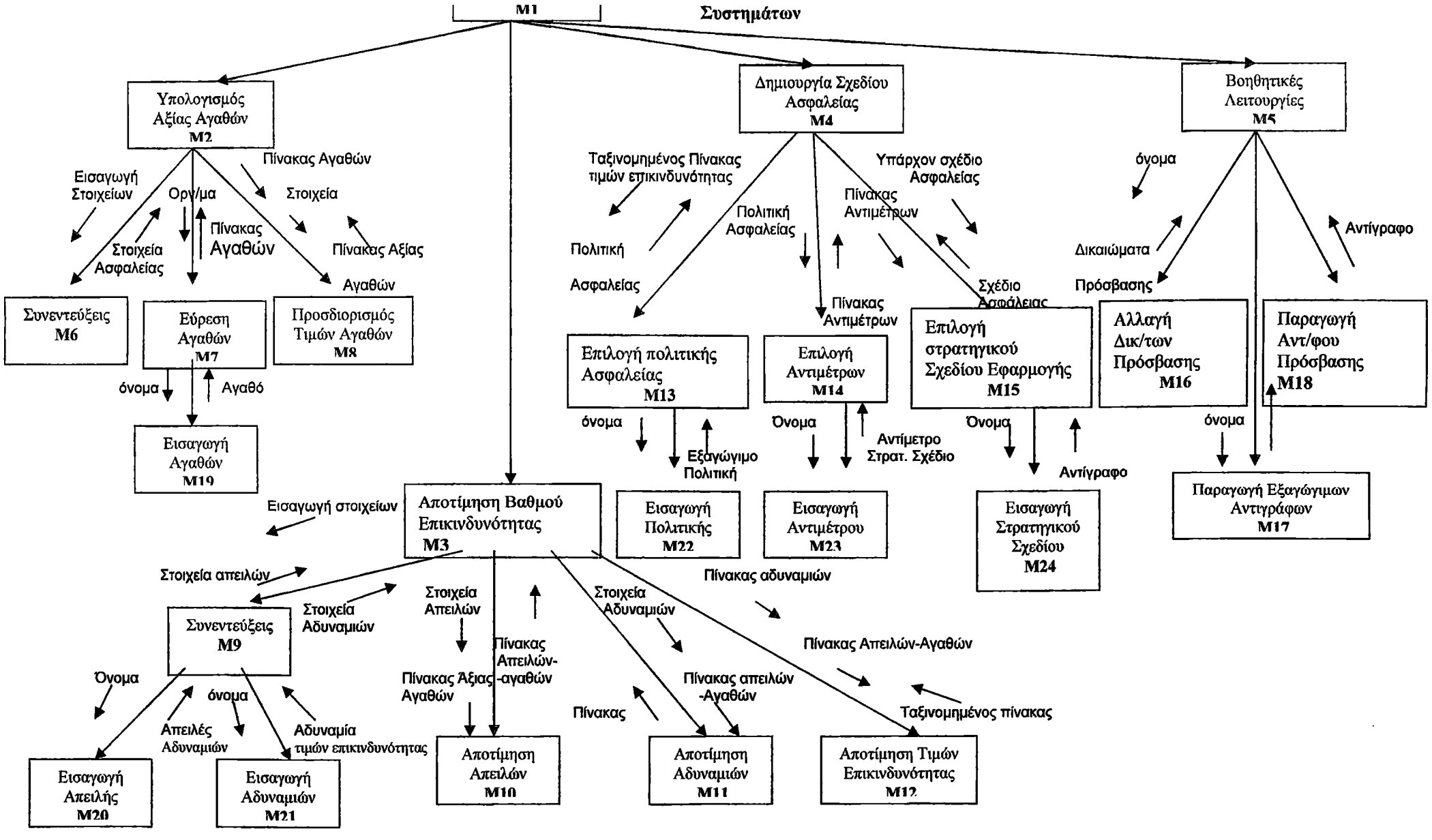
Όπως προαναφέρθηκε η σχεδίαση θα ακολουθήσει το μοντέλου του κύκλου ζωής του λογισμικού του IEEE .Στο κεφάλαιο αυτό θα παραχθεί ένα τμήμα αυτού , το Έγγραφο Περιγραφής Σχεδίου Λογισμικού καθώς το υπό εξέταση εργαλείο είναι λογισμικό, όπως αυτό προσδιορίζεται από το πρότυπο ANSI/IEEE Std 1016/1984. Θα προσπαθήσουμε να διατηρήσουμε την πρότυπη μορφή του προσαρμόζοντας το στια ανάγκες αυτής της εργασίας.

10.1 Έγγραφο Περιγραφής Σχεδίου Λογισμικού

Στο ΕΠΣΛ περιγράφονται όλα εκείνα τα στοιχεία που χρειάζονται για την κωδικοποίηση και συντήρηση του Λογισμικού. Έτσι τα δεδομένα του ΕΠΑΛ εδώ αναλύονται διεξοδικά μετατρέποντας τα στις κατάλληλες μορφές. Δηλαδή αποτελεί μια μεταφορά των απαιτήσεων σε μια περιγραφή της δομής του λογισμικού, των στοιχείων του λογισμικού, των διεπαφών και των δεδομένων που είναι απαραίτητα για την υλοποίηση.

10.1.1 Περιγραφή Αποσύνθεσης

Η περιγραφή της αποσύνθεσης αποτυπώνει τη διαίρεση του συστήματος Λογισμικού σε οντότητες σχεδίου. Για την παρουσίαση θα χρησιμοποιηθούν Διαγράμματα Δομής που παρουσιάζουν την ιεραρχία των μονάδων του συστήματος. Στα παρακάτω σχήματα απεικονίζονται οι μονάδες.
Είναι ορατό ότι οι μονάδες αντιστοιχούν στις λειτουργίες του συγκεκριμένου εργαλείου. Η περαιτέρω αποσύνθεση οφείλεται στην καλύτερη υλοποίηση του συγκεκριμένου λογισμικού


Συστημάτων
Υπολογισμός Αξίας Αγαθών M2
Δημιουργία Σχεδίου Ασφαλείας M4
Βοηθητικές Λειτουργίες M5
Εισαγωγή Στοιχείων
Ορ/μα
Πίνακας Αγαθών
Στοιχεία
Πίνακας Αγαθών
Στοιχεία Ασφαλείας
Πίνακας Αξίας Αγαθών
Ταξινομημένος Πίνακας τιμών επικινδυνότητας
Υπάρχον σχέδιο Ασφαλείας
Πολιτική Ασφαλείας
Πίνακας Αντιμέτρων
Πολιτική Ασφαλείας
Πίνακας Αντιμέτρων
Σχέδιο Ασφάλειας
όνομα
Δικαιώματα Πρόσβασης
Αντίγραφο
Συνεντεύξεις M6
Εύρεση Αγαθών M7
Προσδιορισμός Τιμών Αγαθών M8
Επιλογή πολιτικής Ασφαλείας M13
Επιλογή Αντιμέτρων M14
Επιλογή στρατηγικού Σχεδίου Εφαρμογής M15
Αλλαγή Δικ/των Πρόσβασης M16
Παραγωγή Αντ/φου Πρόσβασης M18
όνομα
Αγαθό
Όνομα
Όνομα
όνομα
Εισαγωγή Αγαθών M19
Εξαγώγιμο Πολιτική
Αντίμετρο Στρατ. Σχέδιο
Αντίγραφο
Παραγωγή Εξαγώγιμων Αντιγράφων M17
Εισαγωγή στοιχείων
Αποτίμηση Βαθμού Επικινδυνότητας M3
Εισαγωγή Πολιτικής M22
Εισαγωγή Αντιμέτρου M23
Εισαγωγή Στρατηγικού Σχεδίου M24
Στοιχεία απειλών
Πίνακας αδυναμιών
Στοιχεία Αδυναμιών
Στοιχεία Απειλών
Στοιχεία Αδυναμιών
Πίνακας Απειλών-Αγαθών
Συνεντεύξεις M9
Πίνακας Απειλών-αγαθών
Πίνακας Άξιας Αγαθών
Πίνακας απειλών -Αγαθών
Πίνακας
Ταξινομημένος πίνακας
Όνομα
όνομα
Απειλές Αδυναμιών
Αδυναμία τιμών επικινδυνότητας
Εισαγωγή Απειλής M20
Εισαγωγή Αδυναμιών M21
Αποτίμηση Απειλών M10
Αποτίμηση Αδυναμιών M11
Αποτίμηση Τιμών Επικινδυνότητας M12

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

1)Γιακουμάκης Ε.Α. ,Τεχνολογία Λογισμικού –Απαιτήσεις Λογισμικού,Σχεδίαση Λογισμικού Τόμος Α, Εκδόσεις Α. Σταμούλης, Αθήνα- Πειραιάς 1994.

2)Κιουντούζης Ε.Α., Μεθοδολογίες Ανάλυσης και Σχεδιασμού Πληροφοριακών Συστημάτων, Εκδόσεις Ευγ. Μπένου, Αθήνα 1997.

3)Κιουντούζης Ε.Α., Διοικητικός Προγραμματισμός έργων Πληροφορικής, Τεχνικές Ελέγχου, Σχεδιασμού και management. Εκδόσεις Σταμούλης, Αθήνα 1993

4)Κιουντούζης Ε.Α. ,Ασφάλεια Πληροφοριακών Συστημάτων, Έκδοσης Μπένου, Αθήνα 2001

5)Σκορδαλάκης Ε. Εισαγωγή στη Τεχνολογία Λογισμικού, Εκδόσεις Συμμετρία, Αθήνα 1991

6)Κάτσικας Σ, Διαχείριση Κινδύνων Πληροφοριακών Συστημάτων, στο Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Κιουντούζης Ε, Αλεξανδρής Ν και Τραπεζάνογλου Β., Εκδόσεις Νέων Τεχνολογιών, 1995.

7)Λαοπόδης Βασίλης. Ανάλυση και Σχεδιασμός Συστημάτων, Εκδόσεις Νέων Τεχνολογιών 1992

8)Δημητριάδης Αντώνης, Διοίκηση – Διαχείριση Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών,1998.

9)Γιαννακόπουλος Διον. ,Παπουτσής Ιωαν. Πληροφοριακά Συστήματα Διοίκησης. Εκδόσεις Έλλην 2000

10)Μπελληγιάννης Γρηγ, Ανάλυση και Σχεδιασμός Πληροφοριακών Συστημάτων(Σημειώσεις),ΑΤΕΙ Μεσολογγιου,2005

11)Καραγιάννης Γεωργ,ΑσφάλειαΠληροφοριακών Συστημάτων (Σημειώσεις),ΑΤΕΙ Μεσολογγίου 2005

12) Γιακουμάκης Ε.Α. ,Τεχνολογία Λογισμικού –Κωδικοποίηση, Έλεγχος και Συντήρηση Λογισμικού Εκδόσεις Α. Σταμούλης, Αθήνα- Πειραιάς 1996.

ΞΕΝΗ

1)Kowalski, IT insecurity :A multi-disciplinary inquiry, PhD Thesis Stockholm University, Sweden 1994.

2)McCumber J.R. Information Systems Security comprehensive model, in Proceedings of the 14th National Computer Security Conference, National Computer Sequrity,1991.

3)Baskerville R, information Systems Security Design Methods : Implications for Information Systems Development, ACM Computing Surveys, 1993

4)Anderson and Shain, Risk Management, in Caelli W, Longley D and Shain M , Information Security Handbook, MacMillan,1991

5)Pfleeger CP, Security in computing, Prentice Hall,1997

6)European Security forum, How to establish a satisfactory IT Risk Analysis Process 1990.

7)Kiountouzis E.A. , Kokolakis S.A. An analyst's view of IS Security, in Information System Security facing the information society of the 21st Century, Chapman &Hall,1996

8)Bernstein PL. against the Gods: The Remarkable Story of Risk, John Wiley &Sons, New York1996

9)Hurst NW, Risk Assessment: The Human Dimension, The Royal Society of Chemistry.Cambridge.1998

ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ-ΔΙΑΔΙΚΤΥΟ

1)www.iso.ch
2)www.bcs.org.uk
3)www.wssn.net
4)www.standards.ieee.org
5)www.ccta.gov.gr