

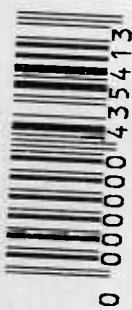


14 ΤΗΜΑ  
ΑΘΗΝΩΝ  
ΕΒΛΙΟΘΗΚΗ  
68655  
005 8  
100... ΜΕ

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ**  
**ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)**  
**στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ  
ΚΑΤΑΣΤΟΣ



**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

«Σχεδίαση εργαλείου υποστήριξης της ανάλυσης και  
διαχείρισης επικινδυνότητας Πληροφοριακών  
Συστημάτων»

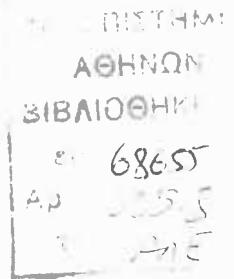
**Αλεξοπούλου Μαρίνα**

**M3990020**

**ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2001**



**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)  
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**



**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

**«Σχεδίαση εργαλείου υποστήριξης της ανάλυσης και  
διαχείρισης επικινδυνότητας Πληροφοριακών  
Συστημάτων»**

**Αλεξοπούλου Μαρίνα**

**M3990020**

**Επιβλέπων Καθηγητής: Ευάγγελος Κιουντούζης  
Εξωτερικός Κριτής: Καθηγητής Δ. Γκρίτζαλης**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ  
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

**ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2001**



## Πρόλογος και Ευχαριστίες

Η εργασία αυτή αποτελεί τη διατριβή που πραγματοποιήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών (MSc) στα Πληροφοριακά Συστήματα του Οικονομικού Πανεπιστημίου Αθηνών. Στην εργασία αυτή συνέβαλαν, με διαφορετικό τρόπο ο καθένας, πολλοί άνθρωποι τους οποίους θα ήθελα να ευχαριστήσω.

Πρώτα από όλα θα ήθελα να ευχαριστήσω τον Καθηγητή Ευάγγελο Κιουντούζη που ήταν και ο επιβλέπων καθηγητής στην εργασία αυτή. Ο τομέας ενασχόλησής του με προέτρεψε να συνεχίσω τις σπουδές μου σε μεταπτυχιακό επίπεδο και να ολοκληρωθεί η παρούσα εργασία με το συγκεκριμένο θέμα, χάρη στην καθοδήγησή του. Ένα ευχαριστώ και στον Καθηγητή Δημήτριο Γκρίζαλη, που ήταν και ο εξωτερικός κριτής, καθώς η παρακολούθηση της διδασκαλίας του γνωστικού του αντικειμένου συνέβαλε στην επιλογή του συγκεκριμένου θέματος. Ακόμη, θα ήθελα να ευχαριστήσω τον Καθηγητή Σωκράτη Κάτσικα και τον Διδάκτορα Σπύρο Κοκολάκη που μου διέθεσαν το χρόνο τους και τις γνώσεις τους.

Ευχαριστώ, επίσης, τον κύριο Κωνσταντίνο Τσιγκριστάρη που πίστεψε σε εμένα, με σεβάστηκε και με διευκόλυνε στο να υλοποιήσω την εργασία αυτή. Ένα ευχαριστώ και σε όλους εκείνους τους συνάδελφους που βοήθησαν με τον τρόπο τους και με την ιδιότητά τους στο να δω την επιστήμη με μία διαφορετική οπτική γωνία.

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

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

*Μαρίνα Αλεξοπούλου*

*Φεβρουάριος 2001*



## Πίνακας Περιεχομένων

Πρόλογος και Ευχαριστίες .....	1
Πίνακας Περιεχομένων.....	2
Ευρετήριο Πινάκων.....	4
Ευρετήριο Σχημάτων .....	5
Ακρωνύμια και βραχυγραφίες.....	6
Executive Summary.....	7
Περίληψη .....	9
<b>1 Εισαγωγή.....</b>	<b>12</b>
1.1 Επισκόπηση – κριτική προηγούμενης εργασίας.....	13
1.2 Οριοθέτηση θέματος – στόχοι.....	14
<b>2 Φιλοσοφία εργαλείου .....</b>	<b>17</b>
2.1 Ορισμός εργαλείου .....	17
2.2 Συμπεράσματα .....	18
2.3 Μεθοδολογία εργαλείου.....	19
2.3.1 Πλεονεκτήματα ανάλυσης και διαχείρισης επικινδυνότητας .....	19
2.3.2 Μειονεκτήματα ανάλυσης και διαχείρισης επικινδυνότητας .....	20
2.3.3 Κριτική μεθοδολογιών εργαλείων.....	20
2.3.4 Επίλογή μεθοδολογίας εργαλείου .....	24
<b>3 Συγκέντρωση Υλικού.....</b>	<b>30</b>
3.1 Χαρακτηριστικά εργαλείου προς εξέταση .....	30

<b>3.2 Απαιτήσεις προς εξέταση .....</b>	<b>35</b>
<b>3.2.1 Βασικές λειτουργίες.....</b>	<b>35</b>
<b>3.2.2 Άλλες απαιτήσεις.....</b>	<b>37</b>
<b>3.2.3 Απαιτήσεις από το λογισμικό και το υλικό .....</b>	<b>45</b>
<b>3.2.4 Απαιτήσεις απόδοσης .....</b>	<b>45</b>
<b>3.2.5 Μη λειτουργικές απαιτήσεις – περιορισμοί .....</b>	<b>45</b>
<b>3.2.6 Ειδικές απαιτήσεις – απαιτήσεις ασφάλειας.....</b>	<b>46</b>
<b>3.2.7 Κριτική - Σύνοψη .....</b>	<b>46</b>
<b>3.3 Συμπεράσματα από συνεντεύξεις .....</b>	<b>48</b>
<b>3.3.1 Σχόλια .....</b>	<b>50</b>
<b>4 Ανάλυση Απαιτήσεων .....</b>	<b>53</b>
<b>4.1 Διαγράμματα Ροής Δεδομένων και Λεξικό Δεδομένων .....</b>	<b>53</b>
<b>4.1.1 Διαγράμματα Ροής Δεδομένων .....</b>	<b>53</b>
<b>4.1.2 Λεξικό Δεδομένων.....</b>	<b>56</b>
<b>4.2 Έγγραφο Παραστατικό Απαιτήσεων Λογισμικού .....</b>	<b>58</b>
<b>4.2.1 Λειτουργικές Απαιτήσεις.....</b>	<b>58</b>
<b>4.2.2 Απαιτήσεις Εξωτερικών Διεπαφών.....</b>	<b>60</b>
<b>4.2.3 Απαιτήσεις Επίδοσης.....</b>	<b>74</b>
<b>4.2.4 Περιορισμοί σχεδίασης.....</b>	<b>74</b>
<b>5 Σχεδίαση Εργαλείου.....</b>	<b>75</b>
<b>5.1 Έγγραφο Περιγραφής Σχεδίου Λογισμικού .....</b>	<b>75</b>
<b>5.1.1 Περιγραφή αποσύνθεσης.....</b>	<b>75</b>
<b>Βιβλιογραφία .....</b>	<b>77</b>

## Ευρετήριο Πινάκων

<b>Πίνακας 2-1 :</b> Κατάταξη των μεθόδων βάσει χαρακτηριστικών κατά Baskerville (βλ. [3]) .....	21
<b>Πίνακας 2-2 :</b> Φάσεις και βήματα μεθοδολογίας ανάπτυξης και διαχείρισης ασφάλειας ΠΣ (βλ. [12]) .....	27
<b>Πίνακας 3-1 :</b> Χαρακτηριστικά εργαλείου προς εξέταση .....	32
<b>Πίνακας 3-2 :</b> Το επίπεδο επικινδυνότητας όταν μία αδυναμία τύχει εκμετάλλευσης από απειλή .....	40
<b>Πίνακας 3-3 :</b> Το επίπεδο επικινδυνότητας όταν δεν υπάρχει αδυναμία να τύχει εκμετάλλευσης από απειλή .....	40
<b>Πίνακας 3-4 :</b> Απαιτήσεις εργαλείου προς εξέταση.....	48
<b>Πίνακας 3-5 :</b> Παρουσίαση της σχέσης ανάμεσα σε συνεντευξιαζόμενους και απαιτήσεις .....	50
<b>Πίνακας 4-1 :</b> Λεξικό Δεδομένων .....	58

## Ευρετήριο Σχημάτων

<b>Σχήμα 1-1 :</b> Σχέση δύο εργασιών .....	15
<b>Σχήμα 2-1 :</b> Φάσεις εικονικής μεθοδολογίας (βλ. [5]) .....	24
<b>Σχήμα 2-2 :</b> Μεθοδολογία ανάπτυξης και διαχείρισης ασφάλειας ΠΣ (βλ. [12]).....	26
<b>Σχήμα 4-1 :</b> Διάγραμμα Πλαίσιο.....	53
<b>Σχήμα 4-2 :</b> Διάγραμμα μηδέν .....	54
<b>Σχήμα 4-3 :</b> Υπολόγισε αξία αγαθών 1.0 .....	54
<b>Σχήμα 4-4 :</b> Αποτίμησε βαθμό επικινδυνότητας 2.0 .....	55
<b>Σχήμα 4-5 :</b> Δημιούργησε σχέδιο ασφάλειας 3.0.....	56
<b>Σχήμα 5-1 :</b> Διάγραμμα Δομής .....	76
<b>Σχήμα 5-2 :</b> Διάγραμμα Δομής συνέχεια.....	76

## Ακρωνύμια και βραχυγραφίες

CCTA	Central Computer and Communications Agency
E-R	Entity Relationship
IEEE	Institute of Electrical and Electronics Engineers
SSM	Soft Systems Methodology
Std	Standard
S/W	Software
άρθ.	άρθρο
βλ.	βλέπε
ΔΡΔ	Διάγραμμα Ροής Δεδομένων
ΕΠΑΛ	Έγγραφο Περιγραφής Απαιτήσεων Λογισμικού
ΕΠΣΛ	Έγγραφο Περιγραφής Σχεδίου Λογισμικού
κεφ.	Κεφάλαιο, υποκεφάλαιο ή ενότητα
κοκ	και ούτω καθεξής
κτλ	και τα λοιπά
ν.	Νόμος
οδ.	Οδηγία
παρ.	Παράγραφος
ΠΣ	Πληροφοριακό Σύστημα
πχ	παραδείγματος χάριν
σελ.	σελίδα
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών



## Executive Summary

Risk is associated with the actions we take. CCTA defines risk as the potential for unwanted consequences ([13]). So the development of a secure IS presupposes the limitation of its risk.

Risk Analysis and Management is a popular solution used for discovering the vulnerabilities of a system and preventing the unwanted consequences. In spite of the plethora of Risk analysis and Management methods and tools...

- ...there is no generally acceptable set of criteria that each IS must fulfil in order to regard it as secure.
- ...there is no generally acceptable set of evaluation criteria for the existing tools and methods and to make things worse, many characteristics of them are not publicly available due to the policy of the S/W houses.
- ...there is no tool available that fits to the particular traits of Greek reality.

The goal of this thesis is to design a tool that supports IS Risk analysis and Management. It is the continuation of the thesis of Elisavet Lagou (student of the previous MSc course) that was titled “Requirement Analysis for the Development of a tool that supports IS Risk Analysis and Management”.

None the less, her thesis was after all a feasibility study concerning this area. So this dissertation will use as a base her meanings, and move forward by finishing the requirement analysis and design (to the maximum achievable degree). In order to carry out the requirement analysis, there must be a philosophy that the tool will follow. This action was not taken in the previous thesis, so it is considered as a must.

The *first* and *introductory chapter* contains a critique about the previous thesis and limits this dissertation and its relevant actions. After all, the design of the tool is not completed due to the fact of the missing parts of the previous thesis. Every action will use as a basis the meanings of the previous thesis with every necessary alteration.

*Chapter 2* is concerned with the philosophy this tool follows. First, the tool is defined and the conclusions drawn from it are fully detailed. Second, a methodology that the tool will follow is chosen. The chosen one combines three approaches : (a) the Soft Systems Methodology – Paradigm II, (b) the business modeling and (c) the Risk Analysis – Paradigm I.

*Chapter 3* deals with the material needed for the requirement analysis. Two tables from the previous thesis are used as a reference (pp 6-85, 6-113) and altered in order to match with the philosophy of the tool. Some requirements have omitted (eg a formal method), some have remained as they were (eg special requirements) and others have altered radically (eg steps of the tool).

The requirement analysis is presented in the *4<sup>th</sup> chapter* by using the S/W life cycle model of IEEE. This model was chosen because is used widely and represents the structural approach. As it has already been said, this tool will be produced through many phases (the previous thesis was the first phase, the present one is the second etc), so the “divide and rule” practice that represents this approach is applied fully. The analysis is presented by following the IEEE Guide to S/W Requirements Specifications. Data Flow Diagrams and dictionaries are used and the analysis covers each type of requirement (functional requirements, external interfaces requirements, design limitations).

The first steps of design are presented in the *5<sup>th</sup> chapter*. The design is presented by following the IEEE Recommended Practice for S/W Design Descriptions. In order to depict the decomposition of the S/W System, Data Structures are used.



## Περίληψη

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 ([13]). Έτσι, η δημιουργία ενός ασφαλούς ΠΣ προϋποθέτει την μείωση της επικινδυνότητας αυτού.

Η ανάλυση και διαχείριση επικινδυνότητας αποτελεί μία δημοφιλής λύση για την ανακάλυψη των ευπαθειών ενός συστήματος και την πρόληψη των αρνητικών γεγονότων. Παρόλη, όμως, την πληθώρα εργαλείων και μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ... :

- ...δεν υπάρχει ένα κοινά αποδεκτό σύνολο κριτηρίων που τα ΠΣ πρέπει να πληρούν ώστε να θεωρούνται ασφαλή.
- ...δεν υπάρχει ένα αποδεκτό σύνολο κριτηρίων που τα εργαλεία ασφάλειας ΠΣ και ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ θα πρέπει να πληρούν, και επιπλέον αποκρύπτονται πληροφορίες για πολλά από τα εργαλεία αυτά λόγω της πολιτικής που ακολουθούν οι εταιρείας κατασκευής των εργαλείων αυτών.
- ...δεν υπάρχει ένα εργαλείο που να είναι προσαρμοσμένο στα ελληνικά δεδομένα.

Σκοπός της παρούσας εργασίας είναι η σχεδίαση ενός εργαλείου υποστήριξης της ανάλυσης και διαχείρισης επικινδυνότητας Πληροφοριακών Συστημάτων προσαρμοσμένο στα ελληνικά δεδομένα. Η παρούσα εργασία, αποτελεί τη συνέχεια της διατριβής της Ελισάβετ Λαγού (φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών στα Πληροφοριακά Συστήματα του προηγουμένου Ακαδημαϊκού Έτους). Η εργασία της τιτλοφορούταν «Ανάλυση Απαιτήσεων για Ανάπτυξη Εργαλείου Υποστήριξης της Ανάλυσης και Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων». Έτσι, η παρούσα εργασία χρησιμοποιεί το εννοιολογικό υπόβαθρο της

Όπως και η ίδια προαναφέρει, η εργασία της τελικά αποτελεί «μία διερευνητική μελέτη στα πλαίσια της ανάλυσης απαιτήσεων για την ανάπτυξη μιας εφαρμογής υποστήριξης της Ανάλυσης και Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων». Έτσι, η παρούσα εργασία χρησιμοποιεί το εννοιολογικό υπόβαθρο της

προηγούμενης διπλωματικής και προχωρά στην ολοκλήρωση της ανάλυσης απαιτήσεων και στην σχεδίαση του εργαλείου (στο μέγιστο δυνατό σημείο). Προτού, όμως, πραγματοποιηθεί η ανάλυση αναγκαία κρίνεται η επιλογή της φιλοσοφίας που το εργαλείο αυτό πρέπει να ακολουθεί και δεν είχε πραγματοποιηθεί τέτοια μελέτη στην προηγούμενη εργασία.

Έτσι, η παρούσα διπλωματική εργασία περιλαμβάνει στο πρώτο και εισαγωγικό κεφάλαιο μία κριτική της προηγούμενης εργασίας και μία οριοθέτηση του θέματος της παρούσας και των ενεργειών που θα πραγματοποιηθούν μέσα σε αυτό το πλαίσιο. Όπως προαναφέρθηκε, η σχεδίαση στην ουσία δεν ολοκληρώνεται, καθότι υπολείπονται ενέργειες σχετικές με την φιλοσοφία του εργαλείου και την ανάλυση απαιτήσεων αυτού. Για τις ενέργειες αυτές θα χρησιμοποιηθεί το εννοιολογικό υπόβαθρο της Λαγού και αυτό θα τροποποιείται όπου κρίνεται σκόπιμο.

Στο 2<sup>ο</sup> κεφάλαιο αναλύεται η φιλοσοφία που το εργαλείο αυτό 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 μία 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 : (α) της Μεθοδολογίας Ευμετάβλητων Συστημάτων (SSM) που ακολουθεί το Paradigm II, (β) της μοντελοποίησης οργανισμών και επιχειρήσεων (business modeling) και (γ) της ανάλυσης επικινδυνότητας που ακολουθεί το Paradigm I.

Το 3<sup>ο</sup> κεφάλαιο σχετίζεται με τη συλλογή του υλικού για την πραγματοποίηση της ανάλυσης απαιτήσεων. Στο υλικό αυτό χρησιμοποιούνται ως βάση τα στοιχεία που συνέλεξε η Λαγού, και αυτά εμπλουτίζονται ή και αναθεωρούνται μέσα από τις συνεντεύξεις που πάρθηκαν και από τα συμπεράσματα που αντλήθηκαν από τη φιλοσοφία που ακολουθεί το εργαλείο. Από την εργασία της Λαγού χρησιμοποιήθηκαν οι πίνακες στις σελίδες 6-85 και 6-113, οι οποίοι τροποποιήθηκαν για να εναρμονιστεί το περιεχόμενο αυτών με την φιλοσοφία του εργαλείου. Έτσι, κάποιες απαιτήσεις προς εξέταση παραλήφθηκαν (πχ η ύπαρξη αυστηρής μεθόδου),

κάποιες παρέμειναν όπως είχαν (πχ οι ειδικές απαιτήσεις) ενώ άλλες τροποποιήθηκαν ριζικά (πχ οι φάσεις – βήματα του εργαλείου).

Στο 4<sup>ο</sup> κεφάλαιο πραγματοποιείται η ανάλυση απαιτήσεων. Για την υλοποίηση της χρησιμοποιήθηκε το μοντέλου του κύκλου ζωής λογισμικού του IEEE. Η επιλογή αυτού του μοντέλου έχει να κάνει με το γεγονός ότι χρησιμοποιείται ευρέως και αντιτροσωπεύει τη δομημένη προσέγγιση. Όπως έχει προαναφερθεί, το εργαλείο αυτό πρόκειται να παραχθεί σε διάφορα στάδια (με πρώτο στάδιο την προηγούμενη διπλωματική εργασία και δεύτερο την παρούσα κοκ), 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 ΕΠΙΑΛ. Μέσα στο έγγραφο αυτό περιγράφονται οι λειτουργικές απαιτήσεις, οι απαιτήσεις εξωτερικών διεπαφών, οι απαιτήσεις επίδοσης και οι περιορισμοί σχεδίασης.

Το 5<sup>ο</sup> κεφάλαιο αποτελεί το πρώτο βήμα για την υλοποίηση της σχεδίασης. Αυτή θα πραγματοποιηθεί ακολουθώντας τις οδηγίες για τη σύνταξη ενός ΕΠΙΑΛ. 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 τα Διαγράμματα Δομής που παρουσιάζουν την ιεραρχία των μονάδων του συστήματος.

## 1 Εισαγωγή

Στις μέρες μας, οι παραβιάσεις ασφάλειας αποτελούν καθημερινό φαινόμενο. Ιστοσελίδες παραβιάζονται, προσωπικά δεδομένα υποκλέπτονται, συστήματα τίθενται εκτός λειτουργίας προκαλώντας αναστάτωση και ζημίες. Τα αποτελέσματα ερευνών σχετικών με την ασφάλεια είναι ανησυχητικά.

Η 6<sup>η</sup> Ετήσια Παγκόσμια Έρευνα Ασφάλειας Πληροφοριών (6<sup>th</sup> Annual Information Security Survey – Ernst & Young, 1998) που πραγματοποιήθηκε σε 35 χώρες και 4312 επιχειρήσεις κατέληξε στο 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 ΠΣ) σημαντική, το 41% αυτών δεν διαθέτουν τεκμηριωμένη πολιτική και διαδικασίες ασφάλειας.

Κυριότερη αιτία της μη επαρκούς αντιμετώπισης των ζητημάτων ασφάλειας 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.

Η ανάλυση και διαχείριση επικινδυνότητας αποτελεί μία δημοφιλής λύση για την ανακάλυψη των ευπαθειών ενός συστήματος και την πρόληψη των αρνητικών γεγονότων. Παρόλη, όμως, την πληθώρα εργαλείων και μεθόδων ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ...

- ...δεν υπάρχει ένα κοινά αποδεκτό σύνολο κριτηρίων που τα ΠΣ πρέπει να πληρούν ώστε να θεωρούνται ασφαλή.
- ...δεν υπάρχει ένα αποδεκτό σύνολο κριτηρίων που τα εργαλεία ασφάλειας ΠΣ και ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ θα πρέπει να πληρούν, και επιπλέον αποκρύπτονται πληροφορίες για πολλά από τα εργαλεία αυτά λόγω της πολιτικής που ακολουθούν οι εταιρείας κατασκευής των εργαλείων αυτών.
- δεν υπάρχει ένα εργαλείο που να είναι προσαρμοσμένο στα ελληνικά δεδομένα.

Έτσι, κρίνεται σκόπιμη η δημιουργία ενός εργαλείου για την υποστήριξη της ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ προσαρμοσμένο στον ελληνικό χώρο και αυτό είναι το έργο της παρούσας διατριβής. Η παρούσα εργασία, όπως προαναφέρθηκε, αποτελεί συνέχεια της διατριβής της Ελισάβετ Λαγού (φοιτήτρια του Προγράμματος Μεταπτυχιακών Σπουδών στα Πληροφοριακά Συστήματα του προηγουμένου Ακαδημαϊκού Έτους). Η εργασία της τιτλοφορούταν «Ανάλυση Απαιτήσεων για Ανάπτυξη Εργαλείου Υποστήριξης της Ανάλυσης και Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων» ([13], σελ. 1-16). Έτσι, η παρούσα διατριβή δεν θα μπορούσε να αναπτυχθεί χωρίς την προηγούμενη κριτική και αναθεώρηση της προαναφερόμενης εργασίας. Στις επόμενες σελίδες ακολουθεί η κριτική αυτή και οριοθετείται το θέμα της παρούσας διατριβής.

## 1.1 Επισκόπηση – κριτική προηγούμενης εργασίας

Η προηγούμενη διατριβή, η οποία κατέληξε σε μία διερευνητική μελέτη, αναλώνεται σε παράθεση αποσπασμάτων επιστημονικών άρθρων και βιβλίων, σχετικών με την ανάλυση και διαχείριση επικινδυνότητας. Η εννοιολογική αυτή παράθεση είναι ευπρόσδεκτη ως προς το γεγονός ότι κατέγραψε όλες τις σχετικές έννοιες και αναφορές γύρω από το θέμα της ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ. Παρόλα αυτά, ένας εξοικειωμένος με τη θεματολογία αυτή θα μπορούσε να προχωρήσει στην ανάγνωση του ουσιαστικού μέρους της διατριβής ([13], σελ. 5-73 έως 6-118), και να επιστρέψει στο πρώτο μέρος, όποτε αυτό είναι απαραίτητο, για την εξέταση του εννοιολογικού υπόβαθρου, στο οποίο στηρίχθηκε η εργασία.

Στις προαναφερόμενες σελίδες, πραγματοποιείται μία έρευνα σχετικά με τις απαιτήσεις που ένα εργαλείο θα έπρεπε να έχει. Η συλλογή των απαιτήσεων πραγματοποιήθηκε μέσω συνεντεύξεων με έμπειρα, στο χώρο της ασφάλειας, άτομα και ακολουθεί μία αναφορά σχετικά με κάθε απαίτηση που παρατίθεται. Όλες οι απαιτήσεις καταγράφονται σε δύο πίνακες ([13], Πίνακας 5.6-1 σελ. 6-85 και

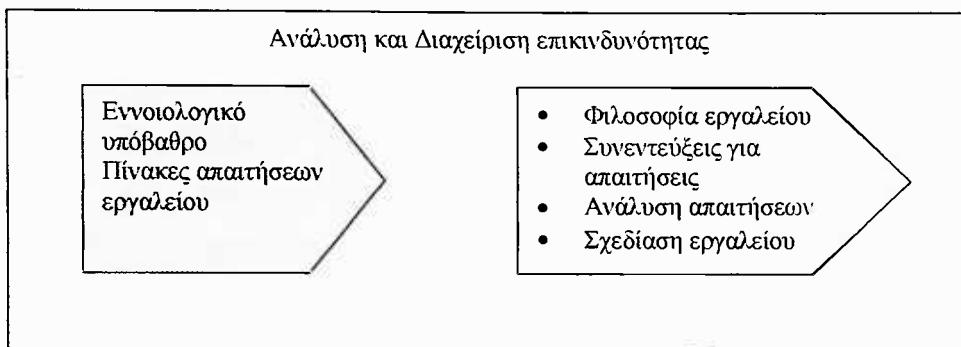
Πίνακας 6.7-2 σελ. 6-113) που αποτελούν και το εφαλτήριο έναρξης της παρούσας διατριβής.

Έτσι, η εργασία της Λαγού Ελισάβετ κρίνεται αναγκαία για το εννοιολογικό πλαίσιο που παρατίθεται (και δεν κρίνεται σκόπιμο να επαναληφθεί) αλλά και θετική για τους προαναφερόμενους πίνακες, οι οποίοι θα τύχουν περαιτέρω επεξεργασίας. Ο ενδιαφερόμενος μπορεί να ανατρέχει για παραδοχές σε εννοιολογικό επίπεδο στην εργασία αυτή. Ο, τιδήποτε θεωρείται διαφορετικό θα επεξηγείται στην παρούσα εργασία. Η επόμενη ενότητα οριοθετεί το θέμα της παρούσας διατριβής και τη σχέση της ή αλληλεξάρτησή της με την προαναφερόμενη.

## 1.2 Οριοθέτηση θέματος – στόχοι

Το θέμα της παρούσας διατριβής είναι η σχεδίαση ενός εργαλείου υποστήριξης της ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ. Το εργαλείο αυτό θα τύχει χρήσης στον ελλαδικό χώρο, έτσι οι απαιτήσεις, όπως προαναφέρθηκε στην αρχή του κεφαλαίου αυτού, πρέπει να λαμβάνουν υπόψη τις ιδιαιτερότητες του χώρου αυτού. Όμως, η ανάλυση των απαιτήσεων αυτών δεν έχει ολοκληρωθεί στην προηγούμενη εργασία.

Όπως αναφέρει και ο Κιουντούζης ([11], κεφ. 10), ο σχεδιασμός ενός συστήματος προαπαιτεί την ανάλυση των απαιτήσεων αυτών. Έτσι, στην παρούσα διατριβή θα ολοκληρωθεί η ανάλυση για να εισέλθουμε στη φάση της σχεδίασης. Όπως, προαναφέρθηκε, το εννοιολογικό υπόβαθρο της εργασίας της Λαγού δεν τροποποιείται, αλλά θα επεκταθεί ανάλογα στα σχετικά σημεία. Το παρακάτω σχήμα απεικονίζει τον τρόπο αλληλοσυσχέτισης των δύο εργασιών και την αλληλουχία των ενεργειών.



Σχήμα 1-1 : Σχέση δύο εργασιών

Προτού, όμως ξεκινήσει η ανάλυση απαιτήσεων, απαραίτητη κρίνεται η φιλοσοφία που το εργαλείο θα ακολουθεί. Δηλαδή, ποια θα είναι η χρήση του και ποια μεθοδολογία θα ακολουθεί. Έτσι, θα προηγηθεί ο ορισμός του εργαλείου αυτού, θα ακολουθήσει η ανάλυση των απαιτήσεων και θα επιτευχθεί, κατά το μέγιστο δυνατό σημείο, η σχεδίαση.

Όπως έχει αναφερθεί και στην εργασία της Λαγού ([13], κεφ. 5.5), το εργαλείο αυτό αποτελεί ένα πακέτο λογισμικού. Έτσι, τόσο οι απαιτήσεις του, όσο και η σχεδίασή του πρέπει να πραγματοποιηθούν με κάποιο από τα μοντέλα ανάπτυξης λογισμικού ακολουθώντας τη δομημένη προσέγγιση. Βάσει αυτών, τόσο η ανάλυση απαιτήσεων, όσο και η σχεδίαση του εργαλείου θα πραγματοποιηθούν κάνοντας χρήση του μοντέλου του κύκλου ζωής λογισμικού του IEEE που αποτελεί παραλλαγή του μοντέλου του καταρράκτη.

Το μοντέλο του καταρράκτη αποτελεί μία δομημένη προσέγγιση (δημιουργία σειριακών φάσεων για εκτέλεση ενός έργου), χωρίζοντας τον κύκλο ζωής λογισμικού σε επιμέρους φάσεις. Η μία φάση προϋποθέτει «πάγωμα» της προηγούμενης, όπως ακριβώς παρατηρείται και στην εργασία αυτή. Ξεκινάμε με παγίωση των προηγούμενων συμπερασμάτων (προηγούμενη διπλωματική εργασία) και προχωράμε με τις νέες ενέργειες όπως υπονοεί και το προαναφερόμενο σχήμα.

Η επιλογή του οφείλεται στο γεγονός ότι χρησιμοποιείται ευρέως, είναι κοινά αποδεκτό και βοηθά τον επόμενο ερευνητή να συνεχίσει την εργασία αυτή. Όπως έχει προαναφερθεί το εργαλείο αυτό πρόκειται να παραχθεί σε διάφορα στάδια, έτσι η πρακτική του «διαιρεί και βασίλευε» με τον τεμαχισμό των εργασιών που αποτελεί κύριο χαρακτηριστικό της δομημένης προσέγγισης, μπορεί μέσω του μοντέλου αυτού να εφαρμοστεί πλήρως.

Βάσει του Σχήματος 1-1 οι εργασίες κινούνται στο χώρο της ανάλυσης και διαχείρισης επικινδυνότητας και η παρούσα εργασία για την επίτευξη των στόχων της (Φιλοσοφία, Συνεντεύξεις, Ανάλυση, Σχεδίαση) κάνει χρήση του εννοιολογικού υποβάθρου και των πινάκων της προηγούμενης διατριβής όπως αυτά προαναφέρθηκαν στην προηγούμενη ενότητα.

## 2 Φιλοσοφία εργαλείου

Όπως αναφέρει ο Κιουντούζης, ([11], σελ. 83) ένα εργαλείο βοηθά στην υλοποίηση μίας μεθοδολογίας, της οποίας τη φιλοσοφία ακολουθεί. Πέρα από τη 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 εργαλείου

Το εργαλείο αυτό, όπως αναφέρεται και στον τίτλο, *υποστηρίζει* την ανάλυση και διαχείριση επικινδυνότητας ΠΣ. 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 ΠΣ εξυπηρετεί κάποιον οργανισμό ([11], σελ. 29, 169) 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 που θα υποστηρίζει την ανάλυση και διαχείριση επικινδυνότητας ΠΣ (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 επικινδυνότητας του ΠΣ προς εξέταση και διαχειρίζεται την επικινδυνότητα προτείνοντας στον οργανισμό (του ελλαδικού χώρου), του οποίου το ΠΣ εξετάζεται, αντίμετρα τα οποία προήλθαν από το εργαλείο και φιλτραρίστηκαν από τον αναλυτή.

Από τον ορισμό αυτό 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 πανεπιστήμιο (μέσω της σχετικής επιστημονικής ομάδας) θα το χρησιμοποιεί αναλαμβάνοντας την εκπόνηση σχετικών έργων. Επίσης, το εργαλείο θα χρησιμοποιείται και από συμβουλευτικές εταιρείες (consultant houses) για πραγματοποίηση της ανάλυσης σε εταιρείες / πελάτες αυτών.
- Ο αναλυτής που θα χρησιμοποιήσει το εργαλείο αυτό πρέπει να είναι γνώστης θεμάτων σχετικών με την ασφάλεια. Δηλαδή, πρέπει να έχει εμπειρία σχετική με ανάλυση ΠΣ, ανάλυση επικινδυνότητας αλλά και με τεχνικά θέματα και θέματα διαχείρισης έργων Πληροφορικής. Οι συμβουλευτικοί 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 ελλαδικό χώρο, οπότε πρέπει να λαμβάνεται υπόψη η ιδιαιτερότητά του Έλληνα (ιδίως η κουλτούρα του). Επίσης, πρέπει η σχετική νομοθεσία να εφαρμόζεται (v. 2472/1997 άρθ. 10 παρ. 3 και οδ. 95/46/ΕC άρθ. 17 παρ. 2) ενώ οι οιθόνες, τα ερωτηματολόγια, οι εκθέσεις (reports) και γενικά κάθε διεπαφή του πρέπει να είναι στην ελληνική γλώσσα.
- Η χρηματική αξία των επιπτώσεων και αντιμέτρων πρέπει να εκφράζεται σε δραχμές και σε EURO.

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 το χρήστη. Βέβαια, δεν πρέπει το εργαλείο αυτό να είναι «στρυφνό» και δύσκολο στη χρήση του, αλλά δεν τίθεται ανάγκης να προσφέρει λεπτομερέστατη βοήθεια.
- Το εργαλείο υποστηρίζει τη διαχείριση επικινδυνότητας μέχρι του βαθμού πρότασης των κατάλληλων και αποδεκτών, από τη διοίκηση του προς εξέταση οργανισμού, αντιμέτρων. Δε 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 όποια ανάλυση και σχέδιο ασφάλειας 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, όμως, από τα συμπεράσματα αυτά πρέπει να επισημανθεί ότι κάθε εργαλείο ακολουθεί – υλοποιεί κάποια μεθοδολογία. Στην επόμενη ενότητα περιγράφεται η μεθοδολογία που το εργαλείο αυτό θα υλοποιεί.

## 2.3 Μεθοδολογία εργαλείου

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

### 2.3.1 Πλεονεκτήματα ανάλυσης και διαχείρισης επικινδυνότητας

Όπως αναφέρει και ο Baskerville ([2], βλ. και [12]), η ανάλυση και διαχείριση 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 ασφάλειας.

Πέρα, όμως, από εργαλείο επικοινωνίας, έρχεται και σε σύμπνοια με τις απαιτήσεις της ελληνικής και ευρωπαϊκής νομοθεσίας (ν. 2472/1997 άρθ. 10 παρ. 3 και οδ. 95/46/ΕC άρθ. 17 παρ. 2). Σύμφωνα με το νόμο και την οδηγία αυτή, τα ΠΣ τα οποία επεξεργάζονται προσωπικά δεδομένα, απαιτούνται να λαμβάνουν μέτρα προστασίας, έτσι ώστε «να εξασφαλίζεται επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων» (νόμος της αναλογικότητας).

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

### 2.3.2 Μειονεκτήματα ανάλυσης και διαχείρισης επικινδυνότητας

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

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

Επίσης, οι στατιστικές μέθοδοι που χρησιμοποιούνται έχουν τύχει αρνητικής κριτικής από διάφορους ερευνητές για την απλότητά τους ([2]). Όλα, όμως, τα πλεονεκτήματα και μειονεκτήματα που παρουσιάζουν τα εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας οφείλονται στις μεθοδολογίες που ακολουθούν.

### 2.3.3 Κριτική μεθοδολογιών εργαλείων

Όπως αναφέρει ο Baskerville σε άλλη επιστημονική του αναφορά ([3]), οι μέθοδοι Ασφάλειας Πληροφοριακών Συστημάτων (στις οποίες εντάσσεται η ανάλυση και διαχείρισης επικινδυνότητας που τα εργαλεία υλοποιούν) μπορούν να χωριστούν σε

τρεις γενέας (βλ. Πίνακας 2-1). 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, δηλ. άλλες δεν είναι μεθοδολογίες, ενώ αυτές που θεωρούνται ως τέτοιες δεν ακολουθούν πλήρως τον προαναφερόμενο ορισμό (βλ. [11] και [13]).

Γενέτες μεθόδων	Πρωταρχικά στοιχεία	Μέθοδοι	Μέθοδοι	Σκοπός	Μέσα	Πρόκληση	Διαλογικές Υποθέσεις	Εργασίες
		Ανάπτυξης Συστήματος & Τυπικά	Ανάπτυξης Ασφάλειας & Τυπικά					
		Εργαλεία	Εργαλεία					
Μέθοδοι checklist	Απεικόνιση των περιορισμένων λύσεων	Τεχνικές λύσεις και διαδικασίες του προμηθευτή	Checklist Ασφάλειας και ανάλυση επικινδυνότητας	Επιλογή συστατικών στοιχείων	Έρευνα διαθεσίμων στοιχείων	Απεικόνιση της λύσης στο πρόβλημα	Καθολικές λύσεις	Krauss 1972 Hoyt 1973 Courtney 1977 Browne 1979
Τεχνολογικές μηχανιστικές μεθόδοι	Κατανεμημένη και πολύτιλη λύση αντίστοιχη των λειτουργικών απαιτήσεων	Top-down engineering, rapid prototyping, system & logic flowcharts	CRAMM, BDSS, πίνακες ανάλυσης έκθεσης και σημείων ελέγχων, ερωτηματολόγια H/Y	Καταμερισμός της λύσης	Επίλυση κάθε λειτουργικής απαίτησης	Οργάνωση και ολοκλήρωση ενός σύνθετου συνόλου στοιχείων	Ιδανικές παραμετροποιημένες λύσεις	Parker 1981 Fisher 1984
Μέθοδοι λογικού πεποιηματού	Υψηλός σε αφαιρετικό επίπεδο σχεδιασμός και έκφρασης του προβλήματος και του χώρου επίλυσης	Δομημένη ανάλυση, μοντελοποίηση δεδομένων, τεχνολογία πληροφοριών, διαγράμματα οντοτήτων συσχετίσεων & ρόης 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 μοντέλο	Baskerville 1988

Πίνακας 2-1 : Κατάταξη των μεθόδων βάσει χαρακτηριστικών κατά Baskerville (βλ. [3])

Οι μεθοδολογίες της τρίτης γενεάς είναι οι πρόσφατες και σ' αυτές μπορούν να προστεθούν και το «Πλαίσιο μεθοδολογίας για τον κύκλο ζωής της ασφάλειας υπολογιστών σε οργανισμό» (βλ. [1]), το «Πλαίσιο IBAg για ασφάλεια τεχνολογιών πληροφορίας σε εμπορικό κλάδο» (βλ. [6]) και η «Μεθοδολογία ανάπτυξης ασφαλών συστημάτων εφαρμογών (application systems)» (βλ. [4]). Οι μεθοδολογίες αυτές,

όπως και της δεύτερης γενεάς, ακολουθούν μία μηχανιστική αντίληψη, με εκτέλεση προκαθορισμένων βημάτων. Τα βήματα αυτά θα μπορούσαν χαρακτηριστικά να περιγραφούν ως εξής :

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

Οι προαναφερθείσες μεθοδολογίες ακολουθούν μία κοινή αντίληψη, παράδειγμα (Paradigm) όπως χαρακτηριστικά αναφέρει ο Kuhn. Κατά τον 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 (βλ. [11], σελ. 48, 146-150). Έτσι, οι παραπάνω μεθοδολογίες στηρίζονται στο **Παράδειγμα I** ακολουθούν, δηλαδή, τις εξής παραδοχές :

- Η πραγματικότητα, όπως την αντιλαμβανόμαστε, είναι **συστημική**, δηλαδή αποτελείται από συστήματα,
- Η μεθοδολογία που χρησιμοποιούμε για να τη διερευνήσουμε είναι **συστηματική**.

Δηλαδή, υπάρχει μία αυστηρή διατύπωση με μία συγκεκριμένη σειρά βημάτων, ενώ περιορίζονται 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 «αντικειμενοποιώντας» την υποκειμενικότητα (μέσω της χρήσης της στατιστικής) που είναι ορατή αφού οι αποτιμήσεις των απειλών και αγαθών στηρίζονται στην εμπειρία και μόνο του αναλυτή.



Ακόμα, παραλείπεται ο ανθρώπινος παράγοντας, είτε θεωρείται ως τεχνικό και μόνο ζήτημα με προβλεπόμενη συμπεριφορά. Ακόμα και το μοντέλο του πίνακα του McCumber (βλ. [9]), 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 δυνατό να προβλεφθεί, πόσο μάλλον να ποσοτικοποιηθεί, η ανθρώπινη συμπεριφορά, γεγονός που εναντιώνεται με την ποσοτικοποίηση και τη βελτιστοποίηση στις οποίες στηρίζεται η «δύσκαμπτη» αυτή προσέγγιση.

Βέβαια, οι μεθοδολογίες αυτές έχουν και πλεονεκτήματα (βλ. [12]):

- 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 I, αναπτύχθηκε η εικονική μεθοδολογία (virtual methodology) (βλ. [5]) που ακολουθεί το Παράδειγμα II, δηλαδή την «ευμετάβλητη» προσέγγιση. Κατά τον Kuhi, στο Paradigm II επικρατούν οι ακόλουθες παραδοχές :

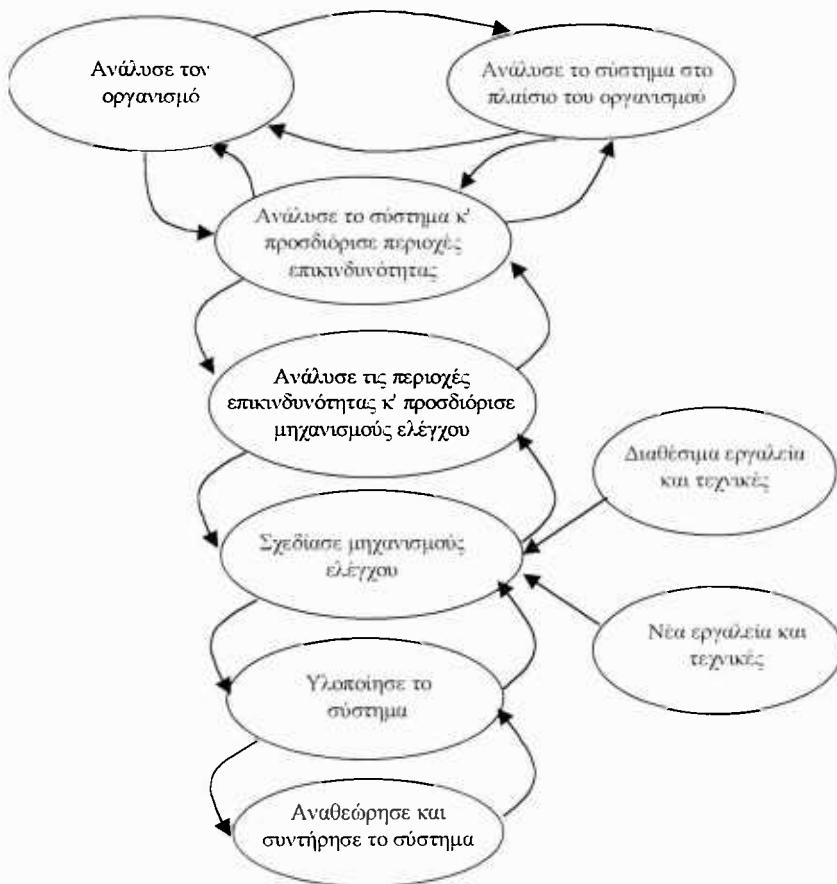
- Η πραγματικότητα, όπως την αντιλαμβανόμαστε, είναι προβληματική,
- Η μεθοδολογία που χρησιμοποιούμε, για τη διερεύνησή της είναι συστηματική.

Η μόνη μεθοδολογία που έχει αναπτυχθεί και ακολουθεί το Paradigm αυτό, είναι της Hitchings (βλ. [5]) η αποκαλούμενη και εικονική μεθοδολογία (virtual methodology). Η Hitchings θεωρεί ότι η μεθοδολογία πρέπει να είναι ένα εργαλείο που θα χρησιμοποιείται σαν καταλόγης 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 ένα εικονικό εργαλείο. Οι φάσεις της εικονικής μεθοδολογίας παρουσιάζονται στο σχήμα 2-1

Στα πλεονεκτήματα της εικονικής μεθοδολογίας περιλαμβάνονται (βλ. [12]) τα εξής :



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



Σχήμα 2-1 : Φάσεις εικονικής μεθοδολογίας (βλ.. [5])

Αντίστοιχα, τα μειονεκτήματά της είναι η αδυναμία αιτιολόγησης του κόστους των αντιμέτρων με όρους κόστους / οφέλους και η έλλειψη συγκεκριμένων μεθόδων και τεχνικών για την υλοποίηση των φάσεων της μεθοδολογίας αυτής έτσι ώστε να ισχυροποιήσουν την εγκυρότητά της. Μέσω της παραπάνω κριτικής – παρουσίασης είμαστε σε θέση να παρουσιάσουμε τη μεθοδολογία που το συγκεκριμένο εργαλείο θα ακολουθεί.

### 2.3.4 Επιλογή μεθοδολογίας εργαλείου

Όπως προαναφέρθηκε, οι μεθοδολογίες που ακολουθούν τα δύο παραδείγματα (paradigms) έχουν ελαττώματα και προτερήματα. Έτσι, κρίνεται σκόπιμη μία

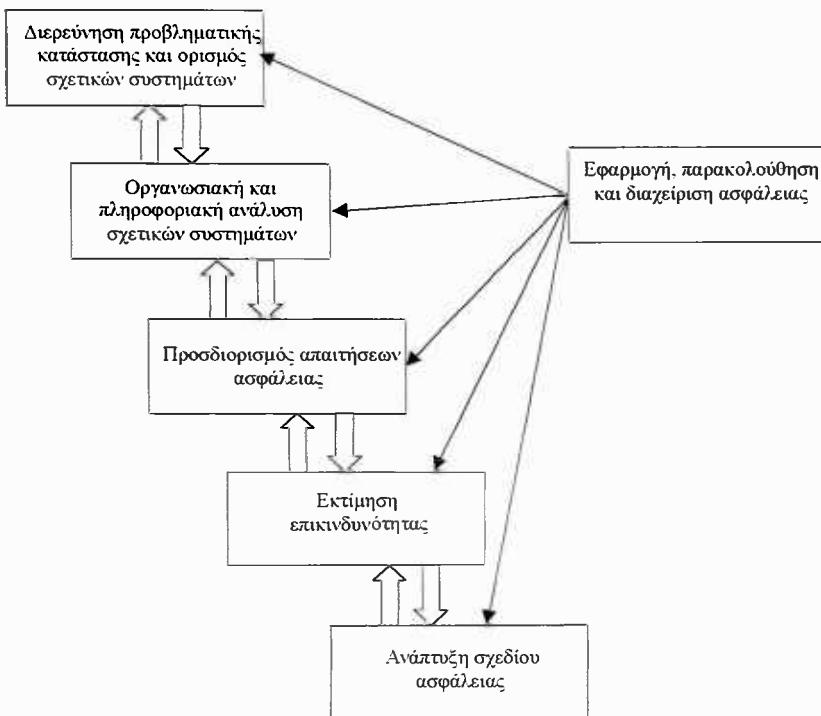
προσπάθεια συνδυασμού των δύο αυτών προσεγγίσεων (συστηματική και συστημική προσέγγιση).

Μία πρώτη νύξη πάνω στο συνδυασμό αυτό, ήταν η επιστημονική δημοσίευση των Κιουντούζη – Κοκολάκη ([7]). Εκεί, αναφέρεται ότι στην ανάπτυξη ενός Πληροφοριακού Συστήματος υπάρχει παλινδρόμηση μεταξύ των δύο αυτών παραδειγμάτων (όπως η πορεία πάνω σε ταινία του Moebius). Οι συγγραφείς θεωρούν ότι ο αναλυτής, για παράδειγμα θα πρέπει πρώτα να εξετάσει το σύστημα outside – in, δηλαδή με όρους εκτός συστήματος (τι βλέπει ο χρήστης), στη συνέχεια όμως θα πρέπει να το εξετάσει inside – out, αφού πρέπει να προσδιορίσει τις ανάγκες των χρηστών.

Στηριζόμενος στην παραδοχή αυτή, ο Δρ Κοκολάκης Σπ δημιούργησε μία σχετική μεθοδολογία στα πλαίσια της διδακτορικής του διατριβής ([12]). «Η μεθοδολογία αυτή συνδυάζει και ολοκληρώνει τρεις δημοφιλείς μεθοδολογικές προσεγγίσεις :

1. *Tη μεθοδολογία των ενμετάβλητων συστημάτων (SSM – Paradigm II),*
2. *Tη μοντελοποίηση οργανισμών και επιχειρήσεων (business modeling) και*
3. *Tην ανάλυση επικινδυνότητας (Paradigm I)).*

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 : Μεθοδολογία ανάπτυξης και διαχείρισης ασφάλειας ΠΣ (βλ.. [12])

Φάση	Βήματα ανά Φάση
<b>Φάση 1.</b> Διερεύνηση προβληματικής κατάστασης και ορισμός σχετικών συστημάτων	<i>Βήμα 1</i> : Κατασκευή και ανάλυση πλούσιας εικόνας (rich picture) <i>Βήμα 2</i> : Καταγραφή και ανάλυση βασικών ορισμών (root definitions) των υπό εξέταση συστημάτων <i>Βήμα 3</i> : Ορισμός ασφάλειας των υπό εξέταση συστημάτων <i>Βήμα 4</i> : Υιοθέτηση ενός βασικού ορισμού και ενός ορισμού ασφάλειας για τα υπό εξέταση συστήματα <i>Βήμα 5</i> : Συγκρότηση ομάδων εργασίας <i>Βήμα 6</i> : Κατάρτιση του πλάνου του έργου
<b>Φάση 2.</b> Οργανωσιακή και πληροφοριακή ανάλυση σχετικών συστημάτων	<i>Βήμα 1</i> : Ανάπτυξη οργανωσιακών / επιχειρησιακών μοντέλων <i>Βήμα 2</i> : Ανάπτυξη ερμηνευτικών πληροφοριακών μοντέλων
<b>Φάση 3.</b> Προσδιορισμός απαιτήσεων ασφάλειας	<i>Βήμα 1</i> : Προσδιορισμός κύριων αγαθών (assets) και ορισμός χαρακτηριστικών ιδιοτήτων ασφάλειας <i>Βήμα 2</i> : Ανάλυση επιπτώσεων στον οργανισμό <i>Βήμα 3</i> : Αποτίμηση κύριων αγαθών <i>Βήμα 4</i> : Προσδιορισμός απαιτήσεων ασφάλειας υποστηρικτικών πόρων <i>Βήμα 5</i> : Επικύρωση
<b>Φάση 4.</b> Εκτίμηση επικινδυνότητας	<i>Βήμα 1</i> : Εντοπισμός και αποτίμηση απειλών <i>Βήμα 2</i> : Εντοπισμός και αποτίμηση αδυναμιών <i>Βήμα 3</i> : Εκτίμηση βαθμού επικινδυνότητας <i>Βήμα 4</i> : Προσδιορισμός προτεραιοτήτων <i>Βήμα 5</i> : Επικύρωση
<b>Φάση 5.</b> Ανάπτυξη σχεδίου ασφάλειας	<i>Βήμα 1</i> : Προσδιορισμός ρόλων και υπευθυνοτήτων <i>Βήμα 2</i> : Ανάπτυξη πολιτικής ασφάλειας <i>Βήμα 3</i> : Επιλογή μέτρων προστασίας <i>Βήμα 4</i> : Ανάπτυξη στρατηγικού σχεδίου εφαρμογής και συνεχούς διαχείρισης επικινδυνότητας
<b>Φάση 6.</b> Εφαρμογή, παρακολούθηση και διαχείριση ασφάλειας	<i>Βήμα 1</i> : Επικύρωση / αποδοχή σχεδίου ασφάλειας <i>Βήμα 2</i> : Εφαρμογή σχεδίου ασφάλειας <i>Βήμα 3</i> : Συνεχής παρακολούθηση και διαχείριση ασφάλειας <i>Βήμα 4</i> : Έλεγχος / επανεκτίμηση / αναθεώρηση

Πίνακας 2-2 : Φάσεις και βήματα μεθοδολογίας ανάπτυξης και διαχείρισης ασφάλειας ΠΣ (βλ. [12])

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 που αναφέρθηκε στην ενότητα 2.1 ενδιαφερόμαστε για τον οργανισμό και την κουλτούρα του.

Η επόμενη φάση μας δίνει τη δυνατότητα να μπορέσουμε να δούμε τον οργανισμό και το Πληροφοριακό Σύστημα δυναμικά. Δεν πρέπει να λησμονείται το γεγονός ότι η πληροφορία είναι μία 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 οργανωσιακών / επιχειρησιακών μοντέλων βοηθά στην αναγνώριση των σημαντικότερων / κρίσιμων διαδικασιών (processes) και στην αναδιοργάνωση αυτών, λόγω υλοποίησης των προτεινόμενων αντιμέτρων, της διαχείρισης επικινδυνότητας και της ανατροφοδότησης (feedback) που επιθυμούμε.

Τα αποτελέσματα της 3<sup>ης</sup> και της 4<sup>ης</sup> φάσης συνδυάζονται με παραγόμενο αποτέλεσμα την αποτίμηση του βαθμού επικινδυνότητας. Τα αποτελέσματα των φάσεων αυτών εξαρτώνται από τα προϊόντα των προηγούμενων φάσεων, ιδιαίτερως 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 επικινδυνότητας. Τόσο η πολιτική ασφάλειας, όσο και τα αντίμετρα (προϊόντα πέμπτης φάσης) εντάσσονται στις ενέργειες της διαχείρισης επικινδυνότητας. Επίσης, η εφαρμογή του σχεδίου ασφάλειας 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 επικινδυνότητας αποτελούν το μέσο επικοινωνίας μεταξύ αναλυτή και



διοίκησης. Άλλο πλεονέκτημα χρήσης της μεθοδολογίας αυτής είναι η προσπάθεια της να συγκεράσει διαφορετικά παραδείγματα.

Δεν πρέπει επίσης να λησμονούμε τον ορισμό (βλ. κεφ. 2.1) για το συγκεκριμένο εργαλείο. Όπως υπαινίσσεται και αναφέρει και η Λαγού στην προηγούμενη διπλωματική εργασία, δεν πρέπει η κουλτούρα και το πλαίσιο του οργανισμού στον οποίο εντάσσεται το υπό εξέταση Πληροφοριακό Σύστημα να αγνοείται. Η προαναφερόμενη μεθοδολογία μπορεί και συνδυάζει στοιχεία σχετικά με τον οργανισμό και το Πληροφοριακό Σύστημα ως συστήματα ανθρώπινης δραστηριότητας, αλλά και στοιχεία τα οποία εμφανίζονται σε κάθε ένα από τα υπάρχοντα εργαλεία ανάλυσης και διαχείρισης επικινδυνότητας.

Παρόλα αυτά, δεν πρέπει να λησμονούμε ότι υπάρχουν μειονεκτήματα (όπως αναφέρει και ο Κοκολάκης) 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 υλοποίησης των βημάτων της (βλ. [12], σελ. 121).

### 3 Συγκέντρωση Υλικού

Έχοντας, θέσει το πλαίσιο στο οποίο θα κινηθούμε και τη μεθοδολογία την οποία θα ακολουθήσουμε, είμαστε σε θέση να συγκεντρώσουμε το κατάλληλο υλικό για την ανάλυση απαιτήσεων που θα επακολουθήσει. Όπως έχει προαναφερθεί, το υλικό αυτό προέρχεται από την προηγούμενη διπλωματική εργασία και από συνεντεύξεις - συζητήσεις με άτομα έμπειρα στο χώρο της Ασφάλειας Πληροφοριακών Συστημάτων.

#### 3.1 Χαρακτηριστικά εργαλείου προς εξέταση

Κατ' αντιστοιχία με την Λαγού θα δημιουργηθεί ένας πίνακας με πιθανά χαρακτηριστικά που το εργαλείο θα μπορούσε να καλύπτει. Έτσι, ο σχετικός πίνακας της Λαγού ([13], σελ. 6-85) τροποποιείται. Παρακάτω παρατίθεται ο πίνακας με τα χαρακτηριστικά και ακολουθεί επεξήγηση για την τροποποίηση αυτού.

Ο πίνακας απεικονίζεται βάσει της μορφοποίησης που ακολούθησε η Λαγού. Με πλάγια γράμματα παρατίθενται τα προτεινόμενα από τη συγγραφέα χαρακτηριστικά:

##### **1. Χρήση της Ανάλυσης Επικινδυνότητας**

Πιστοποίηση

Ασφάλιση

Διαχείριση έργων

Υποστήριξη της λήψης αποφάσεων

Ασφάλεια & 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**

Υπολογισμός ευρεστικών (heuristics)

Ασαφείς μετρικές (Fuzzy metrics)

Ερωτηματολόγια

Αυτόματη διανομή/συλλογή/συγχώνευση ερωτηματολογίων

Ανάλυση στηριζόμενη στη βάση γνώσης

Ανάλυση με βάση προβλ.έψεις (*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 (customisation) - ανασχεδιασμός των διαδικασιών

Τροποποίηση - άμεση ενημέρωση της βάσης γνώσης

**3. Κόστος**

**4. Ευκολία χρήσης**

Ευχρηστία

Ποιότητα εγγράφων/ περιεκτικότητα

Ευκολία στη διαδικασία εγκατάστασης

Δυνατότητα αναίρεσης (Undo)

Δυνατότητα ανατροφοδότησης (*feedback*)

Άλλες χρήσιμες δυνατότητες / πρόσθετες ευκολίες

**5. Χρόνοι**

Διάρκεια εκτέλεσης της ανάλυσης επικινδυνότητας

Συχνότητα πραγματοποίησης ανάλυσης 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 φίλτραρισμάτος

Επαναχρησιμοποίηση των αποτελεσμάτων

Προσαρμογή (customisation) 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 ασφάλειας

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 αντιμέτρων

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. Ενοποίηση με άλλα εργαλεία**

Συμβατότητα υλικού/λογισμικού

Μεθοδολογική συμβατότητα

Πίνακας 3-1 : Χαρακτηριστικά εργαλείου προς εξέταση



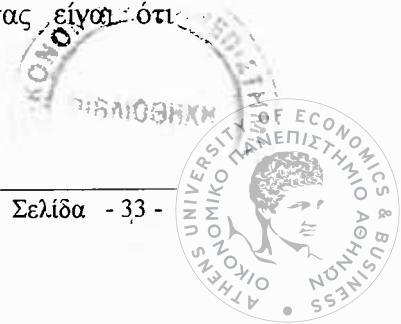
Στο ερωτηματολόγιο που συνέταξε η Λαγού παραλείπονται (ως ένα σημείο) θέματα σχετικά με τις δυσχέρειες / μειονεκτήματα που προαναφέρθηκαν. Όπως αναφέρεται στις πρώτες σελίδες της εργασίας, μία από τις λειτουργίες ενός ΠΣ είναι η εκπαίδευση και η μάθηση. Η εκπαίδευση & η μάθηση δεν πρέπει να περιορίζονται μόνο στην εκμάθηση του εργαλείου αλλά πρωτίστως στο νέο τρόπο οργάνωσης του οργανισμού (αφού κάθε ΠΣ εξυπηρετεί έναν οργανισμό) και στην αλλαγή της κουλτούρας. Κανένα αντίμετρο δε θα επιτύχει αν οι άνθρωποι που το εφαρμόσουν δεν «αλλάξουν».

Πέρα από την αλλαγή της κουλτούρας (που σχετίζεται περισσότερο με τη διαχείριση και όχι με την ανάλυση επικινδυνότητας) απαιτείται και η εξέταση του ΠΣ ως ολότητα (πέρα από την εξέταση και εκτίμηση των περιουσιακών στοιχείων του ΠΣ όπως αυτή αναφέρεται στη σελίδα 6-89 της Λαγού). Άλλωστε, χαρακτηριστικό κάθε συστήματος είναι η ολότητα που το διακρίνει και πρέπει το εργαλείο να εκτιμά και την επικινδυνότητα που το ΠΣ ως σύνολο έχει.

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

Πέρα από αυτά τα γενικά συμπεράσματα για τον Πίνακα της Λαγού έχουμε να προσθέσουμε τα εξής:

- Η ανάλυση 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 επικινδυνότητας είναι ότι αποτελεί εργαλείο επικοινωνίας μεταξύ διοίκησης και αναλυτών.



- Τα αντίμετρα που προτείνονται πρέπει να καλύπτουν θέματα όπως νομικά, ηθικά (αντλούμενα πχ από τον κώδικα δεοντολογίας), διοικητικά, λειτουργικά και τεχνικά όπως τα έχει προτείνει ο Kowalski ([8]), 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 ΠΣ προς εξέταση. Το ΠΣ πρέπει να μοντελοποιείται και ως ολότητα (πέρα από την κάλυψη – μοντελοποίηση των επιμέρους περιουσιακών στοιχείων).
- Πιθανές μέθοδοι για την ανάλυση επικινδυνότητας θα μπορούσαν να είναι η ανάλυση στηριζόμενη στη βάση γνώσης ή / και στις προβλέψεις (prediction analysis). Μέσω της δυνατότητας ανατροφοδότησης, μπορούμε να δημιουργήσουμε μία βάση γνώσης έτσι ώστε να διευκολύνεται η ανάλυση και αυτή (βάση γνώσης) να ενημερώνεται / 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 – διοίκησης.
- Η αιτιολόγηση των αντιμέτρων είναι σημαντική αφού η ανάλυση και διαχείριση επικινδυνότητας αποτελεί το εργαλείο επικοινωνίας – τη διεπαφή μεταξύ διοίκησης 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 αυτό θα ακολουθεί.



### 3.2 Απαιτήσεις προς εξέταση

Το επόμενο βήμα, μετά τα χαρακτηριστικά που επιδιώκονται να εξεταστούν κατά τις συνεντεύξεις, είναι η καταγραφή των σχετικών απαιτήσεων για το συγκεκριμένο εργαλείο. Και σ' αυτήν την περίπτωση θα ακολουθηθεί ο πίνακας της Λαγού ([13], σελ. 6-113) και η επεξήγηση αυτού στις σελίδες που προηγούνται του πίνακα, τροποποιώντας τον όπου κρίνεται αναγκαίο και ανάλογα με τα χαρακτηριστικά που έχουν αναφερθεί προηγουμένως.

#### 3.2.1 Βασικές λειτουργίες

##### 3.2.1.1 Φάσεις – βήματα του εργαλείου

Η ανάλυση και διαχείριση επικινδυνότητας που το εργαλείο θα επιτελεί θα πρέπει να περιλαμβάνει τις ακόλουθες φάσεις :

- **Φάση 1<sup>η</sup> : Ορισμός προβλήματος (ορισμός οργανισμού και ασφάλειας αυτού, ανάλυση οργανισμού, μοντέλοποίηση οργανισμού). Όπως έχει προαναφερθεί, χωρίς τον ορισμό του προβλήματος καμιά λύση δε θεωρείται σωστή. Πρέπει να δοθεί ένας ορισμός του οργανισμού χρησιμοποιώντας τη μεθοδολογία ευμετάβλητων συστημάτων (SSM) για κάθε κύριο δικαιούχο (stakeholder). Αν υπάρχουν πολλά υποσυστήματα, πρέπει, αναφέροντας τον ορισμό της ασφάλειας για τον οργανισμό, να συγκεκριμενοποιηθεί αυτός για κάθε υποσύστημα (εντάσσοντας και το ΠΣ προς εξέταση).**

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 ΔΡΔ ή και τα μοντέλα διαδικασιών (process models). Όσον αφορά το στατικό – δομικό μοντέλο, αυτό μπορεί να αναπαρασταθεί πχ με χρήση του μοντέλου οντοτήτων – συσχετίσεων E-R.

- **Φάση 2<sup>η</sup> : Ανάλυση επικινδυνότητας.** Η ανάλυση επικινδυνότητας πραγματοποιείται βασιζόμενη στα στοιχεία που παράχθηκαν κατά την προηγούμενη φάση. Εδώ έχουμε τον προσδιορισμό και την αποτίμηση των περιουσιακών αγαθών (assets) για κάθε μία από τις ιδιότητες (security properties)

που αυτά έχουν και σχετίζονται με την ασφάλεια (πχ εμπιστευτικότητα, ακεραιότητα). Η αποτίμηση των αγαθών πραγματοποιείται αναλύοντας τις επιπτώσεις που θα έχει η ζημία στα αγαθά αυτά δίνοντας έτσι και τη σχετική τους **αξία**. Δεν πρέπει να λησμονείται ότι η ίδια διαδικασία πρέπει να ακολουθηθεί και για τον οργανισμό ως ολότητα αλλά και για αγαθά που υποστηρίζουν τα κύρια αγαθά καθώς «μεταφέρεται» η ζημία σ' αυτά.

Επιμέρους βήμα της φάσης αυτής είναι ο εντοπισμός και αποτίμηση απειλών. Με την αναζήτηση των **αδυναμιών** μπορούμε να υπολογίσουμε τη σπουδαιότητά 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. Με την ολοκλήρωση των βημάτων αυτών αποτιμάται ο βαθμός επικινδυνότητας ως συνάρτηση των τριών προαναφερόμενων παραγόντων (αξία, σημαντικότητα απειλών, σοβαρότητα αδυναμιών). Για κάθε τέτοια τριάδα προσδιορίζεται ένας διαφορετικός βαθμός επικινδυνότητας.

- **Φάση 3<sup>η</sup> : Υλοποίηση.** Κάθε μία τριάδα που προαναφέρθηκε, περιγράφει ένα σενάριο προσβολής του υπό εξέταση ΠΣ. Έτσι, στη φάση αυτή απαιτείται μία ιεράρχηση των βαθμών επικινδυνότητας ώστε να προσδιοριστούν οι προτεραιότητες. Με την επικύρωση των αποτελεσμάτων αυτών αναπτύσσεται το σχέδιο ασφάλειας καθώς αυτό θα αντιστοιχείται με τις ανάγκες και τα ιδιαίτερα χαρακτηριστικά του ΠΣ και του οργανισμού όπως αυτά καταγράφθηκαν στις προηγούμενες φάσεις.

Το σχέδιο ασφάλειας περιλαμβάνει την πολιτική ασφάλειας, τα μέτρα προστασίας και τη στρατηγική υλοποίησης αυτού. Η πολιτική ασφάλειας 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, τεχνικά) όπως προτείνει ο Kowalski (βλ. [8]) ή οποιασδήποτε άλλης κατηγοριοποίησης.

- **Φάση 4<sup>η</sup> : Παρακολούθηση και αναθεώρηση.** Η φάση αυτή σχετίζεται με τη διαχείριση επικινδυνότητας. Θέματα όπως αλλαγές του οργανισμού, του περιβάλλοντος, της νομοθεσίας καθώς και τεχνολογικές εξελίξεις πρέπει να λαμβάνονται υπόψη έτσι ώστε να παρέχεται αποδοτικότερα η ασφάλεια. Έτσι, απαιτείται μία συνεχής ανάλυση των νέων συνθηκών σε σχέση με αυτές που χαρακτηρίζουν το σύστημα και τον οργανισμό.

Βέβαια, στη φάση αυτή πρέπει πρωτίστως να παρακολουθείται η υλοποίηση των αντιμέτρων και κατά πόσο αυτά ανταποκρίνονται στις τρέχουσες ανάγκες και αν επιφέρουν τα ίδια τα μέτρα προστασίας νέες απειλές. Τα σχετικά στοιχεία θα πρέπει να εισάγονται στη βάση γνώσης ώστε να τύχουν αξιοποίησης, και να σημάνουν την ανάγκη για επαναπροσδιορισμό. Τα προηγούμενα αποτελέσματα θα χρησιμοποιούνται ως μέτρο σύγκρισης, αλλά και για εμπλουτισμό της βάσης γνώσης. Η υλοποίηση του βήματος αυτού, όπως έχει προαναφερθεί, εναπόκειται στην ευθύνη της διοίκησης του προς εξέταση οργανισμού.

### 3.2.2 Άλλες απαιτήσεις

#### 3.2.2.1 Εφαρμογή σε κάθε στάδιο του κύκλου ζωής ανάπτυξης λογισμικού

Το εργαλείο αυτό θα πρέπει να είναι δυνατό να εφαρμόζεται σε κάθε στάδιο αφού ακόμα η ασφάλεια αγνοείται κατά την ανάπτυξη ενός ΠΣ. Έτσι, είναι δυνατή η αξιολόγηση του κόστους των μέτρων ασφαλείας (και των επιπτώσεων) με τη συντομότερη δυνατή ευκαιρία.

#### 3.2.2.2 Προσαρμογή στην ελληνική γλώσσα – κουλτούρα – νοοτροπία

Όπως έχει προαναφερθεί το εργαλείο προορίζεται για χρήση στον ελλαδικό χώρο, έτσι πρέπει να είναι προσαρμοσμένο στα ελληνικά δεδομένα. Σ' αυτά θα πρέπει να περιληφθούν τα εξής :

- Οι Έλληνες δεν είναι ιδιαίτερα νομομαθείς, ειδικότερα όσον αφορά τον ν. 2472/1997 (αρχή της αναλογίας και προστασία προσωπικών δεδομένων).

- Είναι, πολύ εύκολο, για οποιονδήποτε να εισέλθει σε μία 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 αντιμέτρων οργανωτικού χαρακτήρα, καθότι πρέπει να διαμορφωθεί μία κουλτούρα και μία παιδεία που να ενσωματώνει μέσα της το στοιχείο της ασφάλειας. Άλλα χαρακτηριστικά είναι τα εξής :

- Το μέγεθος των ελληνικών οργανισμών είναι μεσαίο. Το εργαλείο πρέπει να απευθύνεται σε τέτοιους οργανισμούς.
- Οι οργανισμοί διακατέχονται από αδυναμίες όσον αφορά την οργάνωσή 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 επικινδυνότητας θα πραγματοποιηθεί και η διαχείριση θα εφαρμοστεί. Οι υπάλληλοι δεν ξέρουν ποια είναι τα καθήκοντά τους είτε γιατί αυτά δεν είναι ορισμένα είτε γιατί δεν υπάρχει αντιστοίχηση θέσεως εργασίας με συγκεκριμένα χαρακτηριστικά του υπαλλήλου που καλύπτει αυτή τη θέση.

Τέλος, τρεις ακόμα απαιτήσεις που πρέπει να ληφθούν υπόψη είναι τα εξής :

- Η ελληνική και η ευρωπαϊκή νομοθεσία πρέπει να είναι ενσωματωμένη στο εργαλείο (ν. 2472/1997 άρθ. 10 παρ. 3 και οδ. 95/46/ΕC άρθ. 17 παρ. 2).

- Οι οθόνες, τα ερωτηματολόγια, οι εκθέσεις (reports) και γενικά κάθε διεπαφή του πρέπει να είναι στην ελληνική γλώσσα.
- Η χρηματική αξία των επιπτώσεων και αντιμέτρων να εκφράζεται σε δραχμές και σε EURO.

### 3.2.2.3 Εφαρμογή σε διάφορους επιχειρηματικούς κλάδους ή τύπους επιχειρήσεων και οργανισμών

Το εργαλείο θα πρέπει να μπορεί να εφαρμόζεται σε διάφορους τύπους επιχειρήσεων. Έτσι, θα είναι σε θέση το εργαλείο να αντιμετωπίζει διαφορετικά περιβάλλοντα και να αντεπεξέρχεται σ' αυτά και να αναπτύξει μία ποικίλη και εξεζητημένη βάση γνώσης.

### 3.2.2.4 Αλληλεξαρτήσεις των διαφορετικών συστημάτων

Είναι χρήσιμη η δυνατότητα αναπαράστασης της αλληλεξάρτησης των διαφόρων συστημάτων και υποσυστημάτων. Έτσι, γνωρίζουμε ότι αν ένα σύστημα A εξαρτάται από το B και το B είναι «επικίνδυνο» τότε το A κληρονομεί την επικινδυνότητα του B.

### 3.2.2.5 Ύπαρξη επιπέδων λεπτομέρειας μίας ανάλυσης

Η δυνατότητα αλλαγής του επιπέδου λεπτομέρειας παρέχει την ευελιξία να επικεντρώνεται ο αναλυτής σε συγκεκριμένες «προβληματικές» περιοχές, χωρίς να υπάρχει ανάγκη να πραγματοποιηθεί μία λεπτομερής ανάλυση. Έτσι, ανάλογα με τις ανάγκες θα μπορεί ο αναλυτής να εναλλάσσεται μεταξύ υψηλού επιπέδου ανάλυσης και λεπτομερούς επιπέδου.

### 3.2.2.6 Γρήγορη και αποτελεσματική εφαρμογή της μεθόδου

Ο χρόνος υλοποίησης της ανάλυσης επικινδυνότητας θα πρέπει να είναι κατά το δυνατόν συντομότερος. Λόγω αυστηρού περιορισμού χρόνου, ο αναλυτής θα πρέπει να είναι σε θέση να πραγματοποιεί την ανάλυση γρήγορα αλλά και αποτελεσματικά.

### 3.2.2.7 Βασικός μηχανισμός

Το εργαλείο θα πρέπει να αποτιμά την επικινδυνότητα βάσει του μηχανισμού, όπως αυτός απεικονίζεται και υπονοείται μέσα από τα παρακάτω σχήματα :



Υπάρχει μία αδυναμία η οποία μπορεί πολύ εύκολα να τύχει εκμετάλλευσης από μία απειλή		Αξία περιουσιακών στοιχείων	
		Μεγάλη	Μικρή
Πιθανότητα πραγματοποίησης μίας απειλής	Χαμηλή		
	Υψηλή	Υψηλό	

Πίνακας 3-2 : Το επίπεδο επικινδυνότητας όταν μία αδυναμία τύχει εκμετάλλευσης από απειλή

Δεν υπάρχει κάποια αδυναμία η οποία να μπορεί να τύχει εκμετάλλευσης από μία απειλή		Αξία περιουσιακών στοιχείων	
		Μεγάλη	Μικρή
Πιθανότητα πραγματοποίησης μίας απειλής	Χαμηλή		Χαμηλό
	Υψηλή		

Πίνακας 3-3 : Το επίπεδο επικινδυνότητας όταν δεν υπάρχει αδυναμία να τύχει εκμετάλλευσης από απειλή

Οι έννοιες «υψηλό», «χαμηλό», «εύκολο» μπορούν να οριστούν με ποιοτικό αλλά και με ποσοτικό τρόπο. Δηλαδή, είτε να πάρουν κάποιες σχετικές τιμές (πχ 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.

### 3.2.2.8 Τιμές επικινδυνότητας αγαθών – επιχειρηματικής επικινδυνότητας

Η επικινδυνότητα αποτελεί συνάρτηση της αξίας, της αδυναμίας και των απειλών για κάθε αγαθό αλλά και για τον οργανισμό γενικότερα. Όσο αυξάνει ο βαθμός της, τόσο η ανάγκη και το επίπεδο προστασίας αυτής πρέπει να αυξάνεται. Έτσι, απορρέουν και τα σχετικά αντίμετρα για να δικαιολογήσουν τα επίπεδα επικινδυνότητας. Η βαθμολόγηση αυτή μπορεί να γίνει είτε με πιθανοτικό τρόπο ή βάσει κάποιας ποιοτικής κλίμακας. Η επιχειρηματική επικινδυνότητα είναι εξίσου σημαντική, αφού όπως έχει ήδη αναφερθεί πρέπει να υπολογίζεται και ο οργανισμός ως σύνολο (καθότι βλέπουμε τον οργανισμό συστημικά).

### 3.2.2.9 Ορισμός ανεκτού επιπέδου επικινδυνότητας – υπόδειξη προβληματικών περιοχών

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.

Πέρα, όμως, από τον ορισμό ανεκτού επιπέδου επικινδυνότητας το εργαλείο θα πρέπει να υποδεικνύει που βρίσκονται τα σημαντικότερα προβλήματα. Όταν οι τιμές επικινδυνότητας των αγαθών έχουν ξεπεράσει κατά πολύ τα ανεκτά επίπεδα, υπάρχει κάποια ένδειξη σοβαρότητας και «κινδύνου». Έτσι, ο αναλυτής θα μπορεί να επικεντρώνεται στις προβληματικές περιοχές και να «αγνοεί» τις λοιπές. Σε αντίθετη περίπτωση, ο αναλυτής θα πρέπει να καταφεύγει σε μεθόδους δοκιμής και σφάλματος (trial and error) ή να εξετάζει λεπτομερώς κάθε συνιστώσα για να αναγνωρίσει την προβληματική περιοχή.

### 3.2.2.10 Αντίμετρα γενικά, ειδικά και οικονομικώς αποδοτικά

Τα αντίμετρα που προτείνονται πρέπει να αναφέρονται σε αντιμετώπιση γενικών απειλών. Όπου απαιτείται ανάγκη για εξειδίκευση, τα αντίμετρα θα πρέπει να είναι ειδικώς και λεπτομερώς περιγραμμένα, ώστε να τύχουν άμεσης και γρήγορης υλοποίησης.

Επιπλέον, τα αντίμετρα πρέπει να συμβαδίζουν με τα ποσά που πρόκειται – επιθυμεί να ξοδέψει ο οργανισμός. Έτσι, για κάθε αντίμετρο θα πρέπει να υπάρχει αιτιολόγηση επιλογής του και πληροφορίες σχετικές με την κοστολόγησή του. Δεν πρέπει να λησμονείται το γεγονός ότι η απόφαση είναι επιχειρηματική και ότι η ανάλυση και διαχείριση επικινδυνότητας αποτελεί το εργαλείο επικοινωνίας μεταξύ διοίκησης και αναλυτή.

### 3.2.2.11 Ισορροπημένο σύνολο από αντίμετρα – σύνδεση με δηλώσεις πολιτικής ασφάλειας

Πρέπει τα αντίμετρα να αντιμετωπίζουν -σε ιδανικές συνθήκες- όλα τα στάδια του κύκλου ζωής μίας απειλής. Δηλαδή, τα προτεινόμενα προς υλοποίηση αντίμετρα, θα πρέπει να εντοπίζουν μία απειλή, να μειώνουν την πιθανότητα εμφάνισής της και να συνεισφέρουν στην ανάκαμψη σε περίπτωση ζημίας.

Πέρα τούτου, τα αντίμετρα θα πρέπει να συνδέονται με δηλώσεις πολιτικών ασφάλειας (policy statements). Καθότι τα αντίμετρα πηγάζουν από την πολιτική ασφάλειας κρίνεται χρήσιμη η αιτιολόγηση σύνδεσης μεταξύ αντιμέτρων και

δηλώσεων καθώς και η δήλωση της σχέσης που υπάρχει ανάμεσά τους (σχέση επικάλυψης, σχέση συνεργασίας, σχέση αντιφατική).

### 3.2.2.12 Ύπαρξη μέτρων αποδοχής αντιμέτρων – μείωση αρνητικών συνεπειών

Καθότι υπάρχουν αντιρρήσεις και αντιστάσεις σε κάθε αλλαγή (και είναι ιδιαίτερα έκδηλο στον ελλαδικό χώρο) πρέπει να υπάρχει πρόβλεψη ύπαρξης μέτρων που θα βοηθούν στην υλοποίηση των προτεινόμενων αντιμέτρων. Μέσα σε τέτοια μέτρα περιλαμβάνονται η εκπαίδευση στο νέο τρόπο υλοποίησης των διαδικασιών καθώς και η αύξηση της ενημερότητας (awareness) του προσωπικού σε θέματα ασφάλειας.

Όπως έχει ήδη αναφερθεί και στην εισαγωγή της διατριβής αυτής, από τους κυριότερους παράγοντες της μη επαρκούς αντιμετώπισης των ζητημάτων ασφάλειας είναι η άγνοια και η περιορισμένη ενημέρωση σε θέματα σχετικά με την ασφάλεια. Επιπλέον, πρέπει να προλαμβάνονται περιπτώσεις εμφάνισης αρνητικών επιπτώσεων από την υλοποίηση των προτεινόμενων αντιμέτρων. 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.

### 3.2.2.13 Δυνητικός χρόνος επανάληψης της διαδικασίας

Στην πολιτική ασφάλειας ενσωματώνεται και η στρατηγική υλοποίησής της. Μέσα σ' αυτήν πρέπει να περιλαμβάνονται και δηλώσεις σχετικές με το χρόνο και τις καταστάσεις που θα πρέπει να επικρατούν έτσι ώστε να επαναληφθεί η διαδικασία για επικαιροποίηση των αντιμέτρων. Οι αιτίες μπορεί να είναι είτε σχετικές με αλλαγές στην τεχνολογία, είτε σχετικές με τη δομή του οργανισμού.

### 3.2.2.14 Δυνατότητα πειραματισμού με διαφορετικά σενάρια - επαλήθευση αποτελεσμάτων – δυνατότητα ιχνηλάτησης

Μία επιθυμητή απαίτηση κρίνεται η δυνατότητα πειραματισμού με διαφορετικά σενάρια. Μία ανάλυση βασισμένη σε σενάρια (scenario-based analysis) βοηθά τον αναλυτή να εξετάσει επιπρόσθετα χαρακτηριστικά και να τροποποιήσει τα υπάρχοντα μέχρι στιγμής αντίμετρα προς υλοποίηση. Μαζί με την ανάλυση βασισμένη σε σενάρια, σκόπιμη κρίνεται και η δυνατότητα επιβεβαίωσης / επαλήθευσης των αποτελεσμάτων. Η επαλήθευση αυτή επιβεβαιώνει τη συνέπεια ή όχι των

προτεινόμενων αντιμέτρων και βοηθά και στην εισαγωγή νέων δεδομένων ή αλλαγής των υπαρχόντων.

Επιπλέον θα ήταν χρήσιμη η δυνατότητα ιχνηλάτησης δηλαδή να κατανοήσουν την επιλογή ενός αντιμέτρου, την τιμή του κτλ. Η αιτιολόγηση κρίνεται απαραίτητη έτσι ώστε να υπάρχει επικύρωση από τη διοίκηση του οργανισμού. Έτσι, η ιχνηλάτηση πρέπει να είναι δυνατή και προς τα εμπρός και προς τα πίσω σε όλη τη διαδικασία ανάλυσης και διαχείρισης επικινδυνότητας, με ένα τρόπο κατά τον οποίο να είναι δυνατή η υποστήριξη οποιωνδήποτε απαιτούμενων δικαιολογήσεων.

### 3.2.2.15 Διαφορετικές μορφές εκθέσεων – δυνατότητα φιλτραρίσματος και επεξεργασίας

Οι εκθέσεις (reports) που παράγονται από το εργαλείο πρέπει να έχουν την συγκεκριμένη κάθε φορά μορφή. Εκθέσεις που απευθύνονται στην ανώτερη διοίκηση πρέπει να είναι πιο γενικές, σύντομες και περιεκτικές και με οικονομικούς όρους, ενώ εκθέσεις που απευθύνονται σε «τεχνικούς», πρέπει να είναι ειδικές και λεπτομερείς.

Επιπλέον, πρέπει να υπάρχει η δυνατότητα φιλτραρίσματος και επεξεργασίας. 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 (spreadsheets).

### 3.2.2.16 Ερωτηματολόγια με ελάχιστο σύνολο ερωτήσεων και προσεκτική / φιλτραρισμένη διατύπωση

Τα ερωτηματολόγια τα οποία θα παράγει το εργαλείο σε μορφή φόρμας (περιλαμβάνοντας στοιχεία όπως όνομα συνεντεύξιαζόμενου, ημερομηνία κτλ) προς εξεύρεση των αδύνατων σημείων του εξεταζόμενου ΠΣ, πρέπει να περιλαμβάνουν τουλάχιστον ένα ελάχιστο σύνολο ερωτήσεων. Το σύνολο αυτό θα υποδείκνυε κατά πόσο είναι συμβατός ο οργανισμός με την ελληνική νομοθεσία (ν 2472/1997).

Επίσης, οι ερωτήσεις πρέπει να είναι με τέτοιο τρόπο διατυπωμένες ώστε να ανταποκρίνονται στην ιδιότητα του συνεντεύξιαζόμενου. Έτσι, οι ερωτήσεις πρέπει να μην περιέχουν ασάφειες και να είναι σύντομες και περιεκτικές χωρίς να αποκλείεται η πιθανότητας διεξαγωγής συζήτησης στη θέση της συνέντευξης.

### 3.2.2.17 Δυναμικό «ξεδίπλωμα» ερωτήσεων με συνοδευτικά έγγραφα

Οι ερωτήσεις πρέπει να έχουν μία 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.

Χρήσιμη κρίνεται και μία επιπρόσθετη πληροφόρηση σε σχέση με τις ερωτήσεις. Όταν οι ερωτήσεις συνοδεύονται από σχετικά έγγραφα και κείμενα που εμπλουτίζουν τις γνώσεις του συνεντευξιαζόμενου και βοηθούν στην καλύτερη απάντηση, τότε η συνέντευξη κρίνεται επιτυχής.

### 3.2.2.18 Διαχείριση της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας

Το ίδιο το εργαλείο θα πρέπει να έχει διαδικασίες που να ελέγχουν την ροή της ανάλυσης και διαχείρισης επικινδυνότητας. Τέτοιες διαδικασίες είναι :

- Καταγραφή στοιχείων σχετικών με την ανάλυση (ορισμοί, μοντέλα, κτλ),
- Καταγραφή στοιχείων σχετικών με τις συνεντεύξεις,
- Καταγραφή στοιχείων σχετικών με το χρονοπρογραμματισμό των διαφόρων εργασιών (πχ διαγράμματα Gantt),
- Μηχανισμός υπενθύμισης (reminder) ημερομηνιών και εργασιών,
- Δημιουργία εκθέσεων προόδου (progress reports) με ταυτόχρονη δυνατότητα αναζήτησης – ιχνηλάτησης του σημείου στο οποίο βρίσκεται ο αναλυτής.

### 3.2.2.19 Εξαγωγή των δεδομένων

Τα δεδομένα που το εργαλείο παράγει κατά την ανάλυση, καθώς και η βάση γνώσης που σε κάθε ανάλυση εμπλουτίζεται θα πρέπει να είναι δυνατόν να εξάγονται σε μία προκαθορισμένη μορφή. Πάντως κρίνεται απαραίτητος ένας μηχανισμός ελέγχου των εκδόσεων των αρχείων για τυχόν προσπάθειες παραποίησης.



### 3.2.3 Απαιτήσεις από το λογισμικό και το υλικό

#### 3.2.3.1 Λειτουργικό Σύστημα και εναλλακτικό λειτουργικό σύστημα

Το εργαλείο θα πρέπει να λειτουργεί σε περιβάλλον MS Windows καθώς αυτό επικρατεί στην αγορά. Προτιμώνται εκδόσεις που είναι πιο δημοφιλείς (αυτή τη στιγμή Windows 98/2000/NT).

Επίσης κρίνεται σκόπιμη και η δυνατότητα λειτουργίας σε εναλλακτικό περιβάλλον (πχ Linux) καθώς αυξάνεται συνεχώς η αγορά του και υπάρχουν ένθερμοι υποστηρικτές του UNIX. Βέβαια, αυτό προϋποθέτει ότι ο χρήστης του εργαλείου θα είναι εξοικειωμένος με το περιβάλλον αυτό (προϋπόθεση που ικανοποιείται καθώς κάθε ερευνητική ομάδα διακατέχεται από έμφυτη τάση εξερεύνησης νέων εργαλείων, συστημάτων, κτλ).

#### 3.2.3.2 Λειτουργία του εργαλείου σε φορητό υπολογιστή

Καθότι η ανάλυση και διαχείριση επικινδυνότητας θεωρείται εργαλείο επικοινωνίας μεταξύ αναλυτή και διοίκησης, εξυπακούεται ότι οι συναντήσεις στο χώρο του οργανισμού του υπό εξέταση ΠΣ θα είναι πολλές. Έτσι, αν το εργαλείο μπορούσε να λειτουργεί σε περιβάλλον φορητού προσωπικού υπολογιστή (desktop PC), τότε θα διευκολύνοταν η εργασία του αναλυτή.

### 3.2.4 Απαιτήσεις απόδοσης

#### 3.2.4.1 Χρόνος για τις συνθετότερες εργασίες

Καθότι οι συνθετότερες εργασίες προϋποθέτουν μεγάλο χρόνο υλοποίησης, πρέπει το εργαλείο να εκτελεί τις εργασίες αυτές μέσα σε εύλογο χρονικό διάστημα. Προϋπόθεση αποτελεί το μηχάνημα εκτέλεσης να είναι τελευταίας τεχνολογίας (state of the art).

### 3.2.5 Μη λειτουργικές απαιτήσεις – περιορισμοί

#### 3.2.5.1 Ανάπτυξη με βάση τους υπάρχοντες πόρους

Το εργαλείο θα πρέπει να αναπτυχθεί (όλες του οι φάσεις) με βάση τους πόρους που έχει το Εργαστήριο Πληροφοριακών Συστημάτων και Βάσεων Δεδομένων. Καθότι η ερευνητική ομάδα (προς στιγμήν) εντάσσεται στο συγκεκριμένο εργαστήριο, πρέπει

τόσο το υλικό και το λογισμικό που το εργαστήριο έχει, να επαρκεί στην υλοποίηση του εργαλείου.

### 3.2.5.2 Ανεξαρτησία από άλλες εφαρμογές

Το εργαλείο θα πρέπει να είναι ανεξάρτητο από άλλα πακέτα λογισμικού και γενικώς από άλλες εφαρμογές. Η ανεξαρτησία βοηθά στην εγκυρότητα του εργαλείου.

### 3.2.6 Ειδικές απαιτήσεις – απαιτήσεις ασφάλειας

#### 3.2.6.1 Προστατευμένα δεδομένα

Βάσει του νόμου 2472/1997, τα δεδομένα της ανάλυσης και διαχείρισης επικινδυνότητας θα πρέπει να προστατεύονται για εξασφάλιση της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας. Η προστασία αυτή μπορεί να ενσωματωθεί στο ίδιο το εργαλείο, αλλιώς θα πρέπει το εργαλείο και τα δεδομένα να φυλάσσονται σε «ασφαλές» (καθότι η απόλυτη ασφάλεια είναι ουτοπία) μέρος.

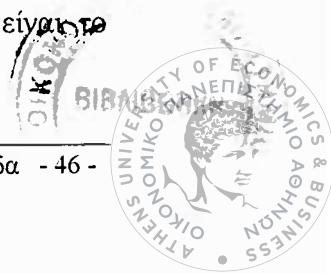
#### 3.2.6.2 Έλεγχος της διαδικασίας πρόσβασης και τροποποίησης

Για να προστατεύονται τα δεδομένα θα πρέπει να υπάρχει ένας μηχανισμός που θα ελέγχει την πρόσβαση στο εργαλείο και στη βάση γνώσης καθώς και την τροποποίηση αυτών. Αποτελεσματική θα ήταν μία διαβάθμιση του επιπέδου πρόσβασης του κάθε μέλους της ερευνητικής ομάδας (χρήστες με δυνατότητα πραγματοποίησης ανάλυσης επικινδυνότητας, τροποποίησης και μόνο ανάγνωσης).

### 3.2.7 Κριτική - Σύνοψη

Βάσει των προηγουμένων, παρατηρούμε μία μείωση του πλήθους των προς εξέταση απαιτήσεων. Αυτό οφείλεται στο ότι κάποιες απαιτήσεις ήταν παρόμοιες ή η μία επακόλουθη της άλλης, είτε στο ότι κάποιες απαιτήσεις ήταν περιττές.

Οι περιττές απαιτήσεις σχετίζονται με τη μεθοδολογία που το εργαλείο ακολουθεί και με τον ορισμό του εργαλείου αυτού. Τέτοιες είναι η ύπαρξη αυστηρής μεθόδου και η απαίτηση για ένα εργαλείο εύχρηστο και φιλικό. Όπως έχει ήδη αναφερθεί, το εργαλείο θα τύχει χρήσης από ερευνητική ομάδα. Δεν απαιτείται η ευχρηστία του εργαλείου για να υλοποιηθεί. Η εμπειρία και οι γνώσεις της ομάδας είναι σε θέση να ξεπεράσουν το εμπόδιο αυτό. Βέβαια, αυτό δεν σημαίνει ότι πρέπει να είγατε εργαλείο εξαιρετικά στρυφνό.



Άλλες απαιτήσεις, όπως τις διατύπωσε η Λαγού, αποτελούν η μία επακόλουθο της άλλης. Για παράδειγμα, οι απαιτήσεις για τη μορφή των εκθέσεων (reports) θα μπορούσαν να ενσωματωθούν σε μία (διαφορετικές μορφές εκθέσεων – δυνατότητα φιλτραρίσματος και επεξεργασίας). Το ίδιο ισχύει και για τα αντίμετρα (αντίμετρα γενικά, ειδικά και οικονομικώς αποδοτικά).

Από την άλλη πλευρά, υπάρχουν απαιτήσεις που έχουν τροποποιηθεί ριζικά με σημαντικότερη τις φάσεις – βήματα του εργαλείου. Εκεί, οι φάσεις έχουν τροποποιηθεί και ιδιαίτερα το περιεχόμενό τους. Αυτό οφείλεται στην επιλογή της μεθοδολογίας που το εργαλείο ακολουθεί.

Υπάρχουν, όμως, και απαιτήσεις που παρέμειναν ως έχουν, καθώς δεν κρινόταν αναγκαία η τροποποίησή τους (πχ Ειδικές απαιτήσεις – απαιτήσεις ασφάλειας, Μη λειτουργικές απαιτήσεις – περιορισμοί, Απαιτήσεις απόδοσης κτλ). Αυτό σημαίνει ότι και τώρα θα τύχουν επεξεργασίας και εξέτασης μέσω των κατάλληλων συνεντεύξεων.

Παρακάτω απεικονίζονται όλες οι απαιτήσεις με τη μορφή πίνακα. Οι απαιτήσεις έχουν ομαδοποιηθεί κατά κατηγορία ώστε ο αναγνώστης να μπορεί συγκεντρωτικά να τις επεξεργαστεί.

### **Βασικές λειτουργίες**

#### **1. Φάσεις –βήματα του εργαλείου**

##### **1.1 Ορισμός προβλήματος**

##### **1.2 Ανάλυση επικινδυνότητας**

##### **1.3 Υλοποίηση**

##### **1.4 Παρακολούθηση και αναθεώρηση**

### **Άλλες απαιτήσεις**

#### **1. Εφαρμογή σε κάθε στάδιο του κύκλου ζωής ανάπτυξης λογισμικού**

#### **2. Προσαρμογή στην ελληνική γλώσσα – κουλτούρα – νοοτροπία**

#### **3. Εφαρμογή σε διάφορους επιχειρηματικούς κλάδους ή τύπους επιχειρήσεων και οργανισμών**

#### **4. Άλληλεξαρτήσεις των διαφορετικών συστημάτων**

#### **5. Ύπαρξη επιπέδων λεπτομέρειας μιας ανάλυσης**

#### **6. Γρήγορη και αποτελεσματική εφαρμογή της μεθόδου**

#### **7. Βασικός μηχανισμός**

#### **8. Τιμές επικινδυνότητας αγαθών – επιχειρηματικής επικινδυνότητας**

#### **9. Ορισμός ανεκτού επιπέδου επικινδυνότητας – υπόδειξη προβληματικών περιοχών**

#### **10. Αντίμετρα γενικά, ειδικά και οικονομικώς αποδοτικά**

#### **11. Ισορροπημένο σύνολο από αντίμετρα – σύνδεση με δηλώσεις πολιτικής ασφάλειας**

#### **12. Ύπαρξη μέτρων αποδοχής αντιμέτρων – μείωση αρνητικών συνεπειών**



13. Δυνητικός χρόνος επανάληψης της διαδικασίας
14. Δυνατότητα πειραματισμού με διαφορετικά σενάρια / επαλήθευση αποτελεσμάτων – δυνατότητα ιχνηλάτησης
15. Διαφορετικές μορφές εκθέσεων – δυνατότητα φιλτραρίσματος και επεξεργασίας
16. Ερωτηματολόγια με ελάχιστο σύνολο ερωτήσεων και προσεκτική φιλτραρισμένη διατύπωση
17. Δυναμικό «ξεδίπλωμα» ερωτήσεων με συνοδευτικά έγγραφα
18. Διαχείριση της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας
19. Εξαγωγή των δεδομένων
<b>Απαιτήσεις από το λογισμικό και το υλικό</b>
1. Λειτουργικό Σύστημα και εναλλακτικό λειτουργικό σύστημα
2. Λειτουργία του εργαλείου σε φορητό υπολογιστή
<b>Απαιτήσεις απόδοσης</b>
1. Χρόνος για τις συνθετότερες εργασίες
<b>Μη λειτουργικές απαιτήσεις – περιορισμοί</b>
1. Ανάπτυξη με βάση τους υπάρχοντες πόρους
2. Ανεξαρτησία από άλλες εφαρμογές
<b>Ειδικές απαιτήσεις – απαιτήσεις ασφάλειας</b>
1. Προστατευμένα δεδομένα
2. Έλεγχος της διαδικασίας πρόσβασης και τροποποίησης

Πίνακας 3-4 : Απαιτήσεις εργαλείου προς εξέταση

### 3.3 Συμπεράσματα από συνεντεύξεις

Τα συμπεράσματα που προκύπτουν στην ενότητα αυτή, αντλούνται από τις συνεντεύξεις που πραγματοποιήθηκαν με έμπειρα στο χώρο της ασφάλειας άτομα. Προτιμήθηκε να επαναληφθεί η συνέντευξη στον έναν από την ομάδα συνεντευξιαζόμενων της Λαγού, λόγω της μεγάλης του εμπειρίας στο χώρο της ασφάλειας και ιδιαίτερα στην ανάλυση και διαχείριση επικινδυνότητας Πληροφοριακών Συστημάτων καθώς και σε έναν δεύτερο που και αυτός έχει μεγάλη εμπειρία, αν όχι την μεγαλύτερη, στο χώρο της ασφάλειας στον ελλαδικό χώρο.

Ο παρακάτω πίνακας παρουσιάζει τις απαιτήσεις που οι συνεντευξιαζόμενοι προτίμησαν να ενσωματωθούν στο εργαλείο. Πρέπει να σημειωθεί ότι ο τρόπος λήψης της συνέντευξης ήταν διαφορετικός στους δύο συνεντευξιαζόμενους λόγω πίεσης χρόνου.

Απαιτήσεις	Συνεντευξιαζόμενοι	
	X1	X2
<b>Βασικές λειτουργίες</b>		
1. Φάσεις -βήματα του εργαλείου	✓	✓
1.1 Ορισμός προβλήματος	✓	✓
1.2 Ανάλυση επικινδυνότητας	✓	✓
1.3 Υλοποίηση	✓	✓
1.4 Παρακολούθηση και αναθεώρηση	✓	✓
<b>Άλλες απαιτήσεις</b>		
1. Εφαρμογή σε κάθε στάδιο του κύκλου ζωής ανάπτυξης λογισμικού		✓
2. Προσαρμογή στην ελληνική γλώσσα - κουλτούρα - νοοτροπία	✓	✓
3. Εφαρμογή σε διάφορους επιχειρηματικούς κλάδους ή τύπους επιχειρήσεων και οργανισμών	✓	✓
4. Άλληλεξαρτήσεις των διαφορετικών συστημάτων		
5. Υπαρξη επιπέδων λεπτομέρειας μιας ανάλυσης	✓	✓
6. Γρήγορη και αποτελεσματική εφαρμογή της μεθόδου	✓	
7. Βασικός μηχανισμός	✓	✓
8. Τιμές επικινδυνότητας αγαθών - επιχειρηματικής επικινδυνότητας	✓	✓
9. Ορισμός ανεκτού επιπέδου επικινδυνότητας - υπόδειξη προβληματικών περιοχών	✓	✓
10. Αντίμετρα γενικά, ειδικά και οικονομικώς αποδοτικά	✓	✓
11. Ισορροπημένο σύνολο από αντίμετρα - σύνδεση με δηλώσεις πολιτικής ασφάλειας	✓	✓
12. Υπαρξη μέτρων αποδοχής αντιμέτρων - μείωση αρνητικών συνεπειών	✓	✓
13. Δυνητικός χρόνος επανάληψης της διαδικασίας		✓
14. Δυνατότητα πειραματισμού με διαφορετικά σενάρια / επαλήθευση αποτελεσμάτων δυνατότητα ιχνηλάτησης	✓	✓
15. Διαφορετικές μορφές εκθέσεων - δυνατότητα φίλτραρισμάτος και επεξεργασίας	✓	✓
16. Ερωτηματολόγια με ελάχιστο σύνολο ερωτήσεων και προσεκτική φίλτραρισμένη διατύπωση	✓	✓
17. Δυναμικό «ξεδίπλωμα» ερωτήσεων με συνοδευτικά έγγραφα		

18. Διαχείριση της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας		✓
19. Εξαγωγή των δεδομένων	✓	✓
<b>Απαιτήσεις από το λογισμικό και το υλικό</b>		
1. Λειτουργικό Σύστημα και εναλλακτικό λειτουργικό σύστημα	✓	
2. Λειτουργία του εργαλείου σε φορητό υπολογιστή	✓	
<b>Απαιτήσεις απόδοσης</b>		
Χρόνος για τις συνθετότερες εργασίες	✓	
<b>Μη λειτουργικές απαιτήσεις – περιορισμοί</b>		
1. Ανάπτυξη με βάση τους υπάρχοντες πόρους	✓	
2. Ανεξαρτησία από άλλες εφαρμογές	✓	✓
<b>Ειδικές απαιτήσεις – απαιτήσεις ασφάλειας</b>		
1. Προστατευμένα δεδομένα	✓	
2. Έλεγχος της διαδικασίας πρόσβασης και τροποποίησης	✓	

Πίνακας 3-5 : Παρουσίαση της σχέσης ανάμεσα σε συνεντευξιαζόμενους και απαιτήσεις

### 3.3.1 Σχόλια

Οι συνεντευξιαζόμενοι κατά τη διάρκεια της συνέντευξης έκαναν μερικές εύστοχες παρατηρήσεις που κρίνεται σκόπιμο να σχολιαστούν. Οι περισσότερες σχετίζονται με τον ορισμό του εργαλείου και το πεδίο δράσης / χρήσης του.

Συγκεκριμένα, το εργαλείο θα πρέπει να τυγχάνει χρήσης από ερευνητές του Πανεπιστημίου και αυτοσκοπός του είναι και παραμένει η ανάλυση. Αυτό όμως δεν αποκλείει και τη χρήση του από άλλους οργανισμούς, βασιζόμενοι όμως στην παραδοχή ότι αυτοί είναι γνώστες του χώρου της ασφάλειας. Παρόλα αυτά το εργαλείο δεν μπορεί να θεωρηθεί αυτοπροσαρμοζόμενο αλλά παραμένει ένα κλασσικό εργαλείο. Μέσα από ένα πλήθος αναλύσεων θα συλλέγονται στοιχεία όπου με κατάλληλη επεξεργασία θα συντελούν σε μία νέα έκδοση.

Επιπλέον, ένα μειονέκτημα των εργαλείων ανάλυσης και διαχείρισης επικινδυνότητας ΠΣ είναι η δυσκολία 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 διαδικασιών είναι εφικτή. Μία άλλη μοντελοποίηση (πχ 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 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 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). Σ' 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 αυτά θα πρέπει να είναι οργανωμένα, παραμετροποιημένα προς χρήση.

Βάσει αυτών παρατηρούμε ότι ανάλογα με τις απαιτήσεις που επιθυμούμε να πραγματοποιήσουμε τροποποιείται και ο τρόπος πραγματοποίησης της ανάλυσης. Αν ακολουθήσουμε τον κλασσικό τρόπο θα χρησιμοποιήσουμε ερωτηματολόγια, αλλιώς αν χρησιμοποιήσουμε ανάλυση σεναρίων τότε τα ερωτηματολόγια κρίνονται περιττά.

Το μόνο σημείο διαφοράς στους δύο συνεντεύξιαζόμενους είναι ως προς την απαίτηση για διαχείριση της διαδικασίας ανάλυσης και διαχείρισης επικινδυνότητας. Ο ένας θεώρησε ως μη αναγκαία την ύπαρξη της διαχείρισης αυτής, ενώ ο δεύτερος τη θεώρησε πολύ σημαντική. Συγκεκριμένα, πιστεύει ότι είναι χρήσιμο να υπάρχουν κάποιοι μηχανισμοί που να παρακολουθούν την ροή της διαχείρισης της

επικινδυνότητας ΠΣ, την υλοποίηση της πολιτικής ασφάλειας και των αντιμέτρων. Έτσι, η διοίκηση θα είναι σε θέση να «ελέγχει» την πορεία υλοποίησης και να λαμβάνει κάποια σήματα σε περίπτωση προβλήματος.

Το σημαντικότερο συμπέρασμα, όμως, και από τις δύο συνεντεύξεις είναι η ανάγκη για «εξυπνότερο» εργαλείο. Και οι δύο συνεντεύξιαζόμενοι τόνισαν ότι είναι απαραίτητο να έχει το εργαλείο κάποια «εξυπνάδα», νοημοσύνη (intelligent, smart tool). Πάντως, τόνισαν ότι δεν είναι σε θέση, αυτή τη στιγμή, να φανταστούν πως θα ενσωματωνόταν αυτή η εξυπνάδα αν και αποτελεί επιθυμία να δουν ένα καινούριο εργαλείο πιο έξυπνο ή να βελτιωθεί ως προς αυτό το σημείο ένα υπάρχον εργαλείο με μία νέα του έκδοση.

Με την ολοκλήρωση των συνεντεύξεων και την επεξεργασία των συμπερασμάτων αυτών είμαστε σε θέση να προχωρήσουμε στην ανάλυση απαιτήσεων. Στα επόμενα κεφάλαια πραγματοποιείται η ανάλυση απαιτήσεων και η σχεδίαση (στο μέγιστο δυνατό σημείο) ακολουθώντας το μοντέλο του κύκλου ζωής λογισμικού του ΙΕΕΕ.

## 4 Ανάλυση Απαιτήσεων

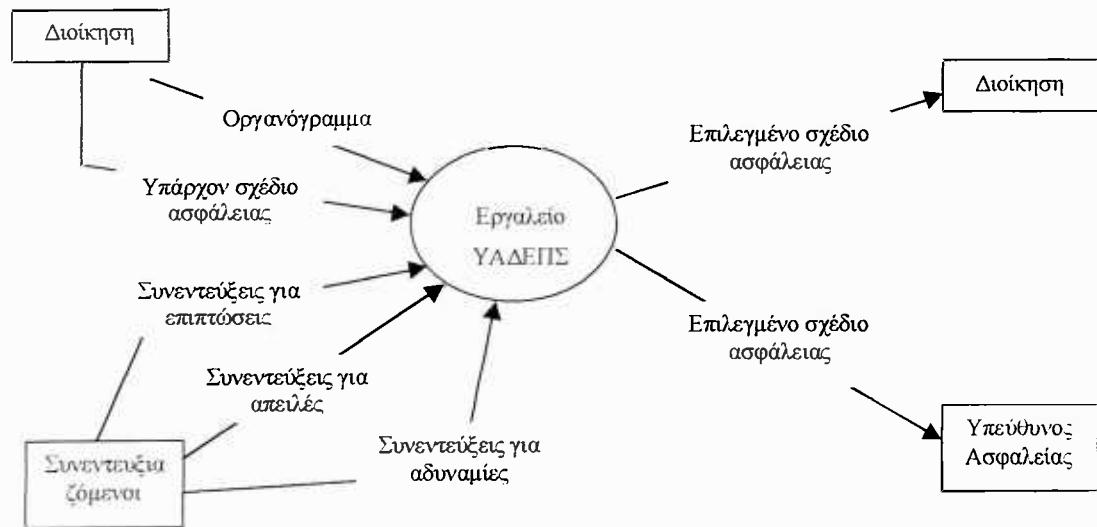
Όπως προαναφέρθηκε η ανάλυση απαιτήσεων θα ακολουθήσει το μοντέλο του κύκλου ζωής λογισμικού του IEEE. Στο κεφάλαιο αυτό θα παραχθεί το Έγγραφο Περιγραφής Απαιτήσεων Λογισμικού (καθώς το υπό εξέταση εργαλείο είναι λογισμικό), όπως αυτό προσδιορίζεται από το πρότυπο ANSI/IEEE Std 830-1984 ([10]). Θα προσπαθήσουμε να διατηρήσουμε την πρότυπη μορφή του προσαρμόζοντάς το στις ανάγκες της εργασίας αυτής.

### 4.1 Διαγράμματα Ροής Δεδομένων και Λεξικό Δεδομένων

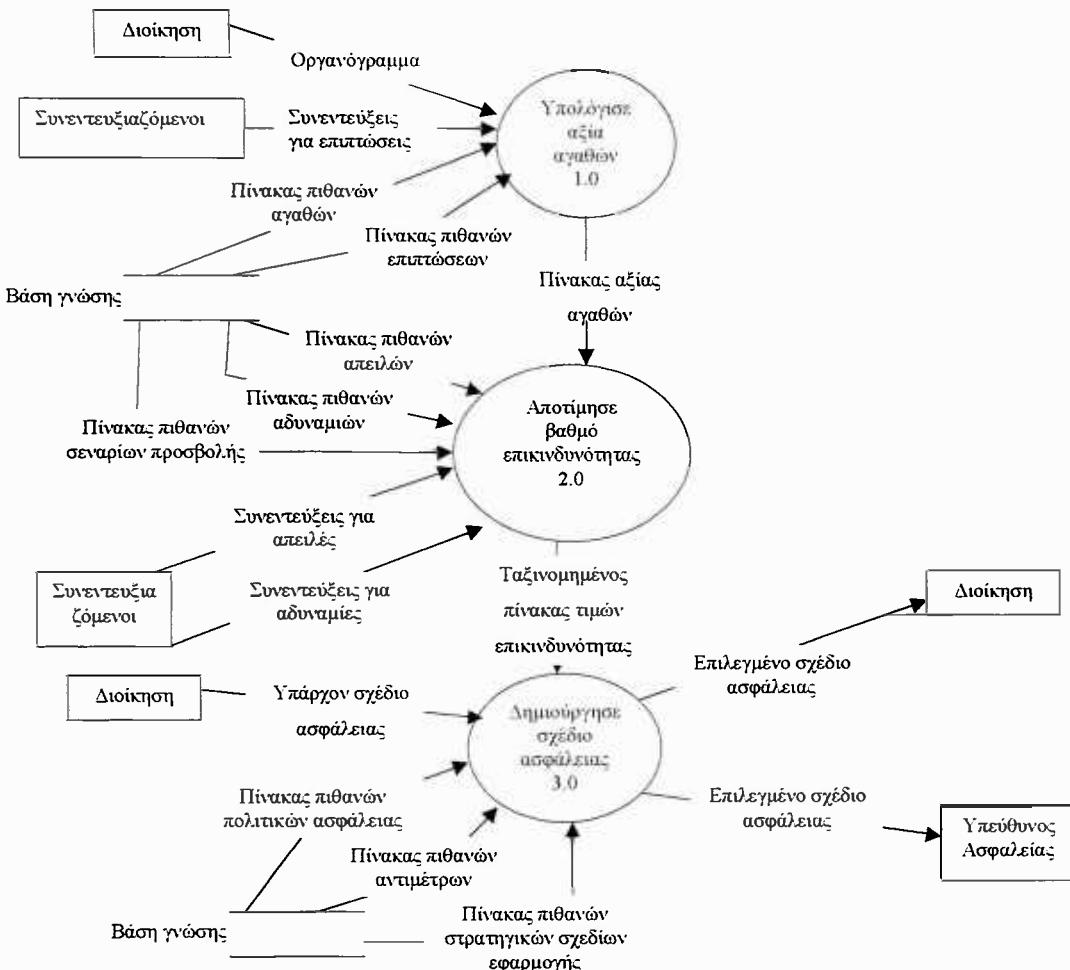
Προτού περιγραφεί το ΕΠΑΛ πρέπει να παρατεθούν τα ΔΡΔ και το σχετικό Λεξικό Δεδομένων. Τα ΔΡΔ που θα παρουσιαστούν θεωρούνται επικυρωμένα έτσι ώστε να προχωρήσει η σχεδίαση του εργαλείου – λογισμικού αυτού.

#### 4.1.1 Διαγράμματα Ροής Δεδομένων

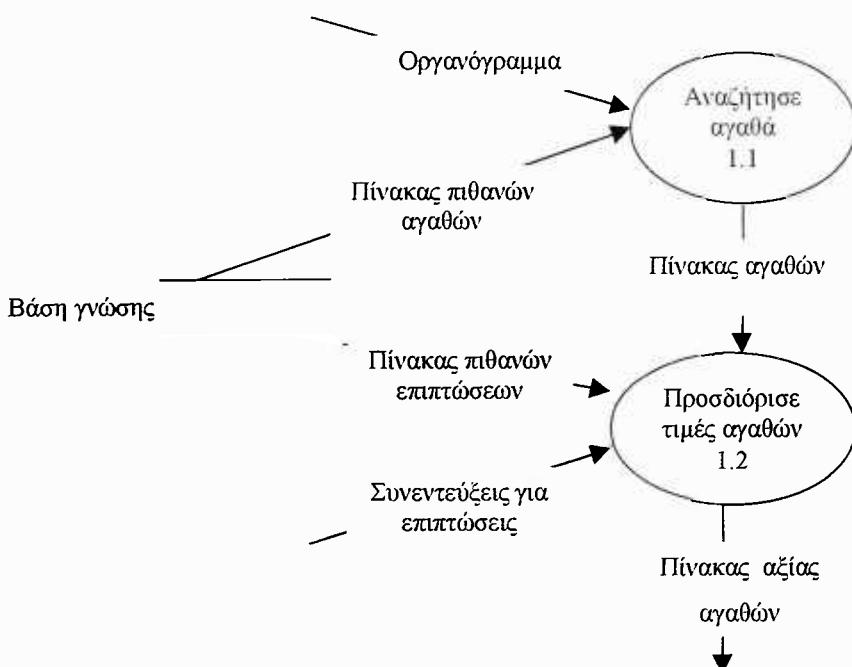
Παρακάτω παρατίθενται τα ΔΡΔ ξεκινώντας από το Διάγραμμα Πλαίσιο και προχωρώντας στα παρακάτω επίπεδα. Το τελικό ΔΡΔ έχει παραληφθεί για λόγους διευκόλυνσης.



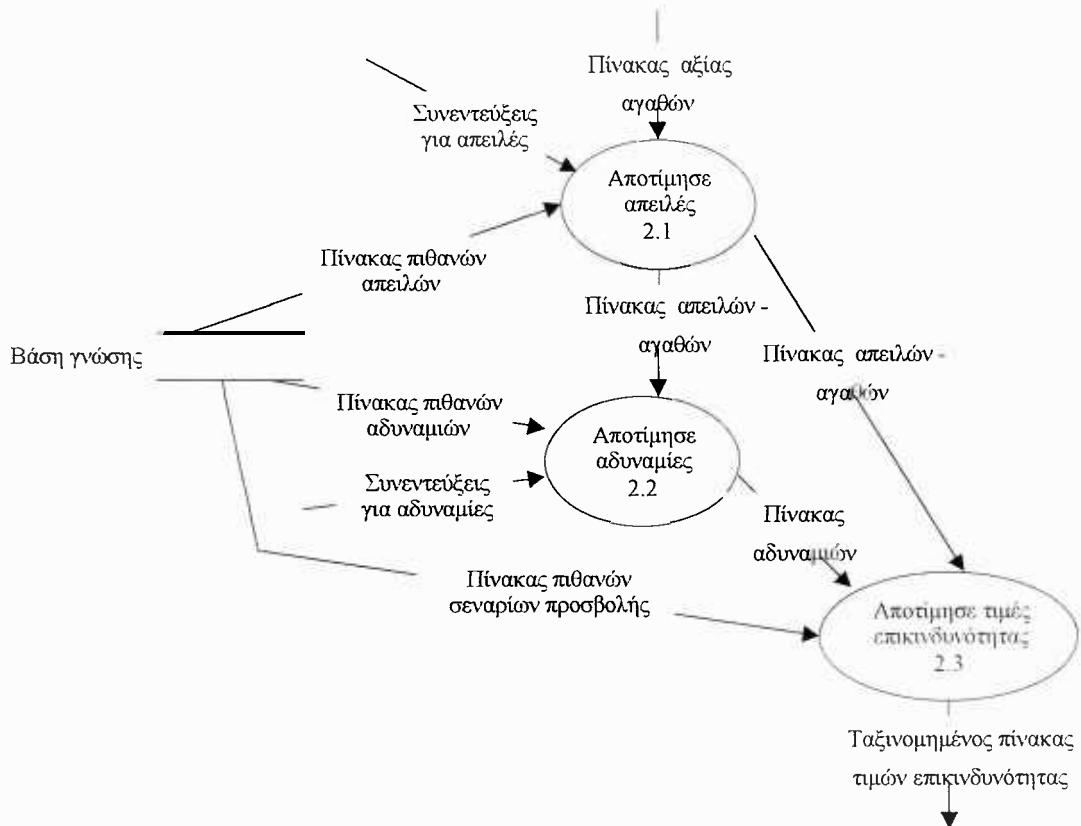
Σχήμα 4-1 : Διάγραμμα Πλαίσιο



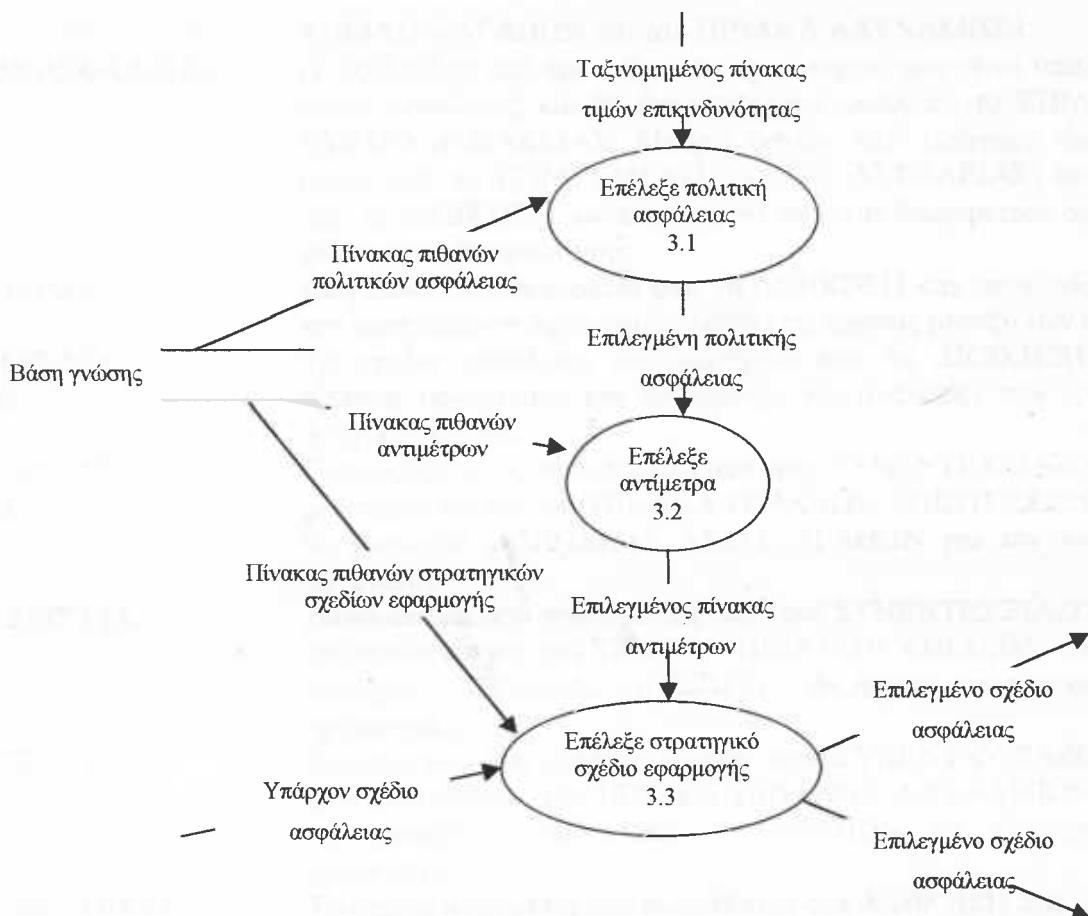
Σχήμα 4-2 : Διάγραμμα μηδέν



Σχήμα 4-3 : Υπολόγιση αξία αγαθών 1.0



Σχήμα 4-4 : Αποτίμηση βαθμό επικινδυνότητας 2.0



Σχήμα 4-5 : Δημιουργησε σχέδιο ασφάλειας 3.0

#### 4.1.2 Λεξικό Δεδομένων

Στο λεξικό δεδομένων περιλαμβάνονται ορισμοί των δεδομένων, των αποθηκευτικών χώρων και των εξωτερικών οντοτήτων (πηγές / καταλήξεις) του ΔΡΔ ([11], σελ. 227)<sup>1</sup>. Οι ορισμοί παρατίθενται ξεκινώντας από το Διάγραμμα Πλαίσιο και προχωρώντας στα παρακάτω επίπεδα<sup>2</sup>.

##### 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 προσδιορισμό του ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ, του ΠΙΝΑΚΑ

<sup>1</sup> Οσοι ορισμοί δεν αναφέρονται εδώ, έχουν περιληφθεί είτε στα εισαγωγικά κεφάλαια της εργασίας αυτής, είτε στην προηγούμενη της Λαγόν ([13]).

<sup>2</sup> Η διπλή γραμμή διαχωρίζει τα επίπεδα στα ΔΡΔ ξεκινώντας από το Διάγραμμα Πλαίσιο.

**ΥΠΕΥΘΥΝΟΣ ΑΣΦΑΛΕΙΑΣ****ΑΠΕΙΔΩΝ-ΑΓΑΘΩΝ και του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ.**

Ο υπάλληλος του προς εξέταση οργανισμού που είναι υπεύθυνος του τομέα ασφάλειας και θα 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 ανάλυσης.

Διάγραμμα που παρέχεται από τη ΔΙΟΙΚΗΣΗ και απεικονίζει στατικά τον προς εξέταση οργανισμό. Δείχνει τις σχέσεις μεταξύ των τμημάτων. Το σχέδιο ασφάλειας που παρέχεται από τη ΔΙΟΙΚΗΣΗ του προς εξέταση οργανισμού και προϋπάρχει της ανάλυσης που πρόκειται να πραγματοποιηθεί.

Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ για τον υπό εξέταση οργανισμό.

Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ για τον υπό εξέταση οργανισμό.

Πληροφορίες που συλλέγονται από τους ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ χρησιμοποιώντας τον ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ με σκοπό να παραχθεί ο ΠΙΝΑΚΑΣ ΑΔΥΝΑΜΙΩΝ για τον υπό εξέταση οργανισμό.

Το σχέδιο ασφάλειας που παραδίδεται στη ΔΙΟΙΚΗΣΗ από τον αναλυτή ύστερα από επικύρωση.

**ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ**

Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με αγαθά που τυχόν ο υπό εξέταση οργανισμός έχει με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΓΑΘΩΝ.

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.

Πίνακας με τα αγαθά του υπό εξέταση οργανισμού και την αξία για καθένα από αυτά.

Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πιθανές απειλές για τον υπό εξέταση οργανισμό για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ για ΑΠΕΙΛΕΣ με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ.

Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με αδυναμίες που τυχόν ο υπό εξέταση οργανισμός έχει για να πραγματοποιηθούν οι ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ, με σκοπό την παραγωγή του ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ.

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.

Πίνακας με τιμές επικινδυνότητας για κάθε αγαθό του υπό εξέταση οργανισμού ταξινομημένες κατά φθίνουσα σειρά.

Πίνακας από τη ΒΑΣΗ ΓΝΩΣΗΣ του εργαλείου με πολιτικές ασφάλειας

ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ	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 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 ΕΠΙΛΕΓΜΕΝΟΣ ΠΙΝΑΚΑΣ ΑΝΤΙΜΕΤΡΩΝ ΒΑΣΗ ΓΝΩΣΗΣ	Η πολιτική ασφάλειας που επιλέγεται για τον υπό εξέταση οργανισμό από τον αναλυτή και επικυρώνεται από τη ΔΙΟΙΚΗΣΗ.
ΥΔΕΠΣ	Πίνακας με τα αντίμετρα που επιλέγονται από τον αναλυτή και επικυρώνονται από τη ΔΙΟΙΚΗΣΗ του υπό εξέταση οργανισμού. Περιλαμβάνει δεδομένα σχετικά με αγαθά, επιπτώσεις, απειλές, αδυναμίες, σενάρια προσβολής, αντίμετρα, πολιτικές ασφάλειας, στρατηγικά σχέδια εφαρμογής. Υποστήριξη της Ανάλυσης και Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων

Πίνακας 4-1 : Λεξικό Δεδομένων

## 4.2 Έγγραφο Παραστατικό Απαιτήσεων Λογισμικού

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.

### 4.2.1 Λειτουργικές Απαιτήσεις

Η ενότητα αυτή περιλαμβάνει τη διάσπαση του λογισμικού σε επιμέρους λειτουργίες με σκοπό τη βελτίωση της αναγνωσιμότητας του ΕΠΑΛ. Όπως γίνεται αντίληπτό στις παρακάτω σελίδες, οι λειτουργίες μπορούν να αντιστοιχηθούν με τις φάσεις της μεθοδολογίας που το εργαλείο ακολουθεί.

#### 4.2.1.1 1<sup>η</sup> λειτουργία

ΟΝΟΜΑ

ΥΠΟΛΟΓΙΣΜΟΣ ΑΞΙΑΣ ΑΓΑΘΩΝ

Η λειτουργία αυτή αποτελείται από τις επιμέρους λειτουργίες *ANAZHTHΣΗ ΑΓΑΘΩΝ* και *ΠΡΟΣΔΙΟΡΙΣΜΟΣ ΤΙΜΩΝ ΑΓΑΘΩΝ*.

ΕΙΣΑΓΩΓΗ	Η λειτουργία αυτή έχει ως σκοπό να υπολογιστεί η αξία των αγαθών του υπό εξέταση οργανισμού, αφού πρώτα αυτά αναζητηθούν. Η υπολογισμένη αξία των αγαθών βοηθά στην εκπλήρωση των επόμενων λειτουργιών.
ΕΙΣΟΔΟΙ	<b>ΟΡΓΑΝΟΓΡΑΜΜΑ</b> <b>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ</b> <b>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ</b> <b>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ</b>
ΕΠΕΞΕΡΓΑΣΙΑ	Πάρε ΟΡΓΑΝΟΓΡΑΜΜΑ από τη ΔΙΟΙΚΗΣΗ και ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΓΑΘΩΝ από ΒΑΣΗ ΓΝΩΣΗΣ. Σύγκρινε τις πληροφορίες αυτές για <i>ANAZHTHΣΗ ΑΓΑΘΩΝ</i> και παρήγαγε <i>ΠΙΝΑΚΑ ΑΓΑΘΩΝ</i> για <i>ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΙΜΩΝ ΑΓΑΘΩΝ</i> . Στα αγαθά θα περιλαμβάνονται και τα επιμέρους – υποστηρικτικά αυτών. Πάρε <i>ΠΙΝΑΚΑ ΑΓΑΘΩΝ</i> από <i>ANAZHTHΣΗ ΑΓΑΘΩΝ</i> , <i>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΕΠΙΠΤΩΣΕΩΝ</i> από ΒΑΣΗ ΓΝΩΣΗΣ και <i>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΕΠΙΠΤΩΣΕΙΣ</i> από <i>ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ</i> . Σύγκρινε τις πληροφορίες για <i>ΠΡΟΣΔΙΟΡΙΣΜΟ ΤΙΜΩΝ ΑΓΑΘΩΝ</i> και παρήγαγε <i>ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ</i> για <i>ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</i> . Οι επιπτώσεις θα υπολογιστούν και για τα επιμέρους – υποστηρικτικά αγαθά των κυρίων αγαθών.
ΕΞΟΔΟΙ	<i>ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ</i>

#### 4.2.1.2 2<sup>η</sup> λειτουργία

ΟΝΟΜΑ	<b>ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</b> Η λειτουργία αυτή αποτελείται από τις επιμέρους λειτουργίες <i>ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ</i> , <i>ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ</i> και <i>ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</i> .
ΕΙΣΑΓΩΓΗ	Η λειτουργία αυτή έχει ως σκοπό να αποτιμηθεί ο βαθμός επικινδυνότητας του υπό εξέταση οργανισμού για κάθε αγαθό αυτού και για το σύνολό του. Ο βαθμός επικινδυνότητας βοηθά στην ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ.
ΕΙΣΟΔΟΙ	<i>ΠΙΝΑΚΑΣ ΑΞΙΑΣ ΑΓΑΘΩΝ</i> <i>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΠΕΙΛΕΣ</i> <i>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ</i> <i>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ</i> <i>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ</i> <i>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ</i>
ΕΠΕΞΕΡΓΑΣΙΑ	Πάρε <i>ΠΙΝΑΚΑ ΑΞΙΑΣ ΑΓΑΘΩΝ</i> από <i>ΥΠΟΛΟΓΙΣΜΟ ΑΞΙΑΣ ΑΓΑΘΩΝ</i> , <i>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΠΕΙΛΕΣ</i> από <i>ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ</i> και <i>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΠΕΙΛΩΝ</i> από ΒΑΣΗ ΓΝΩΣΗΣ. Σύγκρινε τις πληροφορίες αυτές για <i>ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ</i> και παρήγαγε <i>ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ</i> για <i>ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ</i> και <i>ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</i> . Πάρε <i>ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ</i> από <i>ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ</i> , <i>ΣΥΝΕΝΤΕΥΞΕΙΣ ΓΙΑ ΑΔΥΝΑΜΙΕΣ</i> από <i>ΣΥΝΕΝΤΕΥΞΙΑΖΟΜΕΝΟΥΣ</i> και <i>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΔΥΝΑΜΙΩΝ</i> από ΒΑΣΗ ΓΝΩΣΗΣ. Σύγκρινε τις πληροφορίες για <i>ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ</i> και παρήγαγε <i>ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ</i> για <i>ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</i> . Πάρε <i>ΠΙΝΑΚΑ ΑΠΕΙΛΩΝ - ΑΓΑΘΩΝ</i> από <i>ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ</i> , <i>ΠΙΝΑΚΑ ΑΔΥΝΑΜΙΩΝ</i> από <i>ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ</i> και <i>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΕΝΑΡΙΩΝ ΠΡΟΣΒΟΛΗΣ</i> 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**

#### 4.2.1.3 3<sup>η</sup> λειτουργία

<b>ΟΝΟΜΑ</b>	<b>ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ</b>
	Η λειτουργία αυτή αποτελείται από τις επιμέρους λειτουργίες <b>ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ</b> , <b>ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ</b> και <b>ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ</b> .
<b>ΕΙΣΑΓΩΓΗ</b>	Η λειτουργία αυτή έχει ως σκοπό να σχεδιασθεί το σχέδιο ασφάλειας του υπό εξέταση οργανισμού. Στο σχέδιο ασφάλειας θα περιλαμβάνεται και ο τρόπος υλοποίησης και η δυνατότητα ιχνηλάτησης μέσα σ' αυτό.
<b>ΕΙΣΟΔΟΙ</b>	<b>ΤΑΞΙΝΟΜΗΜΕΝΟΣ ΠΙΝΑΚΑΣ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</b> <b>ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ</b> <b>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ</b> <b>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΑΝΤΙΜΕΤΡΩΝ</b> <b>ΠΙΝΑΚΑΣ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ</b>
<b>ΕΠΕΞΕΡΓΑΣΙΑ</b>	Πάρε <b>ΤΑΞΙΝΟΜΗΜΕΝΟ ΠΙΝΑΚΑ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</b> από <b>ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ</b> και <b>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ</b> από <b>ΒΑΣΗ ΓΝΩΣΗΣ</b> . Σύγκρινε τις πληροφορίες αυτές για <b>ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ</b> και παρήγαγε την <b>ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ</b> για <b>ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ</b> . Πάρε <b>ΕΠΙΛΕΓΜΕΝΗ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ</b> από <b>ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ</b> και <b>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΑΝΤΙΜΕΤΡΩΝ</b> από <b>ΒΑΣΗ ΓΝΩΣΗΣ</b> . Σύγκρινε τις πληροφορίες για <b>ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ</b> και παρήγαγε <b>ΕΠΙΛΕΓΜΕΝΟ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ</b> για <b>ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ</b> . Πάρε <b>ΕΠΙΛΕΓΜΕΝΟ ΠΙΝΑΚΑ ΑΝΤΙΜΕΤΡΩΝ</b> από <b>ΕΠΙΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ</b> , <b>ΥΠΑΡΧΟΝ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ</b> από <b>ΔΙΟΙΚΗΣΗ</b> και <b>ΠΙΝΑΚΑ ΠΙΘΑΝΩΝ ΣΤΡΑΤΗΓΙΚΩΝ ΣΧΕΔΙΩΝ ΕΦΑΡΜΟΓΗΣ</b> από <b>ΒΑΣΗ ΓΝΩΣΗΣ</b> . Σύγκρινε τις πληροφορίες αυτές για <b>ΕΠΙΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ</b> και παρήγαγε <b>ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ</b> για επικύρωση από τη <b>ΔΙΟΙΚΗΣΗ</b> και εφαρμογή από <b>ΥΠΕΥΘΥΝΟ ΑΣΦΑΛΕΙΑΣ</b> .
<b>ΕΞΟΔΟΙ</b>	<b>ΕΠΙΛΕΓΜΕΝΟ ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ</b>

#### 4.2.2 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 επικοινωνίες.

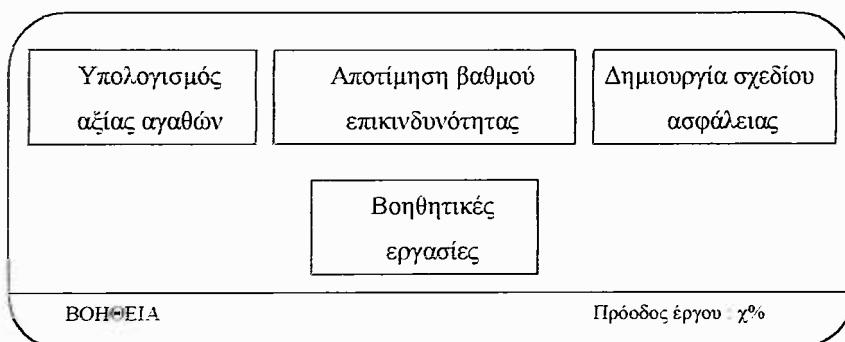
##### 4.2.2.1 Διεπαφές χρήστη

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

#### 4.2.2.1.1 Μορφή οθονών

Πρέπει να επισημανθεί το γεγονός ότι κατά την εισαγωγή στο εργαλείο εμφανίζεται παράθυρο σύνδεσης για πληκτρολόγηση των στοιχείων του αναλυτή. Όπως έχει αναφερθεί, οι ενέργειες του αναλυτή περιορίζονται στα δικαιώματα πρόσβασης που ο καθένας 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 ΒΑΘΟΥΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ ΔΗΜΙΟΥΡΓΙΑ ΣΧΕΔΙΟΥ ΑΣΦΑΛΕΙΑΣ.**



**Οθόνη 4-1 : 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 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 :

Αναζήτηση αγαθών	Προσδιορισμός τιμών αγαθών	Παραγωγή ερωτηματολογίων
ΒΟΗΘΕΙΑ		Πρόοδος έργου <span style="border: 1px solid black; padding: 2px;">χ%</span>

**Οθόνη 4-2 : Υπολογισμός αξίας αγαθών**

Στην ΑΝΑΖΗΤΗΣΗ ΑΓΑΘΩΝ εμφανίζεται το κάτω παράθυρο :

Επιλέξτε τα αγαθά του οργανισμού XYZ :		
<input type="text"/>		
Εισαγωγή αγαθού	Εκπύπωση	Επικύρωση
ΒΟΗΘΕΙΑ		Πρόοδος έργου <span style="border: 1px solid black; padding: 2px;">χ%</span>

**Οθόνη 4-3 : Αναζήτηση αγαθών**

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 :

Όνομα αγαθού ..... Περιγραφή .....
<input type="button" value="OK"/>

**Οθόνη 4-4 : Εισαγωγή αγαθού**

Ο αναλυτής πληκτρολογεί τα σχετικά στοιχεία και επιλέγει το OK 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 :

Επικυρώστε την αξία των κάτω αγαθών :

Εκτύπωση

Επικύρωση

ΒΟΗΘΕΙΑΠρόοδος έργου : χ%

Οθόνη 4-5 : Προσδιορισμός τιμών αγαθών

Στον εσωτερικό πίνακα εμφανίζεται η τιμή κάθε αγαθού για κάθε μία ιδιότητα αυτού σε περίπτωση απώλειάς 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 :

Εκτύπωση

Ενημέρωση

ΒΟΗΘΕΙΑΠρόοδος έργου : χ%

Οθόνη 4-6 : Παραγωγή ερωτηματολογίων

Με την επιλογή ΕΚΤΥΠΩΣΗ εμφανίζεται το παρακάτω παράθυρο :

Όνομα συνεντευξιαζόμενου :	.....
Περιγραφή ιδιότητας :	.....
<input type="button" value="OK"/>	

#### Οθόνη 4-7 : Εκτύπωση

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

Με την επιλογή ΕΝΗΜΕΡΩΣΗ εμφανίζεται το κάτω παράθυρο .

Ενημερώστε την αξία των παρακάτω αγαθών :

.....	.....
.....	.....

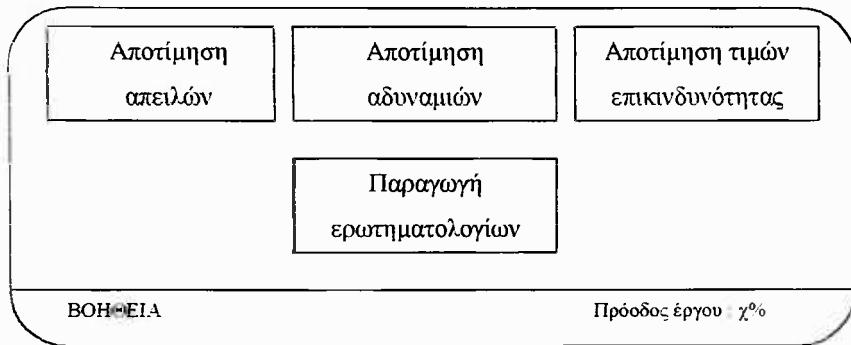
**OK**

#### Οθόνη 4-8 : Ενημέρωση

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

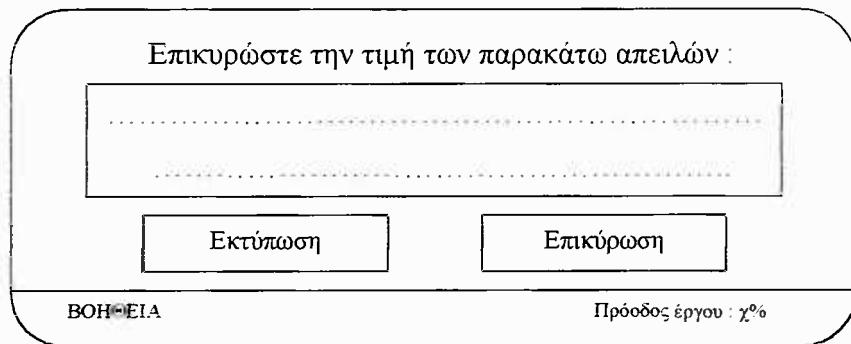
Επιλέγοντας την ΑΠΟΤΙΜΗΣΗ ΒΑΘΜΟΥ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ εμφανίζεται το παρακάτω παράθυρο :





Οθόνη 4-9 : Αποτίμηση βαθμού επικινδυνότητας

Στην ΑΠΟΤΙΜΗΣΗ ΑΠΕΙΛΩΝ εμφανίζεται το παρακάτω παράθυρο :



Οθόνη 4-10 : Αποτίμηση απειλών

Στον εσωτερικό πίνακα εμφανίζεται η τιμή κάθε απειλής βάσει του πίνακα αξίας αγαθών και των συνεντεύξεων για απειλές. 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 αφού επικυρωθεί από τη Διοίκηση, τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην ΑΠΟΤΙΜΗΣΗ ΑΔΥΝΑΜΙΩΝ εμφανίζεται το παρακάτω παράθυρο :

Επικυρώστε την τιμή των παρακάτω αδυναμιών :

Εκτύπωση
Επικύρωση

ΒΟΗΘΕΙΑ
Πρόοδος έργου :  $\chi\%$

**Οθόνη 4-11 : Αποτίμηση αδυναμιών**

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

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

Με την επιλογή ΑΠΟΤΙΜΗΣΗ ΤΙΜΩΝ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ εμφανίζεται το παρακάτω παράθυρο :

Επικυρώστε τις τιμές επικινδυνότητας :

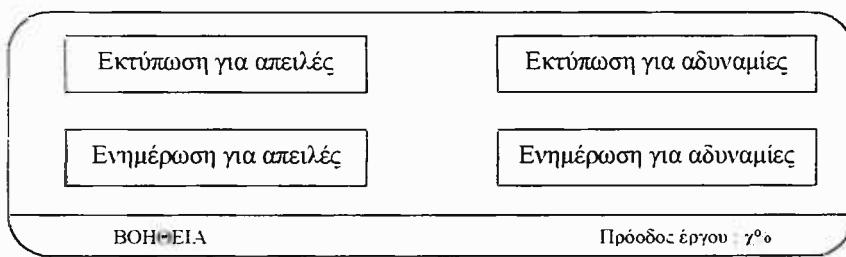
Εκτύπωση
Επικύρωση

ΒΟΗΘΕΙΑ
Πρόοδος έργου :  $\chi\%$

**Οθόνη 4-12 : Αποτίμηση τιμών επικινδυνότητας**

Στον εσωτερικό πίνακα εμφανίζεται η τιμή επικινδυνότητας για κάθε αγαθό του οργανισμού και στο σύνολό του κατά φθίνουσα σειρά, λαμβάνοντας υπόψιν τον πίνακα απειλών – αγαθών, τον πίνακα πιθανών σεναρίων προσβολής και τον πίνακα αδυναμιών. Ο αναλυτής εκτυπώνει τον ταξινομημένο πίνακα αδυναμιών τιμών επικινδυνότητας και αφού επικυρωθεί από τη Διοίκηση, τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

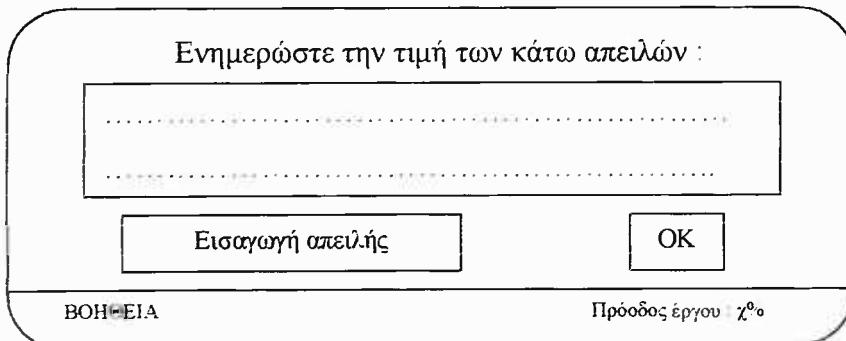
Με την επιλογή ΠΑΡΑΓΩΓΗ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ εμφανίζεται το παρακάτω παράθυρο :



Οθόνη 4-13 : 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 ανάγκη εισαγωγής στοιχείων σχετικών με τους συνεντευξιαζόμενους. Ήδη τα σχετικά στοιχεία έχουν εισαχθεί στο προηγούμενο βήμα, αυτό του υπολογισμού της αξίας αγαθών.

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



Οθόνη 4-14 : Ενημέρωση για απειλές

Μέσω της επιλογής αυτής εμφανίζεται το κάτω παράθυρο :

Όνομα απειλής :	.....
Περιγραφή :	.....
<input type="button" value="OK"/>	

#### Οθόνη 4-15 : 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.

Ενημερώστε την τιμή των κάτω αδυναμιών:

**Εισαγωγή αδυναμίας**

**OK**

#### **Οθόνη 4-16 : Ενημέρωση για αδυναμίες**

Μέσω της επιλογής αυτής εμφανίζεται το κάτω παράθυρο :

Όνομα αδυναμίας :	.....
Περιγραφή :	.....
<input type="button" value="OK"/>	

#### Οθόνη 4-17 :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 :

Επιλογή πολιτικής ασφάλειας	Επιλογή αντιμέτρων	Επιλογή στρατηγικού σχεδίου εφαρμογής
ΒΟΗΘΕΙΑ		Πρόοδος έργου : χ%

Οθόνη 4-18: Δημιουργία σχεδίου ασφάλειας

Στην επιλογή ΕΠΙΛΟΓΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ εμφανίζεται το παρακάτω παράθυρο :

Επιλέξτε πολιτική ασφάλειας :		
.....		
Εισαγωγή πολιτικής	Εκτύπωση	Επικύρωση
ΒΟΗΘΕΙΑ	Πρόοδος έργου : χ%	

Οθόνη 4-19 : Επιλογή πολιτικής ασφάλειας

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

Όνομα πολιτικής : .....
Περιγραφή : .....
OK

Οθόνη 4-20 : Εισαγωγή πολιτικής

Ο αναλυτής πληκτρολογεί όλα τα σχετικά στοιχεία και με το OK ενημερώνεται κατάλληλα η βάση γνώσης. Ο αναλυτής εκτυπώνει την κατάλληλη πολιτική ασφάλειας και αφού επικυρωθεί από τη Διοίκηση, τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Στην επιλογή ΕΠΛΟΓΗ ΑΝΤΙΜΕΤΡΩΝ εμφανίζεται το παρακάτω παράθυρο :

Επιλέξτε αντίμετρα :

Εισαγωγή αντιμέτρου

Εκτινάσιμη

Επικύρωση

ΒΟΗΘΕΙΑ

Πρόοδος έργου

Οθόνη 4-21 : Επιλογή αντιμέτρων

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

Όνομα αντιμέτρου : .....

Περιγραφή : .....

OK

Οθόνη 4-22 : Εισαγωγή αντιμέτρου

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

Στην επιλογή ΕΠΛΟΓΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ εμφανίζεται το παρακάτω παράθυρο :

Επιλέξτε στρατηγικό σχέδιο εφαρμογής :

Εισαγωγή σχ ασφάλειας      Εισαγωγή στρατ σχεδίου      Εκτύπωση      Επικύρωση

ΒΟΗΘΕΙΑ      Πρόσθιος έργου : Χ<sup>ο</sup>

Οθόνη 4-23 : Επιλογή στρατηγικού σχεδίου εφαρμογής

Ο πίνακας περιλαμβάνει στρατηγικά σχέδια εφαρμογής βάσει των στοιχείων του επιλεγμένου πίνακα αντιμέτρων 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 ασφάλειας τότε η βάση γνώσης πρέπει να ενημερωθεί χρησιμοποιώντας τα αντίστοιχα πλήκτρα που εμφανίζουν τα παρακάτω παράθυρα :

Όνομα στρατ σχεδίου : .....  
Περιγραφή : .....

OK

Οθόνη 4-24 : Εισαγωγή στρατηγικού σχεδίου

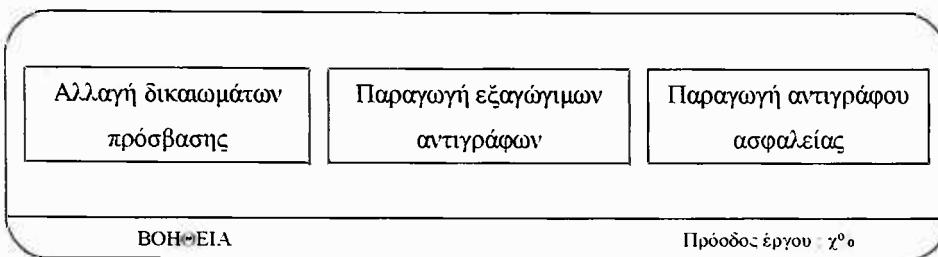
Όνομα σχ ασφάλειας : .....  
Περιγραφή : .....

OK

Οθόνη 4-25 : Εισαγωγή σχεδίου ασφάλειας

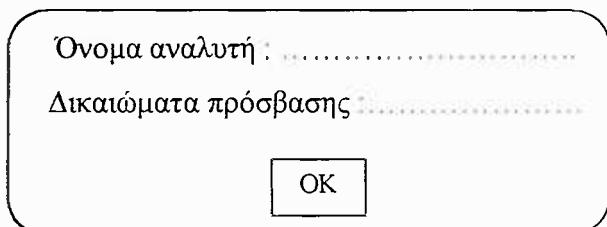
Ο αναλυτής πληκτρολογεί όλα τα σχετικά στοιχεία και με το OK ενημερώνεται κατάλληλα η βάση γνώσης. Ο αναλυτής, στη συνέχεια, εκτυπώνει το επιλεγμένο σχέδιο ασφάλειας και αφού επικυρωθεί από τη Διοίκηση, τότε επιλέγει την ΕΠΙΚΥΡΩΣΗ για να ενημερωθεί κατάλληλα η βάση γνώσης.

Επιλέγοντας τις βοηθητικές λειτουργίες εμφανίζεται το παρακάτω παράθυρο :



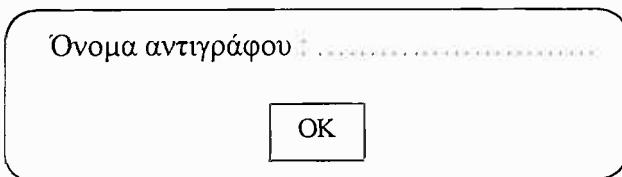
Οθόνη 4-26 : Βοηθητικές Λειτουργίες

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



Οθόνη 4-27 : 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 στο CD ROM. Το αντίγραφο μπορεί να είναι είτε κάποια έκθεση προς τη διοίκηση, είτε κάποιος πίνακας.



Οθόνη 4-28 : Παραγωγή εξαγώγιμων αντιγράφων

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

#### 4.2.2.1.2 Μορφή εκθέσεων

Οι εκθέσεις μπορεί να είναι είτε τα ερωτηματολόγια για επιπτώσεις, απειλές και αδυναμίες του οργανισμού, είτε οι πίνακες αγαθών, αξίας αγαθών, απειλών –αγαθών, αδυναμιών. Επίσης μπορεί να είναι ο ταξινομημένος πίνακας τιμών επικινδυνότητας, η έκθεση με την επιλεγμένη πολιτική ασφάλειας ή με τον επιλεγμένο πίνακα αντιμέτρων ή τέλος το επιλεγμένο σχέδιο ασφάλειας.

Στα ερωτηματολόγια θα αναγράφονται τα στοιχεία του συνεντεύξιαζόμενου, 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 μία 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.

#### 4.2.2.2 Διεπαφές 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 III 755 MHz, 128 MB SDRAM, HDD 18GB, Κάρτα οθόνης AGP, Ποντίκι PS/2, Πληκτρολόγιο PS/2, Οθόνη 17 inch, φίλτρο οθόνης και Εκτυπωτής υψηλής ποιότητας (Laser).

#### 4.2.2.3 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 ασφάλειας που παραδίδεται στον προς εξέταση οργανισμό για χρονοπρογραμματισμό των ενεργειών του. Τέλος έχουμε το Σύστημα Διαχείρισης Βάσεως Δεδομένων για διαχείρισης της βάσης γνώσης που είναι ενσωματωμένο μέσα στο εργαλείο.

#### 4.2.2.4 Διεπαφές επικοινωνιών

Το εργαλείο δεν έχει διεπαφές με επικοινωνίες.

#### 4.2.3 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.

##### 4.2.3.1 Στατικές απαιτήσεις

1. Μέγιστο πλήθος αρχείων 1000
2. Μέγιστο πλήθος εγγραφών 100000

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

##### 4.2.3.2 Δυναμικές απαιτήσεις

1. Οι τετριμμένες ενέργειες, δηλαδή αυτές που γίνονται συχνά (πάνω πχ από 50 φορές) θα πρέπει να εκτελούνται μέσα σε  $1 \frac{1}{2}$  δευτερόλεπτο.
2. Οι ενέργειες με μικρή συχνότητα θα πρέπει να εκτελούνται μέσα σε 15 με 20 λεπτά.

#### 4.2.4 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, καθώς και στην εργασία της Λαγού ([13]).

## 5 Σχεδίαση Εργαλείου

Όπως προαναφέρθηκε η σχεδίαση θα ακολουθήσει το μοντέλο του κύκλου ζωής 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 προσαρμόζοντάς το στις ανάγκες της εργασίας αυτής.

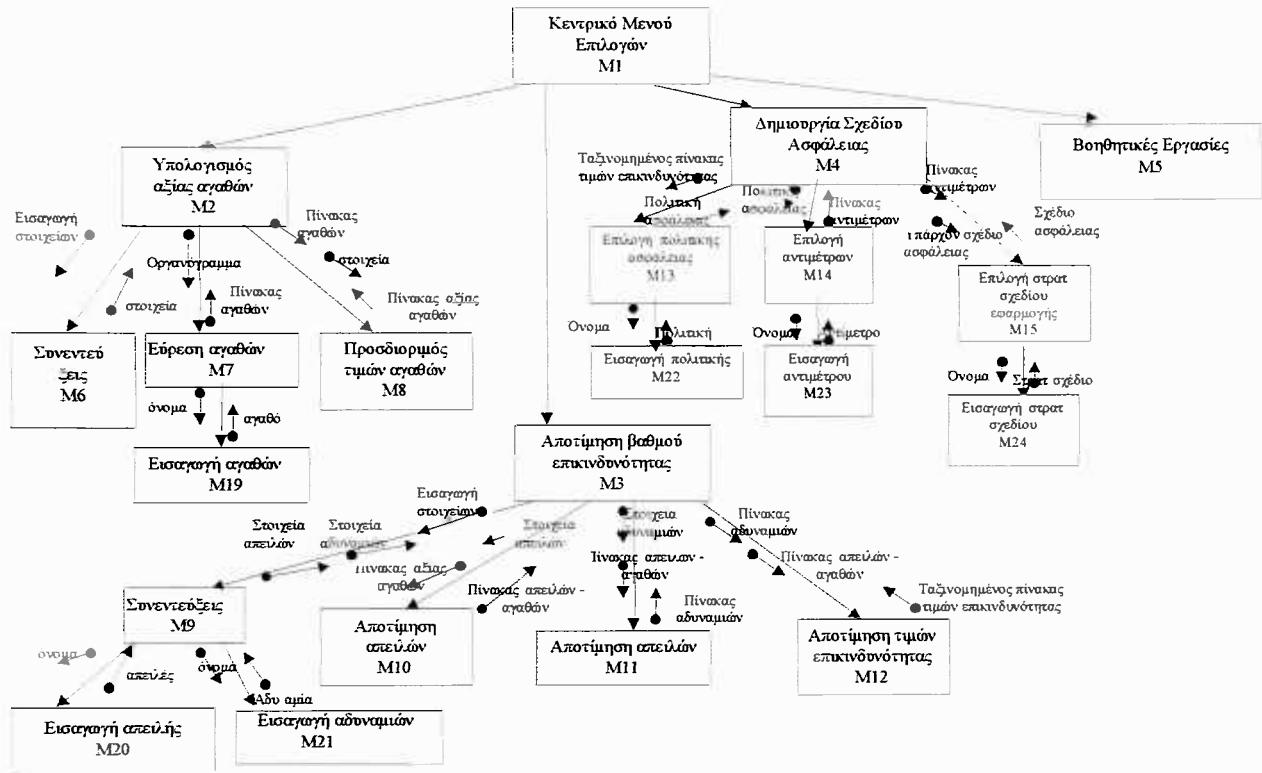
### 5.1 Έγγραφο Περιγραφής Σχεδίου Λογισμικού

Στο ΕΠΣΛ περιγράφονται όλα εκείνα τα στοιχεία που χρειάζονται για την κωδικοποίηση και συντήρηση του Λογισμικού. Έτσι, τα δεδομένα του ΕΠΑΛ εδώ αναλύονται διεξοδικά μετατρέποντάς τα στις κατάλληλες μορφές. Δηλαδή, αποτελεί μία μεταφορά των απαιτήσεων σε μία περιγραφή της δομής του λογισμικού, των στοιχείων λογισμικού, των διεπαφών και των δεδομένων που είναι απαραίτητα για την υλοποίηση ([10], σελ. 237).

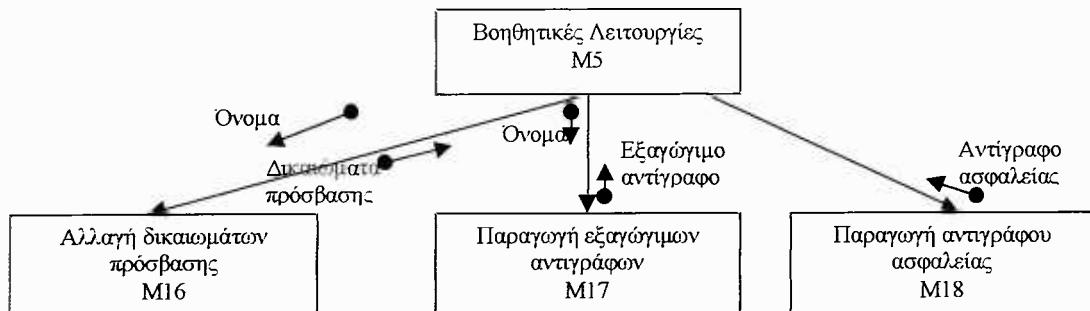
#### 5.1.1 Περιγραφή αποσύνθεσης

Η περιγραφή αποσύνθεσης αποτυπώνει τη διαίρεση του συστήματος Λογισμικού σε οντότητες σχεδίου. Για την παρουσίαση θα χρησιμοποιηθούν τα Διαγράμματα Δομής που παρουσιάζουν την ιεραρχία των μονάδων του συστήματος. Στα παρακάτω σχήματα απεικονίζονται οι μονάδες (η χρήση δύο σχημάτων οφείλεται στην αδυναμία αποτύπωσης όλων των στοιχείων σε ένα σχήμα).

Είναι ορατό, ότι οι μονάδες αντιστοιχούν στις λειτουργίες του συγκεκριμένου εργαλείου. Η περαιτέρω αποσύνθεση οφείλεται στην καλύτερη υλοποίηση του συγκεκριμένου λογισμικού.



Σχήμα 5-1 : Διάγραμμα Δομής



Σχήμα 5-2 : Διάγραμμα Δομής συνέχεια

## Βιβλιογραφία

- [1] Badenhorst K.P., Eloff J.H.P, "Framework of a Methodology for the Life Cycle of Computer Security in an Organization", *Computers & Security*, Vol. 8, pp. 433-442, Elsevier Science Publishers Ltd., 1989
- [2] Baskerville R, "Risk analysis: an interpretive feasibility tool in justifying information systems security", *European Journal of Information Systems*, Vol 1, no 2, pp 121-130, 1991
- [3] Baskerville R, "Information Systems Security Design Methods : Implications for Information Systems Development", *ACM Computing Surveys*, Vol. 25 , No. 4, December 1993
- [4] Booysen H.A.S., Eloff J.H.P., "A methodology for the development of secure Application Systems" in *Information Security : The Next Decade*, (Eds. Ellof, J. and S. Von Solms), IFIP SEC' 95, Chapman & Hall , London 1995
- [5] Hitchings J., "Achieving an Integrated Design : The Way Forward for Information Security", in *Information Security : The Next Decade*, (Eds. Ellof, J. and S. Von Solms), IFIP SEC' 95, Chapman & Hall, London 1995
- [6] Infosec Business Advisory Group, "The IBAG Framework for Commercial IT Security", *IBAG*, Version 2.0, September 1993
- [7] Kiountouzis E.A., Kokolakis S.A., "An analyst's view of IS Security" in *Information System Security facing the information society of the 21<sup>st</sup> Century*, (Eds. S. Katsikas and D. Gritzalis), pp. 23-33, IFIP SEC'96, Chapman & Hall
- [8] Kowalski, S. "IT insecurity: A multi-disciplinary inquiry", *PhD Thesis*, Stockholm University, Sweden, 1994
- [9] McCumber J.R. " Information Systems Security : A comprehensive model" in *Proceedings of the 14<sup>th</sup> National Computer Security Conference*, National Computer Security, October 1991
- [10] Γιακουμάκης Ε.Α., *Τεχνολογία Λογισμικού Τόμος Α*, Εκδόσεις Α. Σταμούλης, Αθήνα-Πειραιάς 1994
- [11] Κιουντούζης Ε.Α., *Μεθοδολογίες Ανάλυσης & Σχεδιασμού Πληροφοριακών Συστημάτων*, Εκδόσεις Ευγ. Μπένου, Αθήνα, 1997
- [12] Κοκολάκης Σπυρίδων, "Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων : Εννοιολογικό Πλαίσιο, Μεθοδολογίες και Εργαλεία", *Διδακτορική Διατριβή*, Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής, Ιούνιος 2000
- [13] Λαγούν Ελισάβετ, «Ανάλυση Απαιτήσεων για Ανάπτυξη Εργαλείου Υποστήριξης της Ανάλυσης και Διαχείρισης Επικινδυνότητας Πληροφοριακών Συστημάτων», *Διπλωματική Διατριβή*, Οικονομικό Πανεπιστήμιο Αθηνών, Τμήμα Πληροφορικής, Φεβρουάριος 2000



80025 75540

